Max Planck Institute
for Innovation and Competition

Max Planck Institute for Innovation and Competition Research Paper No. 21-25

To Break Up or Regulate Big Tech?

Avenues to Constrain Private Power in the DSA/DMA Package

Heiko Richter, Marlene Straub, Erik Tuchtfeld
(*Editors*)

Max Planck Institute for Innovation and Competition Research Paper Series

Heiko Richter • Marlene Straub • Erik Tuchtfeld
(Editors)

To Break Up or Regulate Big Tech?

Avenues to Constrain Private Power in the DSA/DMA Package

Editors

Dr. Heiko Richter, LL.M. (Columbia), Dipl.-Kfm.
Senior Research Fellow, Max Planck Institute for Innovation and Competition, Munich

Marlene Straub, LL.M. (Edinburgh)
Student at the Oxford Internet Institute and Research Assistant at the Centre for Socio-Legal Studies, Oxford, and Editor at Verfassungsblog, Berlin

Erik Tuchtfeld
Research Fellow, Max Planck Institute for Comparative Public Law and International Law, Heidelberg, and External Editor at Verfassungsblog, Berlin

Imprint

2021
Max Planck Institute for Innovation and Competition
Marstallplatz 1, 80539 Munich, Germany

ISBN 978-3-00-070284-6

Published under CC-BY-SA 4.0 Germany License
https://creativecommons.org/licenses/by-sa/4.0/deed.de

Foreword

Together with Verfassungsblog, the Max Planck Institute for Innovation and Competition hosted an Online Symposium on the topic "To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package". These contributions are collected in this eBook. Originally, they were published successively on the Verfassungsblog between 30 August and 7 September 2021 at https://verfassungsblog.de/category/debates/power-dsa-dma/.

The key question is whether the Digital Services Act (DSA) and the Digital Markets Act (DMA) are suitable instruments to regulate private power in the digital arena. The concentration of private power in the digital realm is not tenable – on this there is transatlantic consensus. This consensus extends across domains of private power, ranging from power over markets and consumers' behaviour, power over private rule-making to power of and over opinion. But how to regulate such forms of power? And how to cope with the fact that Big Tech's all-encompassing influence questions even these basic definitions and concepts of power? There is no consensus on solutions, but clear trends towards regulatory intervention are visible.

In the US, the antitrust debate was long dormant, but has returned even stronger, led by academics who have been invited into the Biden administration. The suggestion to 'break up' Big Tech companies carries a different weight, if coming from within the US government. Moreover, the reform of Section 230 on limited liability and Good Samaritan protection has a global impact, potentially overshadowing any regulation outside the US.

The EU has already set a quasi-global standard when it comes to regulating power of and over data subjects, by putting the GDPR in place. In contrast, the European Commission's numerous investigations into anticompetitive conduct from Big Tech have been criticised for being relatively slow and ineffective. Besides, liabilities and right protection on the internet are still governed by rules, which have been conceptualized more than two decades ago. Against this backdrop, the Commission published two proposals in December 2020: the Digital Services Act (DSA) and the Digital Markets Act (DMA). Foreseeably, they will be the landmark pieces of digital policy this legislature.

The DSA aims at protecting users' fundamental rights on intermediaries and platforms, while also making these 'safer'. But introducing greater responsibility and accountability among intermediaries might even entrench their power. This dilemma is particularly salient in the realm of content moderation: there is a genuine risk of reinforcing private actors' role as the governors of and power over speech online. One may legitimately argue for private companies moderating speech at different thresholds rather than referring to the human rights frameworks which bind governments. But if exceptionally powerful intermediaries determine what speech is acceptable at scale, does assigning them responsibility and accountability at the threat of liability invite censorship? Who decides what behaviour is responsible? Circularly, would such assignments

of responsibility and accountability invite dependence on private actors, while public institutions retreat from this space? Also beyond content moderation, similar debates on assigning intermediaries greater responsibility and accountability exist across the DSA's scope. For example, in amorphous due diligence obligations, in the notice and takedown regime, towards systemic risks and towards gaps in the proposal (e.g. an absence of provisions on behavioural targeting or the adtech industry). Each of these issues has the potential to strengthen private power, if not addressed with enough precision.

The DMA is intended to mitigate this concern – at least to some extent and with regards to market power. It aims to establish a level playing field among digital corporations, ensuring competitiveness, growth and fostering innovation, while targeting gatekeeper – meaning very big and powerful – platforms, in particular. This approach means a fundamental shift towards preventive regulation. It contains a bundle of prohibitions of practices (e.g. as self-preferencing, or combining personal data from their core platform services with data from other sources) and obligations (e.g. providing access, interoperability, transparency, and sharing of information and data). But does the DMA provide an effective toolbox, and is it ready to cope with the future realities of digital markets? And to what extent can it sustainably solve the problems of private power? The DMA may be regarded as too cautious, as it does not cover situations of relative power dependency, and it presumes a primacy of behavioral over structural remedies. Yet, the DMA would immensely increase the power of the European Commission as a regulatory authority, and its sole reliance on effective public enforcement presupposes a well-functioning public government apparatus. This inevitably leads to a fundamental question: Must the entrenchment of private power necessarily be accompanied by an empowerment of the state, or is the empowerment of other private actors a desired complement or even a better solution?

Evidently, there is a caveat to every statement made, and every statement invites more questions, but they all boil down to this: how does a regulatory choice affect an intermediary's power, and to what extent can the measures included in the DSA and DMA mitigate adverse effects? Any prudent regulatory solution must stand the test of time and consider the distribution of power long-term. It must prove resilient against the backdrop of constant technological progress and socio-economic developments. When tackling these issues, it is therefore essential to bridge disciplinary silos: data protection law, consumer protection law, copyright law, competition law and constitutional law each consider solutions to address private power. But more than ever before, the age of Big Tech has driven these disciplines to overlap and work with each other.

Accordingly, this eBook brings together several contributions from different perspectives, which also aim to extend the scientific discourse on the topic to a wider audience. We are sincerely grateful for the commitment of all authors and the good cooperation.

The Editors

Table of Contents

II. The Digital Markets Act (DMA)

III. Enforcement

I

The Digital Services Act (DSA)

The DSA Proposal's Impact on Digital Dominance

Ilaria Buri • Joris van Hoboken

One of the most pressing questions in the ongoing debates about the Digital Services Act (DSA) proposal is the question of entrenching dominance. While the DSA aims at providing a harmonized regulatory framework for addressing online harms, there is a risk that imposing accountability at the threat of fines might increase the power of already dominant intermediaries. This problem is particularly evident for content moderation, where over the last decades a handful of services have consolidated their position as the primary arbiters of speech and online activity.

One of the most pressing questions in the ongoing European debates about the Digital Services Act (DSA) proposal[1] is the question of dominance, and specifically the question of the disproportionate power and societal impact of dominant services on online speech and the fundamental rights of users.

With the DSA proposal, the European Commission aims to provide a new regulatory framework for the responsibility of online services in the EU internal market. Specifically, the DSA departs from the self-regulatory paradigm for online service responsibilities. It sets out to overcome the existing fragmentation and regulatory gaps by defining clear and proportionate obligations for online services with regard to illegal content and content moderation practices more generally, which reflect the difference in resources and societal impact of the various actors on the market. In the intention of the Commission, legal clarity should, in turn, translate into a safer online environment, where providers are held accountable and users' fundamental rights (in particular, freedom of expression, privacy and data protection, non-discrimination and right to an effective legal remedy) are duly protected.

Thus, the DSA aims at providing a harmonized regulatory framework for addressing online harms, while protecting users' fundamental rights. However, there is a risk that imposing accountability at the threat of fines might increase the power of already dominant intermediaries. This problem is particularly evident for content moderation, where the DSA framework threatens to further strengthen the role of Big Tech in determining what is acceptable online speech. Over the last decades, a handful of services have consolidated their position as the primary arbiters of speech and online activity. The fact that Facebook is actively calling for increased regulation, widely considered to be informed by a wish to further consolidate its power, may serve as a warning for the potential anti-competitive impacts of regulation such as the DSA.

In this contribution, we discuss the question of whether the DSA can be expected to further entrench the power of dominant services. First, we consider how the DSA impacts the relative competitiveness of dominant and smaller services, and how the economics of content moderation tend to favour very large online platforms (VLOPs). Second, we focus on a selection of provisions in the DSA and how these have the potential to entrench VLOPs' dominance and private power, while providing suggestions for better safeguards.

The Likely Economic Impact of the DSA

We can start with the question whether the DSA can significantly alter the power dynamics underlying innovation and competition in the market of intermediary services. While the DSA focuses on issues of liability for illegal content and responsibility in content moderation processes more generally, a separate proposal, the Digital Markets Act (DMA),[2] aims to address issues of competition in digital markets. General issues of economic dominance and monopoly power will have to be addressed through competition law and the DMA.

With the DSA, a central goal for the European Commission (EC), related to competition, is to overcome legal fragmentation with a set of harmonized rules and provide "the conditions for innovative digital services to emerge and scale up in the internal market" (Recital 4). Legal fragmentation has been a problem since the adoption of the eCommerce Directive (ECD),[3] which left crucial details to self-regulation and national law. In the last years, fragmentation has further increased as a result of legislative developments at the national level (such as the German NetzDG[4]). While a more harmonized framework would certainly benefit dominant companies, well-positioned to respond to a more strictly harmonized EU regulatory environment, a recurring fear is that smaller service providers might falter.

However, the EC's Impact Assessment[5] accompanying the DSA proposal is very positive about the benefits of overcoming fragmentation for smaller companies: they would be able to scale up their offerings in a more robust EU market. Focusing on the increased cross-borders turnover resulting from harmonization, the EC estimates a cost reduction of around 400.000 € per annum for a medium enterprise operating in three Member States and of 4 million € for the same company operating in 10 Member States. In the EC's view, the cost savings would be particularly beneficial to micro and small enterprises, who encounter prohibitive costs when offering services in more than two Member States.

Although the EC acknowledges that compliance with the DSA obligations entails additional costs for all hosting service providers, according to its calculations, however, these costs would be lower than those of facing a fragmented legal environment. Estimating the DSA-related expenditures is complicated though, as these costs are highly dependent on the volume of notices received by the individual service provider.

Overall, the EC's assessment report does not warrant the conclusion that the costs of DSA compliance would be prohibitive for SMEs and/or disproportionately affect them *vis-à-vis* VLOPs. Notably, though, the calculations on costs and administrative burdens at company level are not exhaustive on the economic impact of the DSA: for instance, the costs for out-of-court dispute settlement are not included, and the impact assessment's tables only refer to the costs of notice and action procedures, while it is unclear if this covers the moderation of harmful/undesirable (but not necessarily illegal) content. The impact assessment's calculations should therefore be taken with a grain of salt.

In addition, the economic considerations found in the Impact Assessment primarily relate to the first policy goal of the DSA – strengthening the Digital Single Market by removing legal fragmentation – and do not necessarily capture the broader economics underlying content moderation today. In the absence of a complete overhaul of platform governance, the economics of content moderation significantly benefit larger companies. First, the reduction of costs through legal harmonization does not per se translate into an ability of smaller actors to scale up and compete with the big ones. Content moderation of internationally operating social media services also entails significant investments in personnel (including moderators) with relevant expertise on language, politics, culture, government relations and other jurisdictional specifics, with significant efficiency gains for larger services. The possibilities of automation[6] in detecting and addressing illegal and harmful content issues are likewise significantly greater for services with the largest volume of user activity and content notices. Arguably, the higher costs envisaged for VLOPs are marginal, compared to their structure and turnover, and their established risk management procedures.

In summary, addressing legal fragmentation will have some important benefits for small service providers, but this will likely benefit large service providers as well – if not more – and not affect their ability to dominate. But of course, the question of digital dominance and content moderation extends beyond the economics of content moderation to the other two key policy objectives of the DSA: addressing online harms and protecting users' fundamental rights.

Beyond the Economic Impact

The DSA proposal keeps the basic intermediary liability safe harbor regime of the ECD in place (Articles 3-5 DSA). The importance of a harmonized safe harbor regime is likely significant for smaller service providers. On the contrary, for larger service providers that are actively moderating content, one could raise the question if a safe harbor is still warranted. While we do not support such proposals, considering their probable negative impact on fundamental rights, any initiative to condition the safe harbors on compliance with particular due diligence obligations should be restricted to dominant service providers, to prevent further harm to the competitiveness of smaller players. More importantly, in our view, there are a number of noted

uncertainties[7] about the applicable scope of the DSA's safe harbors and due diligence framework, in particular in relation to search engine, infrastructural, messaging, and ancillary services. There is a risk that the legal certainty provided by the DSA will be the greatest for dominant social media and marketplace services.

The DSA continues, and in some ways further reinforces, the tendency to outsource primary decisions on fundamental rights and speech governance to platforms. This "privatized enforcement" phenomenon[8] is present in many of the DSA procedures for tackling illegal content, including orders to act against illegal content in Article 8 and 9 DSA, the notice-and-takedown mechanisms in Article 14 DSA, the measures and protection against misuse in Article 20 DSA and the notification of suspicions of criminal offences in Article 21 DSA. This tendency combines with the incentives, also present in the DSA, towards over-removal of lawful content in order to avoid fines. The complaint procedure of Article 17 DSA is also noteworthy in this regard. It provides users with an ability to contest undue removals of content by online platforms. But it also places the responsibility for operating these procedures on the platforms and does not impact the discretion of online platforms to act on the basis of their terms of service. This, in combination with the proposed regime for out-of-court dispute settlement, highlights the extent to which content moderation is steered away from more robust judicial processes, which more robustly guarantee users' fundamental rights.

The risk-based approach for content moderation imposed on VLOPs raises some additional concerns in this regard. The risk assessment will involve a complex balancing exercise between fundamental rights and other policy objectives (the eradication of online harm and disinformation, in particular) by dominant online platforms. The only stakeholders with some leverage over these risk assessments are the European Board for Digital Services (composed of the national regulators) and the EC. Specifically, Article 27 DSA requires them to recommend best practices for VLOPs to mitigate the systemic risks identified either in the assessment under Article 26 DSA or through data access and transparency reporting. Once such balancing has been conducted and guidelines have been issued, VLOPs are easily provided with an additional line of defense in imposing their standards for content moderation on users. Additional clarity is needed on the precise focus of the risk assessments, to prevent this new framework from becoming captured by dynamics between dominant platforms and regulators to the detriment of users.

Article 12 DSA proposal obliges intermediaries to provide information on any restrictions applied for the purpose of content moderation, and to act in a diligent, objective and proportionate manner, with due regard for the fundamental rights of users. Dominant online platforms' terms of service exert a particularly strong influence on users' fundamental rights, shaping the boundaries of legitimate online speech globally. Within the current text, the proportionality standard could be used to give horizontal effect[9] to freedom of expression. But Article 12 DSA could more explicitly take into account the dominance of particular online platforms. It could incorporate stricter

standards for dominant services, limiting their discretion in moderating speech on matters of public concern. Given the exceptional power over speech of the VLOPs, Article 12 DSA could more generally clarify[10] that fundamental rights are applicable in the horizontal relation between them and the users and require VLOPs to follow human rights law standards for online content moderation.

Conclusion

This discussion has looked at how the problem of digital dominance is affected by the DSA proposal. While the DSA proposal tries to not aggravate this situation – and we can agree with the EC that addressing legal fragmentation helps smaller companies operating in the EU – there is no doubt that the economics of content moderation strongly benefit larger companies. Outside of a restructuring of the market (through the lens of economic regulation and competition law), obligations on companies to address online harms and at the same time protect fundamental rights end up playing into the hands of dominant companies. Within its current scope, what should be expected from the DSA is to include robust safeguards for users, minimize privatized enforcement dynamics and put more focus on the horizontal effect of fundamental rights, including to limit the discretion of dominant players. These elements could be complemented by stronger restrictions on the business models of dominant platforms (notably based on pervasive tracking and targeting of their users and attention-maximizing algorithms), which have been linked to the spread of harmful content[11] and to a variety of other individual and societal risks, including some of the issues identified by the DSA as "systemic risks". While we cannot expect the DSA (considering its scope and focus) to solve the issues of dominance in content moderation, several improvements are warranted to limit the exceptional power of the big actors in content moderation and thus support a better protection of fundamental rights and key societal interests.

This article has originally been published on Verfassungsblog (2021/8/30), https://verfassungsblog.de/power-dsa-dma-01/, DOI: 10.17176/20210830-112903-0.

Ilaria Buri is a research fellow at the Institute for Information Law, University of Amsterdam, where her work focuses on the "DSA Observatory" project. She previously worked as a researcher at the KU Leuven Centre for IT and IP Law (CiTiP) on matters of data protection and cybersecurity. She is admitted to the Bar in Italy and, prior to joining academia, she gained extensive experience as a practitioner in law firms and worked at the European Commission (DG Clima).

Joris van Hoboken is a Professor of Law at the Vrije Universiteit Brussels and an Associate Professor at the Institute for Information Law, University of Amsterdam. He works on the intersection of fundamental rights protection (privacy, freedom of expression, non-discrimination) and the regulation of platforms and internet services. At the VUB, he is appointed to the Chair 'Fundamental Rights and Digital Transformation', established at the Interdisciplinary Research Group on Law Science Technology & Society, with the support of Microsoft.

[1] European Commission, Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC, COM(2020) 825 final.
[2] European 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), COM(2020) 842 final.
[3] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), (2000) OJ L178/1 (ECD).
[4] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) (2017, BGBl. I 3352), last modified 2021 (BGBl. I 1436).
[5] European Commission, "Impact Assessment Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" (Staff Working Document), SWD(2020) 348 final.
[6] Tarleton Gillespie, "Content moderation, AI, and the question of scale" (2020) 7 Big Data & Society Vol. 2.
[7] European Parliament – Policy Department for Economic, Scientific and Quality of Life Policies, "The Digital Services Act and the Digital Markets Act: A forward-looking and consumer-centred perspective" (Workshop) 2021.
[8] Christina Angelopoulos and others, "Study of fundamental rights limitations for online enforcement through self-regulation" (2016).
[9] Bundesgerichtshof, judgements of 29 July 2021, III ZR 179/20 and III ZR 192/20.
[10] Naomi Appelman and others, "Article 12 DSA: Will platforms be required to apply EU fundamental rights in content moderation decisions?" *DSA Observatory* (31 May 2021) https://dsa-observatory.eu/2021/05/31/article-12-dsa-will-platforms-be-required-to-apply-eu-fundamental-rights-in-content-moderation-decisions/ accessed 25 September 2021.
[11] Karolina Iwańska, "Can the EU Digital Services Act contest the power of Big Tech's algorithms?" *EDRi* (2 August 2021) https://edri.org/our-work/can-the-eu-digital-services-act-contest-the-power-of-big-techs-algorithms/ accessed 25 September 2021.

The European Constitutional Road to Address Platform Power

Giovanni De Gregorio • Oreste Pollicino

The functions exercised by online platforms raise questions about the safeguarding of fundamental rights and democratic values from the autonomous discretion of the private sector, which is not bound by constitutional law. The Digital Services Act horizontally translates European constitutional values to private relationships, to limit governance by platforms.

In the last twenty years, the policy of the European Union in the field of digital technologies has shifted from a liberal perspective to a constitutional strategy, aimed at protecting fundamental rights and democratic values, as driven by European digital constitutionalism[1]. This paradigm shift was primarily triggered by the intolerance of the European constitutional system to the consolidation of platform powers, establishing standards and procedures competing with the rule of law. Looking at online content, the deplatforming of Donald Trump or the Facebook decision to block news in Australia are just two paradigmatic examples of governance by platforms; not only over online speech but also fundamental rights and democratic values.

Evidently, the rise of the algorithmic society[2] has led to a paradigmatic change, wherein public power is no longer the only threat to the respect of constitutional principles. The functions exercised by online platforms raise questions about the safeguarding of fundamental rights and democratic values from the autonomous discretion of the private sector, which is not bound by constitutional law. This encourages reflection on how constitutional law could evolve to face the challenges at the intersection between public authority and private ordering.

The Digital Services Act[3] can be considered an expression of the constitutional path of the Union to address platform power. It is a piece of the broader puzzle of measures to shape Europe's digital future[4]. The GDPR, the proposals for the Digital Markets Act[5] or the Artificial Intelligence Act[6] are other examples of this framework. Against the consolidation of new areas of (private) power, we argue that European constitutional law provides instruments to address this situation. The horizontal effect of fundamental rights and the introduction of substantive and procedural safeguards are two primary pieces to protect European constitutional values in the algorithmic society. The Digital Services Act, in particular, horizontally translates constitutional values to private relationships, thus, representing an example of the European approach to limit platform power.

Framing Platform Power from a Constitutional Perspective

The rise and consolidation of platforms' powers is not just a coincidence driven by market dynamics. It is primarily the result of a liberal approach taken by constitutional democracies across the Atlantic towards digital technologies at the end of the last century. At that time, it was not possible to foresee this development. Nevertheless, immunizing or exempting these actors – Big Tech's predecessors – from third-party responsibility has contributed to the transformation of economic freedoms into something that resembles the exercise of powers as vested in public authorities. In other words, the freedom to conduct business has since gained a new dimension, namely, that of private power, which – it goes without saying – brings significant challenges to the role and tools of constitutional law. Instruments of private law or competition law would, in fact, no longer be sufficient to capture the functioning of these actors.

Private actors are now vested with some forms of power that are no longer of merely economic nature. A broad range of decision-making activities are increasingly delegated to algorithms, which can advise, and, in some cases, take decisions based on the data they process, thus mediating how individuals exercise their rights and freedoms. The case of content moderation shows how platforms take autonomous decisions in designing the rules of moderation, enforcing these standards, while balancing rights and freedoms mirroring constitutional review. These are examples of the exercise of quasi-public powers[7], which *de facto* propose an alternative model to define the boundaries of online speech on a global scale.

The global pandemic has further highlighted the constitutional role of online platforms in the algorithmic society. On the one hand, private platforms have provided (information) services which even the State failed to deliver promptly, while, on the other hand, contributing to the spread of disinformation, inter alia in deciding to rely just on automated moderation[8], sending human moderators home. In other words, their central role during the pandemic, good and bad, has resulted in platform actors being thought of as public utilities or essential parts of the social infrastructure, even more so than before.

Despite this relevance, online platforms are private actors, to whom constitutional law does not generally nor directly apply, thus limiting the horizontal extension of constitutional obligations. Rather, constitutional theory frames power as historically vested in public authorities, which by default hold the monopoly on violence under the social contract. Power distributions in the algorithmic society question this premise.

Therefore, the consolidation of the algorithmic society requires dealing not only with the troubling legal uncertainty relating to digital technologies, or the abuse of powers by public authorities, but also the consolidation of private powers defining standards of protection and procedures, as helped by automated decision-making systems.

Searching for (Constitutional) Remedies

Constitutional law provides at least two remedies to mitigate the consolidation of unaccountable powers: the first concerns the horizontal application of fundamental rights vis-à-vis private parties; the second comes from the new phase of European digital constitutionalism, looking at the constellation of substantive and procedural rights to increase the transparency and accountability of platforms powers.

The doctrine of horizontal effect extends constitutional obligations to private actors. Unlike the liberal spirit of the vertical approach, this theory rejects a rigid separation between public and private actors in constitutional law. While subject to a narrower constraints in the US environment, as shown by the recent decision in *Manhattan v. Halleck*[9], in Europe, there is more room to extend constitutional obligations to private actors, when freedoms reflect the exercise of public powers. In particular, some cases in Italy[10] and Germany[11] have shown that platforms cannot take discretionary decisions on deplatforming political parties and figures. Instead, they should take into account constitutional safeguards, which limit the possibility to censor free speech. Likewise, in Germany, another court's decision[12] addressing hate speech showed the limits applying to content moderation. This framework underlines how courts are horizontally stretching constitutional values to limit platform power while enlarging the boundaries of what, in the US, would be called the public forum doctrine.

However, a broader reliance on the horizontal effect doctrine could lead to some drawbacks. Applying this doctrine extensively could undermine legal certainty. Indeed, virtually every private conflict can be represented as a clash between different fundamental rights. In effect, constitutional obligations could be extended to every private relationship. Further, since fundamental rights can only be applied horizontally *ex post* by courts through the balancing of the rights in question, this process could increase the degree of uncertainty, as well as judicial activism[13], with evident consequences for the separation of powers and the rule of law. Nevertheless, the horizontal extension could be a strategic move for courts to underline abuses of freedoms or the performance of functions mirroring public authorities.

Due to the drawbacks, it is also worth reaching beyond the debate on horizontal/vertical effects of fundamental rights in the digital age. An alternative weapon might be a digital *habeas corpus* of substantive and procedural rights, derived from the positive obligation of States to ensure the protection of human rights, which in the European context primarily comes from the framework of the Council of Europe. This requires public actors to intervene in order to protect rights and freedoms from interferences. While substantive rights concern the status of individuals as subjects of a kind of sovereign power that is no longer exclusively vested in public authorities, procedural rights stem from the expectation that individuals should be able to claim and enforce their rights before bodies other than traditional jurisdictional bodies, which employ methods different from judicial discretion, such as technological and horizontal due process. Another potential option could focus on whether human dignity,

characterising European constitutionalism, can be enforced as 'counter-limit' that, regardless of any horizontal/vertical effect, is likely to create sufficient constraints even for private actors, as the Omega[14] case delivered by the Court of Justice seems to demonstrate.

If, on the one hand, this new digital *pactum subjectionis* requires us to rethink how rights and freedoms are recognised and protected, it is, on the other, also necessary to understand how their enforcement can be effective, how they can actually be put into practice. In other words, the claim for a new catalogue of substantive rights must be coupled with certain procedural guarantees that allow individuals to rely on a new system of rights and remedies limiting platform power. Therefore, it is necessary to consider the procedural counterweight to the creation of new rights, focusing on the fairness of the process by which individuals can enforce them.

The Digital Services Act Expressing European Digital Constitutionalism

Within this framework, the adoption of the Digital Services Act will play a critical role in providing a supranational and horizontal regime to mitigate the challenges raised by the power of online platforms in content moderation. This legal package promises to provide a comprehensive approach to increase transparency and accountability in content moderation. The adoption of the Digital Services Act can be considered a milestone of the European constitutional strategy, still subject to a regulatory framework that dates back to 2000, established by the e-Commerce Directive[15]. The Digital Services Act will also contribute to fostering the rule of law by counteracting fragmentation resulting, for instance, from the introduction of different guarantees and remedies at supranational and national level by the Copyright Directive[16] or the amendments to the AVMS Directive[17].

Even if the Digital Services Act proposal maintains the rules of exemption of liability for online intermediaries, it will introduce some (constitutional) adjustments to increase the level of transparency and accountability of online platform. By addressing transparency gaps and providing for novel redress systems, the Commission aims at protecting users from unwarranted interferences, potentially harmful to their constitutional rights to freedom of expression and protection from discrimination. In the meantime, the goal is seemingly also that of guaranteeing the 'passive' dimension of freedom of information, that is, the right to receiving pluralistic and unpolluted information, by making sure that individuals are more aware of the functioning of and risks connected to recommender systems.

A variety of the Digital Services Act provisions precisely limit the discretion of platforms in governing their services, by introducing substantive and procedural safeguards. For instance, the Digital Services Act proceduralises the process of notice and take down (Article 14), while also requiring platforms to provide a reason when removing content (Article 15). It is worth underlining also how the Digital Services Act introduces additional obligations with respect to "very large online platforms" (VLOPs),

with specific respect to content curation and to the need to foster transparency regarding such an activity. In particular, these platforms are required to conduct a risk assessment about any significant systemic risks stemming from the functioning and use made of their services in the Union, at least once a year (Article 26), while putting in place reasonable, proportionate and effective mitigation measures (Article 27). Likewise, pursuant to Article 29, VLOPs will be required to include in their terms and conditions, in a clear, accessible and easily comprehensible manner, the parameters used by recommender systems. These obligations are just some examples limiting platform discretion, thus, pushing these actors to be more transparent and accountable in their process of content moderation, as inspired by the new phase of European digital constitutionalism.

Therefore, the Digital Services Act can be taken as an example of the resilience of the European constitutional model reacting to the threats of platform power. This new phase should not be seen merely as a turn towards regulatory intervention or an imperialist extension of European constitutional values. It is more a reaction of European digital constitutionalism to the challenges for fundamental rights and democratic values in the algorithmic society. In effect, this framework underlines how constitutional law could play a critical role in limiting platform power, while promoting the protection of fundamental rights and freedoms.

This article has originally been published on Verfassungsblog (2021/8/31), https://verfassungsblog.de/power-dsa-dma-03/, DOI: 10.17176/20210831-113009-0.

Giovanni De Gregorio (@G_De_Gregorio) is postdoctoral researcher working with the Programme in Comparative Media Law and Policy at the Centre for Socio-Legal Studies at the University of Oxford and Academic Fellow at Bocconi University. His research focuses on digital constitutionalism, platform governance and digital policy.

Oreste Pollicino is Professor of Constitutional Law at Bocconi University in Milan, where he also teaches Information and Internet Law, Public Law and Transnational Constitutional Law. He is a member of the Managing Board of the European Agency for Fundamental Rights.

[1] Giovanni De Gregorio, "The rise of digital constitutionalism in the European Union" (2021) 19 International Journal of Constitutional Law 41.
[2] Jack M Balkin, "Free Speech in the Algorithmic Society: Big Data, Private Governance, and New School Speech Regulation" (2018) 51 UC Davis Law Review 1149.
[3] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.

[4] European Commission, "Shaping Europe's digital future" (Communication), COM(2020) 67 final.
[5] European 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)", COM(2020) 842 final.
[6] European Commission, "Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act) and amending certain Union legislative acts" (Proposal), COM(2021) 206 final.
[7] Giovanni De Gregorio, "From Constitutional Freedoms to the Power of the Platforms: Protecting Fundamental Rights Online in the Algorithmic Society" (2019) 11 European Journal of Legal Studies 65.
[8] Elizabeth Dwoskin, Nitasha Tiku, "Facebook sent home thousands of human moderators due to the coronavirus. Now the algorithms are in charge" *The Washington Post* (24 March 2020) https://www.washingtonpost.com/technology/2020/03/23/facebook-moderators-coronavirus/ accessed 25 September 2021.
[9] US Supreme Court, Opinion *Manhattan Community Access Corp. v. Halleck* (2019) 587 U.S. ___.
[10] Tribunale di Roma, *Facebook v. CasaPound* (2020) 80961/19.
[11] Bundesverfassungsgericht, Order of 22 May 2019, 1 BvQ 42/19.
[12] Bundesgerichtshof, judgements of 29 July 2021, III ZR 179/20 and III ZR 192/20.
[13] Oreste Pollicino, "Judicial Protection of Fundamental Rights on the Internet – A Road Towards Digital Constitutionalism?" (Hart Publishing 2021).
[14] ECJ C-36/02 *Omega Spielhallen- und Automatenaufstellungs-GmbH v. Oberbürgermeisterin der Bundesstadt Bonn* (2004) EU:C:2004:614.
[15] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), (2000) OJ L178/1.
[16] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, (2019) OJ L130/92.
[17] Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities, (2018) OJ L303/69.

Five Reasons to be Skeptical About the DSA

Alexander Peukert

In an effort to establish a "safe, predictable and trusted online environment" for the EU, the Digital Services Act proposal sets out an extensive catalogue of due diligence obligations for online intermediaries, coupled with tight enforcement rules. A freedom of expression perspective on the proposal reveals that it partly reinforces Big Tech's control over communication, and moreover fights fire with fire by establishing a powerful public/private bureaucracy able to monitor and potentially manipulate online communication trends.

In an effort to establish a "safe, predictable and trusted online environment" for the EU, the Digital Services Act (DSA) proposal[1] sets out an extensive catalogue of due diligence obligations for online intermediaries, coupled with tight enforcement rules. Whereas the power of Big Tech about the digital public sphere is indeed a reason for concern, a freedom of expression perspective on the DSA proposal reveals that it is problematic in several respects. It partly reinforces Big Tech's control over communication and moreover fights fire with fire by establishing a powerful public/private bureaucracy able to monitor and potentially manipulate online communication trends.

What Freedom of Contract?

The first reason to be skeptical about the DSA is its relation to freedom of contract. The proposal not only covers illegal content of all kinds but also "information incompatible with [...] terms and conditions" of intermediaries (Art. 2(g)(p)(q) DSA). Addressees of the DSA have to be transparent about their contractual speech restrictions (Arts. 12(1), 13(1)(b), 15(2)(e), 20(4) DSA), and they have to apply and enforce these in a "diligent, objective and proportionate manner" (Art. 12(2) DSA).

On the one hand, this scope of application is a correct acknowledgment of the fact – brought to light *inter alia* by experiences with the German Network Enforcement Act[2] (NetzDG) – that Big Tech companies base by far most content moderation measures on their terms and conditions, which they apply on a global scale. If the EU wants to effectively reign in on this practice, it thus has to address terms and conditions. On the other hand, the DSA provisions on point are highly problematic in that they are insufficiently tied to the power of the addressees. None is targeted to very large online platforms (VLOPs). Arts. 12 and 15 DSA even apply to micro or small conduit, caching and hosting services. Whereas courts may eventually draw distinctions between the content moderation of startups and that of VLOPs, Art. 12(2) DSA will, in the meantime, put an additional burden on SMEs while granting broad discretion to VLOPs. Whereas the

former have to cope with an additional financial burden in competing with Big Tech, the latter remain free to define what may and can be said on their platforms – note that Art. 12(2) DSA only regulates the application and enforcement of speech restrictions, not their content.

Such an undifferentiated rule is untenable from the perspective of the freedom of contract. According to the German Federal Constitutional Court[3], the patron of Drittwirkung, in principle all persons have the freedom to choose when, with whom and under what circumstances they want to enter into contracts. Only under "specific circumstances" does the right to equality have horizontal effects between private actors. Whether Facebook's and other VLOPs' community standards present such "specific circumstances" has not yet been settled[4]. What is clear though is that the contractual relationships between SME intermediaries and their users are – beyond consumer protection and antidiscrimination laws – subject to party autonomy. As a consequence, Art. 12(2) DSA should be moved to the VLOP section of the DSA.

Preventing Vague Risks

The second reason to be skeptical about the DSA is its risk prevention approach. Art. 26 DSA obliges VLOPs to constantly identify, analyse and assess "any significant systemic risks" stemming from the functioning and use of their services in the Union. According to Art. 27 DSA, they have to put in place reasonable, proportionate and effective measures to mitigate these risks, for example by adapting their algorithmic content moderation or recommender systems. Again, the DSA proposal delegates wide-ranging and highly sensitive decisions to Big Tech.

Of particular concern in this context is Art. 26(1)(c) DSA, which orders VLOPs to assess the risk of

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

This extremely broad and vague provision not only covers fake accounts and bots spreading illegal content (recital 57) but all kinds of "intentional manipulations" of a VLOP service with a "foreseeable negative effect" on "civic discourse" or effects (of any kind) "related to electoral processes and public security". Such "manipulations" need neither be illegal nor violate terms and conditions when they occur. This follows from Art. 27(1)(a) DSA, according to which VLOPs may have to adapt their terms and conditions in order to manage a systemic risk. Further questions arise: What information is to be banned from the EU Internet via the notion of "civic discourse"? Is exercising freedom of expression online a systemic risk to be mitigated? Rephrasing[5] Art. 26(1)(c) DSA will hardly provide sufficient clarity. Instead, the provision should be deleted.

Over-blocking

The third reason to be skeptical about the DSA is a classical freedom of expression concern: over-blocking. The size of this problem is difficult to ascertain, but the study of Liesching et al.[6] on the practical effects of the German Network Enforcement Act and numerous decisions of German courts ordering Facebook and other platforms to put back posts[7] that had been deleted for violation of community standards show that over-blocking is real. The put back obligation of Art. 17(3) s. 2 DSA proposal is an implicit acknowledgment of this phenomenon.

Nonetheless, the DSA proposal integrates the private practice of automated content blocking into its compliance regime (cf. Arts. 14(6), 15(2)(c), 17(5), 23(1)(c) DSA). It remains a fundamental contradiction of the DSA that algorithmic decision-making is both a reason for its proposal and a measure accepted if not required by it. Worse still, the DSA will create compliance duties with regard to any type of illegal content. The broader though the scope of application of the DSA, including hard cases at the borderline between legality and illegality, the higher the risk of false positives.

When it comes to algorithmic enforcement of copyright on sharing platforms such as YouTube, the Commission apparently shares this skepticism. In her June 2021 guidance[8] on the implementation of Art. 17 of the 2019 Digital Single Market Directive (DSMD)[9], the Commission states that "automated blocking […] should in principle be limited to manifestly infringing uploads" whereas "uploads, which are not manifestly infringing, should in principle go online and may be subject to an ex post human review when rightsholders oppose by sending a notice". Advocate General Saugmandsgaard Øe similarly finds[10] that Art. 17 DSMD is compatible with the right to freedom of expression and information only if interpreted to the effect that "ambiguous" content is not subject to preventive blocking measures. In line with these cautious approaches, the German act transposing Art. 17 DSMD[11] takes great pains to avoid "disproportionate blocking by automated procedures".

The ensuing question for the DSA is this: If automated decision-making does not ensure a balance of all fundamental rights at stake in the area of copyright, then why is it appropriate for all types of illegal content – including copyright infringements but also very sensitive issues like allegedly defamatory political speech? The answer: It is not, and therefore, the DSA should allow automated decision-making only in cases of manifestly illegal content[12].

Regulating "Harmful" Content, in Particular "Disinformation"

The fourth reason to be skeptical about the DSA is that it is not limited to fighting illegal information but that it also addresses the issue of "harmful" content, in particular "disinformation", which is generally understood[13] as

> "*verifiably false or misleading information that is created, presented and disseminated for economic gain or to intentionally deceive the public, and may cause public harm*".

It is true that the DSA proposal neither defines nor directly regulates, in the form of removal obligations, this "delicate area with severe implications for the protection of freedom of expression"[14]. However, recital 5 already refers to the role of intermediaries in the "spread of unlawful or otherwise harmful information and activities". And several recitals mention "disinformation" as one reason for obliging VLOPs to be transparent about the advertisements they display (Art. 30 DSA with recital 63), for future codes of conduct (Art. 35 DSA with recital 68) and for crisis protocols to be facilitated by the Commission in response to "extraordinary circumstances affecting public security or public health" (Art. 37(2)(a) DSA with recital 71). The DSA proposal generally forms part and parcel of EU anti-disinformation policies[15]. Recital 69 refers to the 2018 Code of Practice on Disinformation[16], and in her May 2021 Guidance[17] on strengthening that Code, the Commission promotes its respective suggestions as an "early opportunity for stakeholders to design appropriate measures in view of the adoption of the proposed DSA".

The difficulty with this public-private fight against "disinformation" has become abundantly clear though in the course of the COVID-19 pandemic. In order to get the facts right and tackle COVID-19 disinformation[18], the Commission initiated a monitoring and reporting program[19], under which platforms are "asked" to make their respective policies and actions public. As part of this program, Facebook reported in February 2021[20] that "following consultations with leading health organizations", including the WHO, it will remove the "debunked" claim that "COVID-19 is man-made or manufactured". On May 26, 2021, Facebook informed the public[21], however, that

> "*in light of ongoing investigations into the origin of COVID-19 and in consultation with public health experts, we will no longer remove the claim that COVID-19 is man-made or manufactured from our apps*."

An adequate comment on this affair can be found in Hannah Arendt's 1971 essay "Lying in Politics"[22]. The "right to unmanipulated factual information", posits Arendt, is the "most essential political freedom", without which "all freedom of opinion becomes a cruel hoax". I agree, and therefore the DSA should not establish any direct or indirect removal obligations concerning "disinformation" or other "harmful" yet legal content.

Establishment of a Communication Oversight Bureaucracy

The fifth and final problem with the DSA proposal is that it would create a bureaucracy with the power to supervise not only DSA compliance but general communication trends.

The DSA bureaucracy consists of several interconnected state and non-state actors. The central player in this network is the Commission, which estimates[23] that it needs

50 additional full time positions to manage its various DSA-related tasks. In addition, each Member State shall designate a Digital Services Coordinator (DSC, Art. 38 DSA). The 27 DSCs form an independent advisory group "on the supervision" of intermediaries, named "European Board for Digital Services" (EBDS), which is, again, chaired by the Commission (Arts. 47-48 DSA). The Commission, national DSCs and the EBDS operate in a coordinated manner (Arts. 45-46 DSA).

On the DSA addressee side, VLOPs have to appoint one or more DSA compliance officers who have to ensure inter alia that VLOPs cooperate with authorities (Art. 32 DSA). Further civil society actors complement the DSA bureaucracy, namely entities that are awarded by a DSC the privileged status of a "trusted flagger" (Art. 19 DSA), organisations performing independent DSA audits (Art. 28 DSA) and transnational bodies developing and implementing voluntary industry standards (Art. 34 DSA).

At first sight, these actors are merely there to enforce the DSA. In light of the all-encompassing scope of application of the DSA, the fulfilment of this task requires, however, to oversee all communication transmitted or stored by intermediaries. And indeed, Art. 49(1)(e) in conjunction with recital 89 s. 2 mandates the EBDS to identify and analyse "emerging general trends in the development of digital services in the Union".

Such a bird's eye view on online communication in the EU presupposes enormous amounts of up-to-date information, which the Commission and the 27 national DSCs will indeed be able to gather under the DSA: Firstly, intermediaries and VLOPs in particular have to make much relevant information available to the public, namely speech restrictions applied by them (Art. 12(1) DSA), the number of their active users (Art. 23(2) and (3) DSA), the main parameters of recommender systems (Art. 29(1) DSA) and further data to be included in transparency reports (Arts. 13, 23, 33 DSA). Host providers of whatever size have to publish all blocking decisions and their respective legislative or contractual grounds in a publicly accessible database managed by the Commission (Art. 15(4) DSA). Finally, VLOPs have to compile and make publicly available a real-time repository of all commercial and non-commercial, including political, advertisements (Arts. 2(n), 30, 36 DSA). According to recital 63, these ad repositories are meant to "facilitate supervision and research into emerging risks", including "manipulative techniques and disinformation".

Secondly, competent authorities will be supplied with much additional, granular information about what is going on online. Copies of all orders to act against illegal content and to provide information are transmitted through an "information sharing system" (ISS) to the Commission, other DSCs, and the EBDS (Arts. 8(3), 9(3), 67 DSA). Intermediaries receiving such orders are obliged to inform the issuing authority of the effect given to it, specifying what action was taken at which moment in time (Arts. 8(1), 9(1) DSA). The proposal is silent as to whether these compliance reports may be channeled through the DSA ISS. It is in any event likely that problems in this context will be addressed as "emerging trends" in EBDS meetings. Finally, the parts removed from

public transparency reports of VLOPs for reasons of confidentiality, security or "harm" to recipients still have to be submitted to the competent DSC and the Commission (Art. 33(3) DSA).

Last but not least, national DSCs and the Commission may order VLOPs to provide access to, and explanations relating to, their databases and algorithms, including "data on the accuracy, functioning and testing of algorithmic systems for content moderation, recommender systems or advertising systems, or data on processes and outputs of content moderation or of internal complaint-handling systems" (Arts. 31(1), 57(1) s. 2 DSA with recital 64). The Commission expects[24] that it will conduct two such in-depth analyses for every VLOP every year.

Taken together, the DSA proposal would turn the tables on who knows what online. Whereas Big Tech nowadays possesses more information about online communication than public authorities, the latter would in the future occupy the top of the information hierarchy – across all intermediaries. Such a panoptical position creates new risks of manipulation and misuse, which the proposal does not address at all. For example, the information sharing and further correspondence between the Commission and national authorities will be kept secret (cf. Art. 63(4) DSA). EBDS meetings will take place behind closed doors. A public communicative sphere with such intense yet opaque involvement of executive authorities does not, however, deserve the trust the DSA proposal is meant to foster in the first place.

This article has originally been published on Verfassungsblog 2021/8/31, https://verfassungsblog.de/power-dsa-dma-04/, DOI: 10.17176/20210831-233126-0.

Prof. Dr. Alexander Peukert is Professor for Civil Law and Economic Law with focus on International Intellectual Property Law at the Goethe University Frankfurt.

[1] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[2] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) (2017, BGBl. I 3352), last modified 2021 (BGBl. I 1436)
[3] Bundesverfassungsgericht, Order of 11 April 2018, 1 BvR 3080/09.
[4] Bundesverfassungsgericht, Order of 22 May 2019, 1 BvQ 42/19.
[5] European Data Protection Supervisor, "Summary of the Opinion of the European Data Protection Supervisor on the Proposal for a Digital Services Act", (2021) OJ C149/3.
[6] Marc Liesching and others, "Das NetzDG in der praktischen Anwendung" (Carl Grossmann 2021).
[7] Oberlandesgericht Düsseldorf, judgement of 4 December 2020, 7 U 131/19.
[8] European Commission, "Guidance on Article 17 on Directive 2019/790 on Copyright in the Digital Single Market" (Communication), COM(2021) 288 final.

[9] Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC, (2019) OJ L130/92.
[10] ECJ Advocate General C-401/19 *Republic of Poland v European Parliament, Council of the European Union* (2021) EU:C.2021:613.
[11] Act on the Copyright Liability of Online Content Sharing Service Providers (2021, BGBl. I 1204).
[12] Giancarlo Frosio, Christophe Geiger, "Taking Fundamental Rights Seriously in the Digital Services Act's Platform Liability Regime" *SSRN* (22 March 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3747756 accessed 25 September 2021.
[13] European Commission, High Representative of the Union for Foreign Affairs and Security Policy, "Action Plan against Disinformation" (Communication), JOIN(2018) 36 final.
[14] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final, 9.
[15] European Commission, "Tackling online disinformation", https://digital-strategy.ec.europa.eu/en/policies/online-disinformation accessed 25 September 2021.
[16] European Commission, "Code of Practice on Disinformation", https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation accessed 25 September 2021.
[17] European Commission, "European Commission Guidance on Strengthening the Code of Practice on Disinformation" (Communication), COM(2021) 262 final.
[18] European Commission, "Tackling COVID-19 disinformation – Getting the facts right" (Communication), JOIN(2020) 8 final.
[19] European Commission, "First baseline reports – Fighting COVID-19 disinformation Monitoring Programme" (10 September 2020), https://digital-strategy.ec.europa.eu/en/library/first-baseline-reports-fighting-covid-19-disinformation-monitoring-programme accessed 25 September 2021.
[20] Facebook, "Facebook response to the European Commission Communication on Covid-19 Disinformation – Report for February 2021", https://ec.europa.eu/newsroom/dae/redirection/document/75741 accessed 25 September 2021.
[21] Guy Rosen, "An Update on Our Work to Keep People Informed and Limit Misinformation About COVID-19" *Facebook* (16 April 2020) https://about.fb.com/news/2020/04/covid-19-misinfo-update/ accessed 25 September 2021.
[22] Hannah Arendt, "Lying in Politics: Reflections on The Pentagon Papers" *The New York Review* (18 November 1971) https://nybooks.com/articles/1971/11/18/lying-in-politics-reflections-on-the-pentagon-pape/ accessed 25 September 2021.
[23] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final, 91.
[24] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final, Annex to the legislative financial statement, p. 9).

Using Terms and Conditions to apply Fundamental Rights to Content Moderation

Naomi Appelman • João Pedro Quintais • Ronan Fahy

Under EU law, platforms presently have no obligation to incorporate fundamental rights into their terms and conditions. The Digital Services Act seeks to change this in its draft Article 12, however, there has been severe criticism on its meagre protection. As it stands and until courts intervene, the provision is too vague and ambiguous to effectively support the application of fundamental rights.

Is Article 12 DSA a Paper Tiger?

As the European Court of Human Rights (ECtHR) has emphasised, online platforms, such as Facebook, Twitter and YouTube, provide an "unprecedented[1]" means for exercising freedom of expression online. International human rights bodies have recognised the "enormous power[2]" platforms wield over participation in the online "democratic space[3]". However, it is increasingly clear that the systems operated by platforms, where (automated[4]) content moderation decisions are taken based on a platform's terms of service, are "fundamentally broken[5]". Content moderation systems have been said to "undermine freedom of expression[6]", especially where important public interest speech ends up being suppressed, such as speech by minority and marginalised groups[7], black activist groups[8], environmental activist groups[9], and other activists[10]. Indeed, the UN Special Rapporteur on freedom of expression has criticised[11] these content moderation systems for their overly vague rules of operation, inconsistent enforcement, and an overdependence on automation, which can lead to overblocking and pre-publication censorship. This criticism is combined with, and amplified by, the notion that Big Tech exercises too much power over our online public sphere. Therefore, in order to better protect free expression online, the UN Special Rapporteur, and free speech organisations[12], have argued that platforms "should incorporate directly[13]" principles of fundamental rights law into their terms and conditions (T&Cs).

In EU law, platforms presently have no obligation to incorporate fundamental rights into their T&Cs. An important provision in the EU's proposed Digital Services Act[14] (DSA), may change this. Art. 12 DSA[15] lays down new rules on how platforms can enforce their T&Cs, including that platforms must have "due regard" to the "fundamental rights" of users under the EU Charter of Fundamental Rights[16] (Charter). The EU Council and Parliament[17] are considering the proposal in parallel, and several far reaching amendments[18] have been advanced in Parliament. Civil society is tracking

these developments closely, and there has been severe criticism on the meagre protection of fundamental rights in the DSA[19]. In this chapter, we examine Art. 12 DSA, including some of the proposed amendments. We ask whether this provision requires online platforms to apply EU fundamental rights law and to what extent it may curb the power of Big Tech over online speech. We conclude that, as it stands and until courts intervene, the provision is too vague and ambiguous to effectively support the application of fundamental rights. But there is room for improvement during the legislative process, and to avoid that Art. 12 DSA becomes a paper tiger.

The systematic context and scope of Article 12 DSA

The DSA proposal is divided into five chapters. Chapter II sets out the regime for the liability of intermediary services providers, updating and adding to the rules set out in Arts. 12 and 15 e-Commerce Directive[20].

Chapter III deals with due diligence obligations that are *independent* of the liability regime assessment of the previous chapter. These new rules, a novelty in relation to the e-Commerce Directive, distinguish between specific categories of providers. They set out asymmetric obligations that apply in a tiered way to all providers of intermediary services (Arts. 10 to 13 DSA), hosting providers (Arts. 14-15 DSA), online platforms (Arts. 16-24 DSA) and very large online platforms or "VLOPs" (Arts. 25-33 DSA). Providers of intermediary services are subject to the fewest obligations and VLOPs – covering Big Tech platforms – are subject to the most obligations. All providers are subject to Art. 12 DSA.

Art. 12 DSA is titled "*Terms and conditions*", a term that is defined in Art. 2(q) DSA as "all terms and conditions or specifications, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services and the recipients of the services." The provision aims to increase the transparency of these T&Cs and bring their enforcement in direct relation to fundamental rights.

Crucially, unlike Chapter II, Art. 12 DSA applies not only to illegal content but also to harmful content, as defined in the T&Cs of an intermediary. As such, since it applies to all providers, Art. 12 DSA extends the obligations of Chapter III beyond illegal content. Interestingly, the European Parliament's Committee on Legal Affairs (JURI), has proposed to limit the application of fundamental rights in Art. 12 DSA *only* to harmful content (see amendments 39 and 40[21]). Either way, the result is that the DSA will expand the scope of content moderation decisions subject to regulation as compared to e-Commerce Directive. Still, as we show, it remains unclear how these T&Cs relate to fundamental rights.

Art 12's DSA aims of transparency and enforcement are dealt with in two distinct paragraphs. Whereas paragraph (1) includes information obligations, paragraph (2) deals with application and enforcement and, arguably, brings providers' T&Cs within the scope of EU fundamental rights.

Article 12(1) DSA: Information Obligation

Art. 12(1) DSA[22] sets out an information obligation for providers of intermediary services regarding certain content moderation practices outlined in their T&Cs. It aims to ensure that the T&Cs are transparent and clear as to how, when and on what basis user-generated content can be restricted. The objective of the obligation appears to be acts of content moderation by providers that impose "any restriction" on users. But it is unclear whether content moderation actions by the provider that do not *stricto sensu* restrict what content their users can post, such as ranking, recommending or demonetising content, are within the scope of Art. 12 DSA.

The second sentence of paragraph (1) explicitly refers to "content moderation", a concept defined in Art. 2(p) DSA as covering activities undertaken by providers to detect, identify and address user-generated content that is either (i) "illegal content" (Art. 2(g) DSA) or (ii) incompatible with their T&Cs. Interestingly, the JURI Committee proposes to limit the scope of Art. 12(1) DSA to illegal content (amendment 38[23]), whereas the European Parliament's Committee on Internal Market and Consumer Protection (IMCO) aims to expand this provision by mandating providers to also inform users of any "significant change" made to the T&Cs (amendment 84[24]).

Further, the provision explicitly mentions "algorithmic decision-making", raising the important question of what providing information on "any policies, procedures, measures and tools" might look like[25]. However, the exact scope of the paragraph remains unclear, as the phrasing in the first sentence of "any restrictions" appears wider than the definition of content moderation in Art. 2(p) DSA, thereby broadening the provision's scope.

In its last sentence, Art. 12(1) DSA sets out *how* this information should be conveyed. Echoing Arts. 7(2), 12(1) and 14(2) GDPR[26], the T&Cs should be "clear". However, where the GDPR refers to "clear and plain" language, Art. 12(1) DSA goes one step further by requiring "unambiguous" information, which appears to result in a higher threshold obligation.

Finally, Art. 29(1) DSA sets out a somewhat similar (although less detailed) information obligation for VLOPs regarding recommender systems[27].

Article 12(2) DSA: Applying fundamental rights in content moderation?

From a fundamental rights perspective, the exciting part of Art. 12 DSA is paragraph (2), which regulates the application and enforcement of T&Cs:

> "*Providers of intermediary services shall act in a diligent, objective and proportionate manner in applying and enforcing the restrictions referred to in paragraph 1, with due regard to the rights and legitimate interests of all parties involved, including the applicable fundamental rights of the recipients of the service as enshrined in the Charter*."

The scope is the same as paragraph (1): it only applies to the enforcement of T&Cs that restrict user-generated content. The core obligation is directed at the providers to weigh the "rights and legitimate interests of all parties involved" in a "diligent, objective and proportionate" way when applying their T&Cs. Several legislative amendments expand on this obligation with requirements for application, such as that it must be timely, non-discriminatory, fair, transparent, coherent, predictable and non-arbitrary (see e.g. IMCO 85[28] and LIBE 59[29]).

As with paragraph (1), the extent of this obligation is unclear. In particular, the provision obligates intermediaries to have due regard to the "applicable" fundamental rights without clarifying what fundamental rights are already applicable in the horizontal relationship between intermediary and user. This matters, since the extent to which users can directly or even indirectly appeal to their fundamental rights vis-à-vis an intermediary in its content moderation decisions is a controversial issue[30].

In our view, Art. 12(2) DSA can be read in two ways. First, it can be understood as only referring to fundamental rights, which are already applicable in the horizontal relation between intermediaries and users. If so, the provision leaves undetermined the extent to which these are applicable and only obligates intermediaries to have "due regard" if any such rights are applicable. A second and broader interpretation is that Art. 12(2) DSA aims to declare fundamental rights directly applicable in the horizontal relation between intermediaries and users. This would certainly include the right to freedom of expression in Art. 11 Charter (e.g., for users posting content) and the right to non-discrimination in Art. 21 Charter (e.g., for users targeted by content) as well as, potentially, via Art. 52(3) Charter, the extensive case law of the ECtHR.

An obligation in line with the second interpretation would be remarkable, as it would target private actors and presumably apply with equal intensity to all intermediaries. Regrettably, the DSA offers little to no guidance on how to actualise this obligation in practice.

For example, even if what is meant by "restrictions" was properly defined, the scope of "diligent, objective and proportionate" behaviour is fuzzy. Still, promoting "diligent behaviour by providers of intermediary services" seems to be a core aim of the DSA (Recital 3). The requirement of diligence pops up at various other places in the DSA – in Arts. 14, 17, 19 and 20 DSA – primarily in the context of complaint handling by *hosting* providers. Similarly, the cloudy obligation of enforcing the T&Cs with "due regard" for fundamental rights gives no concrete insight on the extent to which these rights should be considered in individual (including algorithmic) decision-making processes by service providers.

The upshot is that users might not be able to rely on Art. 12 DSA before a court as a means to effectively protect their fundamental rights against a provider. Concretely: can an individual user appeal directly to fundamental rights based on Art. 12(2) DSA in a complaint procedure under Art. 17(3) DSA? The LIBE Committee partially

circumvents this problem by proposing a new paragraph 12(2)a that provides that "legal information" can only be excluded or limited from the providers' services when "objectively justified and on clearly defined grounds" (LIBE 60[31]).

Finally, it is unclear as how broad the scope of "all parties involved" should be understood. It explicitly includes the users affected by the restriction being applied and enforced. For online platforms, it will also presumably include trusted flaggers and other notifiers covered by Arts. 19 and 20 DSA. Beyond that it is difficult to identify other relevant parties at this stage.

Conclusion: avoiding paper tigers

On the surface, Art. 12 DSA looks like a substantial expansion of intermediaries' responsibilities and a key provision to reign in platforms' private power over online speech. It holds particular promise to constrain Big Tech's algorithmic content moderation practices. But a deeper analysis leaves more questions than answers.

Art. 12(1) DSA imposes an information obligation regarding restrictions imposed on users of intermediary services, which obligation extends to algorithmic decision-making. Art. 12(2) DSA introduces an apparently broad obligation for providers to act in a diligent, objective and proportionate manner when applying and enforcing such restrictions, explicitly linked to the respect of fundamental rights. Furthermore, the provision expands the scope of the obligations beyond illegal content, applying also to content which intermediaries consider harmful or undesirable in their T&Cs. These horizontal obligations for all providers of intermediary services providers are welcome additions to EU law.

However, Art. 12(2) DSA, in particular, is too vague on what its crucial obligation entails and the extent to which intermediaries are required to apply fundamental rights in content moderation. The amendments under discussion in the European Parliament are unlikely to offer the necessary clarity in this regard. As a result, if the legislative text remains unchanged or is significantly improved, the application and enforcement dimension of Art. 12 DSA will likely only be effective if and when courts are called to interpret it. Until then, the risk is that Art. 12 DSA remains a paper tiger, ineffectual in regulating the private power of Big Tech via-à-vis online speech.

To avoid this outcome, the EU legislator should first take a normative stand in the DSA and clarify whether the express purpose of Art. 12 DSA is to oblige providers to apply fundamental rights law in content moderation decisions. Platforms may already be going some way in this direction, as exemplified in Facebook's Oversight Board[32] decisions[33] that apply freedom of expression principles under the International Covenant on Civil and Political Rights[34]. Similarly, some national courts are applying fundamental rights to decisions taken by platforms to remove content due to their immense power over public debate online[35]. Second, the legislative process should be used to incorporate more concrete links to Art. 12 throughout the DSA, so as to substantiate

the meaning and effect of the provision. In particular, if the main concern is to constrain the private power of Big Tech, legislative intervention should focus on linking Art. 12 DSA to the due diligence obligations of VLOPs.

This article has originally been published on Verfassungsblog 2021/9/01, https://verfassungsblog.de/power-dsa-dma-06/, DOI: 10.17176/20210901-233103-0.

Naomi Appelman is a PhD Candidate at Institute for Information law at the University of Amsterdam.

João Pedro Quintais is an Assistant Professor at the Institute for Information Law at the University of Amsterdam.

Ronan Fahy is a Senior Researcher at the Institute for Information Law at the University of Amsterdam.

---

[1] ECtHR, *Cengiz and others v Turkey* 48226/10 and 14027/11 (2015).
[2] UN Human Rights Council, "Rights to freedom of peaceful assembly and of association – Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association", (2019) A/HRC/41/41.
[3] *Ibid.*
[4] Elizabeth Culliford, Katie Paul, "Facebook offers up first-ever estimate of hate speech prevalence on its platform" *Reuters* (19 November 2020) https://www.reuters.com/article/uk-facebook-content/facebook-offers-up-first-ever-estimate-of-hate-speech-prevalence-on-its-platform-idINKBN27Z2QY accessed 25 September 2021.
[5] Jillian C York, Corynne McSherry, "Content Moderation is Broken. Let Us Count the Ways." *EFF* (29 April 2019) https://www.eff.org/deeplinks/2019/04/content-moderation-broken-let-us-count-ways accessed 25 September 2021.
[6] Amnesty International, "Surveillance Giants" (2019).
[7] Dottie Lux, "Facebook's Hate Speech Policies Censor Marginalized Users" *wired* (14 August 2017) https://www.wired.com/story/facebooks-hate-speech-policies-censor-marginalized-users/ accessed 25 September 2021.
[8] Jessica Guynn, "Facebook while black: Users call it getting 'Zucked,' say talking about racism is censored as hate speech" *USA Today* (24 April 2019) https://eu.usatoday.com/story/news/2019/04/24/facebook-while-black-zucked-users-say-they-get-blocked-racism-discussion/2859593002/ accessed 25 September 2021.

[9] Justine Calma, "Facebook says it 'mistakenly' suspended hundreds of activists' accounts" *The Verge* (24 September 2020) https://www.theverge.com/2020/9/24/21454554/facebook-acitivists-suspended-accounts-coastal-gaslink-pipeline accessed 25 September 2021.
[10] Akin Olla, "Facebook is banning leftwing users like me – and it's going largely unnoticed" *The Guardian* (29 January 2021) https://www.theguardian.com/commentisfree/2021/jan/29/facebook-banned-me-because-i-am-leftwing-i-am-not-the-only-one accessed 25 September 2021.
[11] UN Human Rights Council, "Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression – Note by the Secretariat", (2018) A/HRC/38/35.
[12] Article 19, "Side-stepping rights: Regulating speech by contract" (2018) https://www.article19.org/resources/side-stepping-rights-regulating-speech-by-contract/ accessed 25 September 2021.
[13] *n 11.*
[14] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[15] *Ibid.*
[16] Charter of Fundamental Rights of the European Union, (2012) OJ C326/2.
[17] Procedure 2020/0361/COD, https://eur-lex.europa.eu/procedure/EN/2020_361 accessed 25 September 2021.
[18] Procedure 2020/0361(COD), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2020/0361(OLP) accessed 25 September 2021.
[19] Digital Services Act Observatory, https://dsa-observatory.eu accessed 25 September 2021; Article 19, "At a glance: Does the EU Digital Services Act protect freedom of expression" (11 February 2021) https://www.article19.org/resources/does-the-digital-services-act-protect-freedom-of-expression/ accessed 25 September 2021; Jan Penfrat, "All hands on deck: What the European Parliament should do about the DSA" *EDRi* (14 July 2021) https://edri.org/our-work/all-hands-on-deck-what-the-european-parliament-should-do-about-the-dsa/ accessed 25 September 2021; Electronic Frontier Foundation, "Digital Services Act Proposal: Recommendations for the EU Parliament and Council" (2021) https://www.eff.org/pages/digital-services-act-proposal-recommendations-eu-parliament-and-council accessed 25 September 2021.
[20] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ("Directive on electronic commerce"), (2000) OJ L178/1; European Parliamentary Research Service, "Reform of the EU liability regime for online intermediaries: Background on the forthcoming digital services act" (May 2020).
[21] European Parliament Committee on Legal Affairs, "Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" (22 June 2021).
[22] *n 14.*
[23] *n 21.*
[24] European Parliament Committee on the Internal Market and Consumer Protection, "Draft Report on the proposal for a regulation of the European Parliament and of the Council on Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" (28 May 2021).
[25] Maranke Wieringa, "What to account for when accounting for algorithms: a systematic literature review on algorithmic accountability" FAT* '20: Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency 1; Lilian Edwards, Michael Veale, "Slave to the algorithm? Why a 'Right to an Explanation' is probably not the remedy you are looking for" (2017) 16 Duke Law & Technology Review 18; Council of Europe, "Recommendations and declarations of the Committee of Ministers of the Council of Europe in the field of media and information society" (2016).
[26] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016) OJ L119/1.
[27] *For a discussion see here:* Natali Helberger and others, "Regulation of news recommenders in the Digital Services Act: empowering David against the Very Large Online Goliath" (2021) Internet Policy Review.
[28] *n 24.*
[29] European Parliament Committee on Civil Liberties, Justice and Home Affairs, "Draft Opinion on the proposal for a regulation of the European Parliament and of the Council on Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" (19 May 2021).

[30] Matthias C Kettemann, Anna Sophia Tiedeke, "Back up: Can users sue platforms to reinstate deleted content? (2020) Internet Policy Review; Aleksandra Kuczerawy, "Intermediary Liability and Freedom of Expression in the EU: from Concepts to Safeguards" (Intersentia 2018).
[31] *n 29*.
[32] Facebook Oversight Board, https://oversightboard.com accessed 25 September 2021.
[33] Facebook Oversight Board Decisions, https://oversightboard.com/decision/ accessed 25 September 2021.
[34] International Covenant on Civil and Political Rights, General Assembly resolution 2200A (XXI) of 16 December 1966.
[35] *See a Dutch example here:* Rechtbank Amsterdam, judgement of 9 September 2020, C/13/687385 / KG ZA 20-650 CdK/BB; Ronan Fahy and others, "Deplatforming Politicians and the Implications for Europe" *Global Digital Cultures* (12 February 2021) https://globaldigitalcultures.org/2021/02/12/de-platforming-politicians-and-the-implications-for-europe/ accessed 25 September 2021.

General and specific monitoring obligations in the Digital Services Act

Herbert Zech

The Digital Services Act contains regulation that does not directly interfere with platforms' freedom to operate but indirectly creates incentives for their handling of risk-aware behaviour, for example, towards personality right violations. Within the context of general and specific monitoring obligations in the Act, in particular, indirect regulation can encourage innovative and pragmatic decision-making, although further guardrails are necessary.

Observations regarding machine filters from a private lawyer's perspective

Platform regulation can be seen as a re-assertion of public power over private actors. Self-regulation leaves power with private actors, whereas legal regulation creates publicly defined boundaries and influences behaviour. The Digital Services Act (DSA) contains regulation that does not directly interfere with platforms' freedom to operate but indirectly creates incentives for their handling of risk-aware behaviour, for example, towards personality right violations. Within the context of general and specific monitoring obligations in the DSA, in particular, indirect regulation can encourage innovative and pragmatic decision-making, although further guardrails are necessary.

I. Platforms as a challenge for the law, liability as indirect regulation

Digital platforms mediate transactions using extensive data analysis and automated decision making. Often, one or two sides of the transaction are private parties, and quite often, for them, using the platform is free of charge – that is, they pay with data instead of money. These personal data-driven business models bring about many societal and legal challenges, not only concerning the autonomy of platform users but also regarding the protection of fundamental and civil rights of both users and third parties.

Among the areas of law concerned with regulating digital platforms are not only areas of direct regulation, but also competition law (see Podszun[1]), data privacy law or, not to forget, liability law. Indirect regulation, where feasible, provides several advantages: Foremost, it relies on decentralised decision-making, and therefore, it allows for more flexibility and demands less knowledge on the side of the legislator. Both aspects are advantageous in rapidly developing areas of society, especially where changes are technology-driven. And the digital transformation is maybe the single-most important technology-driven societal change of the present.

Liability law is a classic example of indirect regulation, creating incentives for liable parties to choose certain risk levels. However, some of the risks posed by using digital technology (and digital platforms in particular) are less clear-cut than risks for traditional interests like live and limb. This is especially true for privacy risks, addressed by data protection law, and other personality risks. Therefore, liability rules concerning the infringement on personality rights are of particular interest when it comes to regulatory efforts in the digital sphere.

A fundamental problem in this context is the intermediary status of digital platforms: They do not commit infringements in a direct manner but enable infringing acts of third parties by providing the platform infrastructure. Digital platforms, in this respect, act as intermediaries enabling infringing acts by other parties. This problem is addressed in the Directive on electronic commerce[2] and is currently part of the DSA proposal[3]. The general aim is, of course, to strike a perfect balance between the advantages of using digital platforms, especially for the freedom of expression and information, and the mitigation of the associated risks.

II. General and specific monitoring obligations and the role of automated filters

The question of how to best strike a balance between the protection of personality rights and the fundamental rights of third parties forms background of this debate. When it comes to personality rights, online platforms create a vastly enhanced risk of violation. For one, infringers can hide behind a pseudonymous or anonymous account and thus avoid legal enforcement. For another, the infringements are of a greater intensity because they can reach a very large audience. At the same time, however, digital platforms also provide a considerably enhanced space for the exercise of the freedoms of expression and information.

An important aspect of the DSA proposal is the continuation of the rules on monitoring obligations, already developed under the Directive on electronic commerce. General monitoring describes a process whereby an intermediary is obliged to introduce technological measures which monitor *all* user activity on its services. Such general monitoring obligations remain illicit according to Article 7 of the DSA proposal (which contains the same rule as Article 15 of the Directive on electronic commerce). However, the CJEU[4] differentiates between general monitoring obligations and monitoring obligations in *specific* cases, which may be ordered by national authorities. Recital 28 of the proposal now expressly upholds this distinction.

When it comes to removal obligations of platform providers, the CJEU distinguishes between three categories of unlawful content: content uploaded already, identical content uploaded in the future, and equivalent content. The obligations to remove unlawful content ("take down") and identical content ("stay down") are undisputed. Controversies arise with the category of equivalent content, which is not syntactically identical but semantically similar. Not allowing injunctions barring semantically similar, equivalent content invites circumvention. Allowing them might, in effect, lead to a quasi-

general monitoring obligation. The CJEU took the first position[5] and decided that an "injunction must be able to extend to information, the content of which, whilst essentially conveying the same message, is worded slightly differently, because of the words used or their combination, compared with the information whose content was declared to be illegal".

The reason for the CJEU to allow specific monitoring obligations in *Glawischnig-Piesczek*[6] is that the Court believes them to be practically feasible. The Court established a concept of "specific elements" which must be identified in the injunction. The order, in turn, must be "limited to information conveying a message the content of which remains essentially unchanged compared with the content which gave rise to the finding of illegality and containing the elements specified in the injunction". The key passage of the judgement, however, is about automation: The protection, according to the CJEU,

> "*is not provided by means of an excessive obligation being imposed on the host provider, in so far as the monitoring of and search for information which it requires are limited to information containing the elements specified in the injunction, and its defamatory content of an equivalent nature does not require the host provider to carry out an independent assessment, since the latter has recourse to automated search tools and technologies*".

In effect, the CJEU limits monitoring obligations to such that are feasible with the help of machine tools.

III. Automated filters and the balancing of interests

Is the insistence on automated filters good news for the balancing of personality protection and third parties' fundamental rights? When discussing this question, factual and normative problems must be discerned.

A central problem with automated filters is that they have problems with semantics. This problem is aggravated by the fact that personality right violations are largely dependent on context, unlike, for example, copyright violations where context is only relevant in special cases, like with parodies. But the debate coincides with a rapid development in artificial intelligence, which increasingly enables semantically sound decisions. Therefore, as far as it is practically possible to enclose relevant context as a specific element in the injunction order, automated filtering might be feasible in the long-term.

This leaves the second problem: The influence of machines on fundamental rights (cf. Daphne Keller, GRUR Int. 2020, 616[7]). Concerning personality protection, it seemingly makes a lot of sense that what contributed to an enlarged risk (i.e. information technology, whether online platforms or automated filters) should also be used to minimise it as much as possible. From a fundamental rights perspective, the use of automated filters would be the less restrictive measure, if the (only) alternative was to ban high-risk online platforms entirely. Platforms serve as the central forums for the exchange of views and ideas in a digital society – shutting them down can only be

considered as the ultima ratio. Still, technology cannot be the solution to all technologically-generated problems. Evgeny Morozov[8] warned against the "folly of technological solutionism". However, there is no reason against using digital technology – like any other technology – as a tool for specific legally sanctioned purposes. In fact, the point of indirect regulation is to create incentives for innovative solutions that promote legally accepted objectives.

Of course, indirect regulation does not mean the complete absence of regulation. Rather, it is about encouraging innovative and pragmatic decision-making within a clear legal framework. Where guardrails are necessary, legal rules must be introduced. Therefore, with respect to monitoring obligations, put-back claims are an important additional feature (cf. Specht-Riemenschneider, at 51-69[9]). In the area of liability for copyright infringement, such a feature (or at least something similar) has already been introduced by the German legislator. Section 18 (4) UrhDaG (Urheberrechts-Diensteanbieter-Gesetz[10], Copyright Service Provider Act, for an overview see Hofmann[11]), which entered into force on 1 August 2021, stipulates that "after an abusive blocking request with regard to works in the public domain or those whose free use is permitted by everyone, the service provider must ensure [...] that these works are not blocked again". Regarding the enforcement of put-back claims, internal platform complaint mechanisms are becoming increasingly important. Only recently, the German legislator amended the Network Enforcement Act (Netzwerkdurchsetzungsgesetz[12], NetzDG): According to section 3b NetzDG, providers of social networks must provide an effective and transparent procedure with which removal decisions can be reviewed. A similar "internal complaint-handling system" is also included in the DSA proposal (Art. 17).

Moreover, the systemic risks of machine filters must be addressed separately, as done by the proposal for very large online platforms in Article 26 of the DSA proposal. This is an (important) attempt to address another risk of digital platforms which is even more amorphous than privacy risks: autonomy risks. Systemic risks might be too important for society as a whole and too difficult being addressed by creating incentives for individuals, so that the legislator does not want to rely on indirect regulation. However, in the context of digital regulation, it is always important to consider what function the instrument of indirect regulation can fulfil.

This article has originally been published on Verfassungsblog 2021/9/02, https://verfassungsblog.de/power-dsa-dma-07/, DOI: 10.17176/20210902-113002-0.

Prof. Dr. Herbert Zech holds the Chair of Civil Law, Technology Law and IT Law at Humboldt University, Berlin, and is a Director at the Weizenbaum Institute for the Networked Society. He is interested in the regulation of new technologies with a focus on IP law and liability law.

[1] Rupprecht Podszun, „Gutachten F zum 73. Deutschen Juristentag Hamburg 2020/Bonn 2022: Empfiehlt sich eine stärkere Regulierung von Online-Plattformen und anderen Digitalunternehmen?“ (C.H.Beck 2020).
[2] Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (“Directive on electronic commerce”), (2000) OJ L178/1.
[3] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC”, COM(2020) 825 final.
[4] CJEU C-18/18 *Eva Glawischnig-Piesczek v Facebook Ireland Limited* (2019) EU:C:2019:821.
[5] *Ibid.*
[6] *Ibid.*
[7] Daphne Keller, „Facebook Filters, Fundamental Rights, and the CJEU’s Glawischnig-Piesczek Ruling“ (2020) 69 GRUR International 616.
[8] Natasha Dow Schüll, “The Folly of Technological Solutionism: an Interview with Evgeny Morozov” (9 September 2013) *Public Books* https://www.publicbooks.org/the-folly-of-technological-solutionism-an-interview-with-evgeny-morozov/ accessed 25 September 2021.
[9] Louisa Specht-Riemenschneider and others, “Grundlegung einer verbrauchergerechten Regulierung interaktionsmittelnder Plattformfunktionalitäten” (June 2020).
[10] Act on the Copyright Liability of Online Content Sharing Service Providers (2021, BGBl. I 1204).
[11] Franz Hofmann, “Das neue Urheberrechts-Diensteanbieter-Gesetz” (2021) 74 NJW 1905.
[12] Act to Improve Enforcement of the Law in Social Networks (Network Enforcement Act) (2017, BGBl. I 3352), last modified 2021 (BGBl. I 1436).

Human Ads Beyond Targeted Advertising

Catalina Goanta

If the bridling of harmful targeted advertising is a core objective of the DSA, the exclusion of influencer marketing is a grave oversight. Amendments introduced by the Internal Market and Consumer Protection Committee in the European Parliament may remedy this omission. If "human ads" were omitted, Big Tech platforms' sophisticated data-related business models will continue to escape encompassing regulation and hence, their power will remain unchecked.

Content monetization as the blind spot of the Digital Services Act

The European Union (EU) has big plans for platform governance. The new Digital Services Act[1] (DSA[2]) package, delivered in late 2020, proposes new rules on digital markets, particularly on intermediary liability, while better protecting consumers and fundamental rights online (see my writing about the DSA's general structure and relationship with the *EU Consumer Acquis* here[3]). According to the Explanatory Memorandum[4], the DSA is intended as an umbrella instrument that is supposed to tackle a wide array of issues arising on digital markets (e.g. illegal content; smart contracts). One of its central issues relates to the proliferation of online (targeted) advertising, which the European Parliament made clear[5] ought to be one of the areas of reform, so to create less dependence on and exploitation of algorithms toward consumers and citizens.

Tackling the harms associated with online profiling and creating more transparency on data brokerage markets is a solid, necessary policy objective. Indeed, much of Big Tech platforms' power, market dominance and other market actors' dependence derives from their monetization of user data for the advertising purposes. Yet in the past five years, the section of the advertising industry targeted by the DSA has slowly but steadily been complemented by a new form of advertising, now ubiquitous on social media. In a nutshell, it reflects a fascinating and complex new iteration of the gig-economy: any Internet user can monetize their online presence by sharing multimedia content, and platforms intermediate demand, supply and sometimes payments. Many types of specific business models have lent their name to the description of this new form of advertising, such as 'influencer' or 'affiliate marketing'.

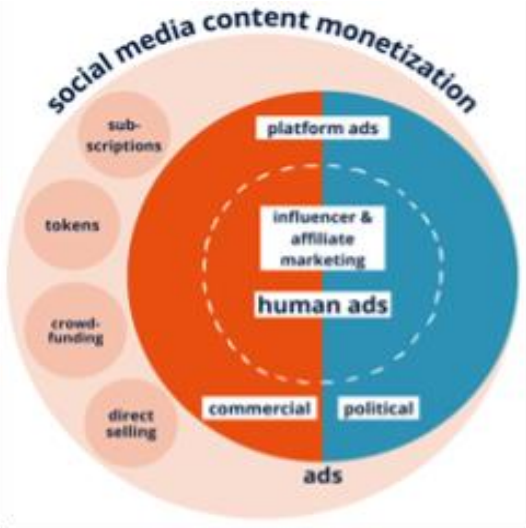

Figure 1 – Content monetization and business models (based on Goanta & Ranchordas[6]; De Gregorio & Goanta[7])

If the bridling of harmful targeted advertising is a core objective of the DSA, the exclusion of influencer marketing is a grave oversight. Amendments introduced by the Internal Market and Consumer Protection Committee in the European Parliament may remedy this omission, but long-term, the goal must be 'content as compliance', in line with European consumer protection standards. Otherwise, Big Tech platforms' sophisticated data-related business models will continue to escape encompassing regulation and hence, their power will remain unchecked.

From platform ads to human ads

When we think about digital advertising, we imagine brands around the world paying digital platforms for ad space, where they compete for user attention and engagement – an industry that can be referred to as *platform ads*. Brands register their ads in databases called 'ad archives'[8] from where they can target selected platform demographics. The best example is Facebook's Ad Library[9], where anyone can check the ads registered by Facebook to be displayed on their platforms, as an attempt by Facebook to create more transparency regarding its targeted advertising, especially after public incidents (e.g. Cambridge Analytica) emphasized the opacity of its infrastructure. An ad's occurrence on a timeline will always be marked as 'Sponsored' by Facebook.

In the past decade, however, digital advertising has been generating new business models, focused on the monetization of original and authentic content, particularly on social media. Based on an increase in social media consumption, content monetization makes it profitable for Internet users to not only engage with advertising, but to *become* advertising.

As Google puts it[10], "advertising is becoming, well, less like advertising", as the Internet has taken this industry into the "age of authenticity", wherein resources are shifted from platform to 'human ads'. Human ads are influencers, also called content creators, who earn revenue from social media advertising by creating authentic, relatable content for their followers. In turn, they receive money, goods or services (influencer marketing), or sales commissions (affiliate marketing). By hiring humans as ad banners,

marketers and brands offer information (e.g. reviews) and explore persuasive narratives (e.g. social causes), which audiences can relate to and engage with. The popularity of such advertising approaches is undeniable. In 2021, influencer marketing is projected to reach a global market size of $13.8 billion (700% increase since 2016)[11]. However, the business of influence is also rapidly changing, with a plethora of new stakeholders emerging in the content monetization supply chain. Examples include influencer data analytics companies (e.g. Heepsy[12]) and ambassador management platforms (e.g. Fohr[13]), who are new categories of advertising intermediaries on digital markets, connecting brands and creators. The popularity of these new forms of digital marketing is matched by its potential risks.

The pursuit of monetization, combined with market trends towards inconspicuous "authentic" advertising, have revived a long-standing media and consumer law struggle: the misleading or deception of consumers with hidden commercials. Such undisclosed product placement or native advertising is prohibited in the European Union (e.g. via the Unfair Commercial Practices Directive[14]), and reflect decades of regulatory reforms focused on protecting consumers from subliminal manipulation. The rationale behind this prohibition is that the law draws a line between mere commercial puffs used to make advertising more appealing and the deception of consumers. Other harms relating to human ads are beginning to emerge in the realm of political advertising[15]. Commercial and political ads look the same, are posted by the same individuals, are displayed in the same digital space, to the same audiences, and raise the same transparency issues.

Human ads as the new prosumers

As highlighted above, content monetization through advertising is a new iteration of the gig economy, whereby content is shared, instead of cars or apartments. From a legal perspective, to say they are hard to define is an understatement. Earlier iterations of the gig economy have left us with a considerable definitional debt: the inability to redefine and enforce new forms of legal personhood to reflect the granularity of transactions taking place on digital markets. Is a seller of seven items on a peer-to-peer online market a trader in the meaning of EU consumer protection? In *Kamenova*[16], the Court of Justice of the European Union answered this question negatively, but asking courts to undertake individual tests for even 1% of all market participants is simply an impossible feat. We could argue content creators are the new prosumers[17], namely they are not consumers (or generally peers), but they also do not possess the bargaining power of other traders, such as platforms. To the contrary, they may sometimes become victims of platform discretion and power themselves, as I explored in this piece[18]. This status has not gotten any statutory clarification, and therefore does not improve legal uncertainty. But why is it so important to define human ads or content creators? Clarifications in this direction can be relevant for business, tax and social security purposes, and especially to determine whether consumer protection is applicable.

While advertising through content creation is an industry that finds itself in full bloom, the way in which regulators and public authorities have tackled it so far has been

ineffective for at least two reasons. First, advertising rules are a combination of (*inter alia*) mandatory European and national media law, consumer law (including unfair competition) and self-regulation, such as the Social Code for Youtubers[19] set up in collaboration with the Dutch Media Authority. The enforcement landscape thus raises tensions relating to competence and sanctions. Second, the number of content creators and their supply chains are too vast to be handled systematically without more legal certainty and some automation. This is why the DSA is so central, as it complements the focus on the individual creator with platform responsibilities.

Advertising and the DSA

The DSA reflects the issue of advertising in its draft Art. 24, mandating transparency in advertising displayed by platforms – the traditional ad archives, discussed above. However, the proposal makes no acknowledgement whatsoever of new advertising business models emerging from content monetization. Moreover, the scarce and inconsistent references to influencer marketing in research contracted by the Commission for earlier regulatory fitness checks[20] show a considerable research gap affecting the European regulator in this policy area. In terms of political advertising, the Commission will propose new transparency measures[21] in the third quarter of 2021, to further the goals of the European Democracy Action Plan and harmonize rules on political advertising beyond soft law initiatives such as the EU Code of Practice on Disinformation[22].

The IMCO Report

Of course, the DSA proposal is only the beginning of what is expected to be a lengthy and by no means dull legislative procedure. The Report of the Committee on the Internal Market and Consumer Protection (IMCO Report[23]) already brings some much-needed amendments to the Commission's draft DSA. The draft wording of Art. 24 DSA on online advertising transparency focuses on the role of platforms in advertising transactions to which they are a party. However, human ads are popular vehicles of advertising which fall outside of this paradigm, as platforms are not part of their advertising transactions, but do contribute to the dissemination of ad content through their architecture. The IMCO report highlights this absence, and proposes three amendments to the DSA draft:

1. recital 39d, which acknowledges 'digital influencers' and explains that platforms should make sure remunerated content is 'clearly identifiable', and that contractual relationships relevant to the content ought to be disclosed;
2. Art. 2(1), which adds the distinction between 'direct' and 'indirect' promotion of a message under the definition of 'advertising';
3. Art. 13c, on online advertising transparency, proposes a number of transparency duties which are supposed to harmonize the marking of ads and facilitate the monitoring of how platforms comply with such transparency duties.

These amendments improve the DSA draft from the perspective of consumer protection, since they acknowledge and include influencer marketing within advertising

transparency. In this policy area, compliance translates into disclosure duties placed on platforms by the DSA. For instance, platforms could use their verification mechanisms (e.g. the blue check mark) to signal content creators' accounts and propose affordances (e.g. the 'paid partnership with' label on Instagram) which such accounts should use. This would not only benefit users, but also public authorities and researchers who can better monitor the landscape of native advertising on social media, especially with the rise of social commerce[24].

Do the IMCO amendments solve all the problems of native advertising models, such as influencer marketing? Certainly not. Until we systematically clarify how to define the economic activity of influencers, respective articles will most likely lead to diverging interpretations. Potential definitions may take inspiration from labour standards, as a group of researchers on the creator economy has highlighted in a comment submitted to the UK Parliament[25] call for evidence on the influencer economy (which also has a broad literature list on the content creator economy). In addition, the justification behind Art. 13c DSA shows the focus on "commercial influencer content". But what about political ads for which influencers are hired? What should we focus on in determining the applicable rules? On the nature of the transaction, which leads to a commercial engagement? Or on the (political) nature of speech, which leads to more protection and less transparency owed to the same audiences who engage with the commercial communications of their favourite influencers?

Some reflections

These questions still need to be addressed. To provide clarity, we need to move away from the paradigm of 'content as speech' on social media, and into the era of 'content as compliance'. Such a direction is, I would argue, supported by the IMCO amendments. One of the most important shifts which the DSA may very well bring is the tendency of the Commission to 'fight fire with fire', as my colleague Thibault Schrepel[26] puts it. In other words, digital markets that generated sophisticated data-related business models and industries need to be monitored at scale, using that very same data for forensic investigation perspectives (some reflections on digital monitoring and dark patterns are available here[27]). The DSA already proposes such investigations elsewhere (e.g. Art. 46 DSA). Legal compliance will therefore suffer from what currently seems to be an insurmountable tension of 1) aligning legal standards from a plethora of different fields that govern online content (e.g. fundamental rights, electoral law, consumer protection, criminal law); and 2) interpreting applicable standards in such a way that monitoring legal compliance at scale is not an impossible task. With these realizations in mind, it might help to see the DSA as a more modest initiative: a procedural bridge between different fields of European and national law, whose success depends on further sectoral harmonization and alignment.

This article has originally been published on Verfassungsblog 2021/9/05, https://verfassungsblog.de/power-dsa-dma-11/, DOI: 10.17176/20210905-213932-0.

Catalina Goanta is an Assistant Professor at Maastricht University. Her multidisciplinary research focuses on platform governance, content monetization and decentralization, and brings together methods from law and computer science.

[1] European Commission, "The Digital Services Act package" https://digital-strategy.ec.europa.eu/en/policies/digital-services-act-package accessed 25 September 2021.
[2] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[3] Caroline Cauffman, Catalina Goanta, "A New Order: The Digital Services Act and Consumer Protection" (2021) European Journal of Risk Regulation (FirstView).
[4] *n 2*.
[5] European Parliament Press room, "Digital: The EU must set the standards for regulating online platforms, say MEPs" (20 October 2020) https://www.europarl.europa.eu/news/en/press-room/20201016IPR89543/digital-eu-must-set-the-standards-for-regulating-online-platforms-say-meps accessed 25 September 2021.
[6] Catalina Goanta, Sofia Ranchordas, "The Regulation of Social Media Influencers: An Introduction" (2019) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3457197 accessed 25 September 2021.
[7] Giovanni De Gregorio, Catalina Goanta, "The Influencer Republic: Monetizing Political Speech on Social Media" (2021) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3725188 accessed 25 September 2021.
[8] Paddy Leerssen and others, "Platform Ad Archives: Promises and Pitfalls" (2019) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3380409 accessed 25 September 2021.
[9] Facebook Ad Library, https://www.facebook.com/ads/library/?active_status=all&ad_type=political_and_issue_ads&country=NL&media_type=all accessed 25 September 2021.
[10] Celie O'Neil-Hart, Howard Blumenstein, "Why YouTube stars are more influential than traditional celebrities" (July 2016) *Think with Google* https://www.thinkwithgoogle.com/marketing-strategies/video/youtube-stars-influence/ accessed 25 September 2021.
[11] Statista "Influencer marketing market size worldwide from 2016 to 2021" (2021) https://www.statista.com/statistics/1092819/global-influencer-market-size/ accessed 25 September 2021.
[12] Heepsy, https://www.heepsy.com accessed 25 September 2021.
[13] Fohr, https://www.fohr.co 25 September 2021.
[14] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive'), (2005) OJ L149/22.
[15] *n 7*.
[16] ECJ C-105/17 *Komisia za zashtita na potrebitelite v Evelina Kamenova* (2018) EU:C:2018:808.
[17] Chris Marsden, "Prosumer Law and Network Platform Regulation: The Long View Towards Creating OffData" (2018) 2 Georgetown Law Technology Review 376.
[18] Catalina Goanta, Jerry Spanakis, "Influencers and Social Media Recommender Systems: Unfair Commercial Practices in EU and US Law" (March 25,2020) *SLS Working Paper* https://law.stanford.edu/publications/no-54-influencers-and-social-media-recommender-systems-unfair-commercial-practices-in-eu-and-us-law/ accessed 25 September 2021.
[19] Social Code: YouTube, https://www.desocialcode.nl accessed 25 September 2021.
[20] GfK Consortium, "Behavioural Study on Advertising and Marketing Practices in Online Social Media" (June 2018).
[21] European Commission Have your say: Political advertising – improving transparency, https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12826-Transparency-of-political-advertising_en accessed 25 September 2021.

[22] European Commission, "Code of Practice on Disinformation", https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation accessed 25 September 2021.
[23] European Parliament Committee on the Internal Market and Consumer Protection, "Draft Report on the proposal for a regulation of the European Parliament and of the Council on Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC" (28 May 2021).
[24] Christine Riefa, "Consumer Protection on Social Media Platforms: Tackling the Challenges of Social Commerce" (2019) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3373704 accessed 25 September 2021.
[25] See https://docs.google.com/document/d/1avkyL4YUZYIgXycFBNZSaIsaYY_ZHnwgJkpMWM-iS_4/edit accessed 25 August 2021.
[26] ICLE, "Thibault Schrepel on Computational Antitrust" (11 February 2021) https://lawecon-center.org/thibault-schrepel-on-computational-antitrust/ accessed 25 September 2021.
[27] Constanta Rosca and others, "Digital monitoring of unlawful dark patterns" in Position paper at the Workshop "What Can CHI Do About Dark Patterns?" at the CHI Conference on Human Factors in Computing Systems (CHI '21) (2021).

Re-Subjecting State-Like Actors to the State

Hannah Ruschemeier

The Digital Services Act aims to limit the power of the Big Tech companies and to place more responsibility on them to control the content which is posted on their websites. Rather than providing even more power to the platforms via de facto self-regulation, the DSA should strengthen the interference opportunities of public authorities.

Potential for improvement in the Digital Services Act

From the quasi-monopolistic power of platform companies, several side effects are evolving into serious problems. To name only a handful: While Facebook and Twitter have been troubled by Fake News, attempts at electoral fraud, and radicalisation for a couple of years now, Instagram and TikTok, popular especially among people under 25, have also been criticised for censorship and insufficient child protection measures.

Taken together, these services have a persistent, significant influence on society, and their associated problems do not seem to solve themselves. Meanwhile, especially in respect to the moderation of the above content, critics claim that Facebook is acting like a state[1], without being held responsible for its actions. Usually, decisions over speech are made by courts and not by private actors. Likewise, public governments are primarily responsible for ensuring democratic rules and the possibility to exercise fundamental rights, such as the freedom of expression, within a democratically legitimized legal framework.

Following this, the Digital Services Act (DSA)[2] aims to limit the power of the large platform companies and to place more responsibility on them to control the content which is posted on their websites. In theory, the DSA is following the right approach, but the proposal has been shying away from imposing concrete legal obligations on the platforms when it comes to systemic risks. The focus on the broadly phrased and abstract systemic risks could dilute the focus on specific tasks to fight the mentioned problems. Instead, the DSA should strengthen the interference opportunities of public authorities rather than providing even more power to the platforms via de facto self-regulation.

Concentration of Power

The similarities between the platforms and the state end with the one thing they have in common: a certain concentration of power. This concentration of power does not correspond to a monopoly of force on the side of the platforms, and it should not. Otherwise, a *direct* binding effect of fundamental rights would most likely not solve the problems associated with the platforms. Instead, it would legitimate the platforms in an undesirable way.

The situation of the platforms is not directly comparable to the 'situational state-like binding of fundamental rights'[3], established in the Stadionverbot[4] decision of the Federal Constitutional Court. Above all, the power of the platforms has resulted from the systemic digital environment they created with millions of users. This is not situational but universal. Yet, the relationship between platforms and their users is more similar to the citizen-state relationship than that between two private actors, even considering costumer protection rules and other situations of disparity. Hence, the platforms are neither comparable to the state nor merely a powerful private actor who is exploiting a structural (dis)advantage, but something in-between, due to their systemic power and influence. Therefore, solving the problems of the digital platform-sphere is a task for public law[5].

For now, the public authorities must be strengthened to effectively regulate the digital sphere, not be replaced by private companies. This leads to the question which concrete instruments – whether self-regulation, public-regulation, breaking up Big Tech companies, etcetera – are effective and feasible.

Regulating Big Tech Players

The current legal framework, the e-Commerce Directive[6], does not regulate these issues. Yet recently, the Big Tech companies' business model is under fire: In the European Union and the United States, political initiatives are pushing for more regulation, the (postponed) discussion about a global digital tax reform[7] is just one example. The DSA[8] and the Digital Markets Act (DMA)[9] are following this strategy. Certainly, the idea of the DSA and the DMA is to establish responsibility of platforms for the content of their users.

Ensuring responsibility in the digital sphere is one of the biggest challenges for law in the era of digitalisation. Foremost, platforms' concentration of power undermines the rule of law. For one, the law loses its effectiveness if it can be circumvented, ignored or if it is not implemented or enforced by public authorities.

Here, platforms are criticised for acting 'state-like': they create their own 'law' via their terms of service, in an attempt to avoid legal regulation. As far as possible, large, globally-positioned IT companies are interested in operating with uniform structures that have a global or transnational reach. Regulations that are set down in various legal systems and hence differ from one another constitute an impediment to such business models. For this reason, platforms seek out and exploit opportunities to avoid such regulations. Additionally, their influence on democratic procedures such as voting seems to be substantial. But Facebook is not a state[10] within the state above the rule of law. For another, requiring only platforms to monitor user posts does not only burden the companies[11], but it also endangers the rights to data protection, privacy, and the freedom of expression, leading to rising concerns about effective remedy and even censorship. Nevertheless, the main state-like Big Tech actors must take a degree of responsibility, even if mandated by law.

Legal Implications for Very Large Online Platforms

The DSA proposal aims to target 'very large online platforms' with specific obligations because they are 'where the most serious risks' for fundamental rights occur, and have the capacity to absorb this additional burden (p. 11; section 4). Additional obligations are laid down in Art. 4 DSA proposal for those platforms which provide their services to a number of average monthly active users in the European Union equal to or higher than 45 million (Art. 25 (1) DSA). This category is most interesting regarding systemic risks for democracy and fundamental rights.

Risk assessment for fundamental rights

Therefore, these platforms shall perform a risk assessment at least once a year, identifying any significant systemic risks stemming from the functioning and use of their services in the Union (Art. 26 DSA), especially with regard to illegal content, negative effects for the fundamental rights of privacy, family life, freedom of expression and information, the prohibition of discrimination, the rights of the child, as well as intentional manipulation. The latter intends to avoid negative effects on public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security. Unquestionably, these obligations explicitly aim to conquer the systemic risks arising from the concentration of power of the mentioned online platforms. The risk assessment and the accompanying mitigation of risks in Art. 27 DSA evoke the state protection obligation of fundamental rights – including the same level of uncertainty if concrete duties or claims could emerge from these obligations. First, the online platforms shall implement reasonable, proportionate, and effective mitigation measures, which may include adapting content moderation, reinforcing the internal processes or supervision or initiating cooperation with other online platforms through the code of conduct (Arts. 27 (1) b), 35 DSA). These obligations only address internal actions chosen by the platforms themselves – the specific nature and scope is up to them. At the same time, the platforms are now responsible for the systemic risks, which empowers them to regulate these risks on their terms – this has been the classic responsibility of public authorities. Theoretically, the requirements can be substantiated by the Commission in cooperation with the Digital Services Coordinators (DSCs), discussed in greater detail below, via general guidelines. This kind of soft law, like the recommendations of the EDPD has become quite important in practice, but it all depends on the quality of the best practice recommendations. Whether the general guidelines for best practices of the Commission and the decisions of the national regulatory bodies or questions of liability[12] will be able to rectify this into a uniform application of the DSA remains unclear at this point.

Consequently, the broad obligations of the platforms to conquer systemic risks give them more power to control themselves and seem to only marginally extend opportunities for external intervention – meaning by public authorities.

Moreover, the important differences between the state protection of fundamental rights and the risk assessment of the platforms are within the execution of these

obligations. Very large online platforms shall be subject to audits to assess compliance with the DSA. These audits ought to be performed by independent organisations with proven expertise and professional ethics, which is very vague. As a result, member states' public authorities are not necessarily involved in the direct oversight of very large platforms.

Especially in this situation, where the platforms are well known for avoiding legal regulation, the self-regulatory approach is not enough when it comes to the protection of fundamental rights and the legal interests the Commission is describing as endangered in the DSA. Following this, the DSA should provide concrete actions for the platforms to take in addition to the abstract goals of preventing systemic risks. For example, the compliance officer in Art. 32 DSA is not sufficient to replace the requirement of hiring of enough staff to moderate illegal content.

Transparency

Further worth mentioning is the transparency requirement laid down in Art. 29 DSA; platforms shall set out in their terms and conditions the main parameters used in their recommender systems in a clear, accessible, and easily comprehensible manner. Additionally, Art. 30 DSA requires the platforms to make information about online advertisement publicly available until one year after the ad was displayed for the last time. These kinds of obligations are known from the GDPR (e.g. the right to information in Arts. 13, 14 GDPR). But transparency alone does not put the users in control over the content which is prioritised solely by the platform's own algorithms. This should have been a lesson learnt from the GDPR.

Execution

As a result, the broadly defined requirements of Art. 27 DSA seem to, in fact, be a framework for the self-regulation of the companies in scope. Consequently, this could lead to insufficient regulation or overregulation. Either the risk obligations are too vague to require actions which are not already covered by internal compliance rules, or platforms are likely to aim at reducing their exposure to penalties by deleting content, which is legal, but associated with systemic risk-potential. It remains unclear whether these risks can be mitigated by the audit and the required implementational report in Art. 28 DSA, or the transparency requirements of Art. 29 DSA. Evidently, the efficiency of the DSA is inseparable from the oversight of and execution by the designated authorities.

In comparison, the subsequent data access right in Art. 31 DSA enables public authorities to request data from the platforms via the DSC, for example to the benefit of vetted researchers, for the purpose of conducting research about the systemic risks. The DSC is an innovation of the DSA to ensure the administrative execution of the regulation, following the 'country of origin principle' (Chapter IV DSA). In this situation, the DSCs must be independent from any other public authority or any private party, comparable with the federal and state data protection officers. The DSCs' powers are laid down in Arts. 41, 42 DSA, including information, investigation, and infringement rights, among

them, for example, the power to impose penalties of up to 6% of the annual income of the platform provider, further specified in rules by the member states (Art. 42 DSA), or options for enhanced supervision (Art. 50 DSA). Correspondingly, the DSA wants to establish the cooperation with the very large online platforms via soft law, like codes of conduct (Arts. 35-36 DSA). In effect, the DSA weaves an intricate web of responsibilities and oversight measures. The latter centrally rely on Art. 31 DSA, which establishes a new obligation to provide the DSCs or the Commission with the data that are necessary to monitor and assess compliance with the regulation. The platform must answer the request within 15 days (Art. 31 (6) DSA). This is an important and concrete information right, which enables the DSC or the Commission to take actions.

At first glance, therefore, it seems that the member states could play an influential role, enforcing the DSA via the DSCs. Obviously, the opportunity to impose penalties as laid down in Art. 42 DSA is a potent competence, but as the GDPR has shown, high fines alone do not ensure effective execution. The concept of the DSC has the potential to become a powerful, but likely controversial authority. For example, the GDPR's data protection officers are quite disputed: some say they are blocking innovation, others claim that they have not taken enough action against the large platforms. In practice, it will be crucial whether the DSCs are able to establish a structure with sufficient personnel and financial resources.

The Commission has the final say…

Nevertheless, the Commission has the final say and can initiate own proceedings if the DSC did not take any investigatory or enforcement measures pursuant to the request of the Commission (Art. 51 DSA). In fact, the DSA allows the Commission to take on potentially very broad enforcement measures, including requesting the DSC to go to court (Art. 65 DSA). The European Board of Digital Services appears similar to the EDPB (see Art. 68 GDPR). The 'Board' shall advise the DSCs and the Commission to achieve consistent application of the regulation within the Union. Still, the decentralised principle has not always been very successful in Data Protection Law. Similarly, an uncoordinated 'side-by side' of different supervisory authorities should be prevented.

What's next?

All in all, the Commission promotes the DSA with its advantages for citizens, businesses, and providers as well as for the society at large. It promises greater democratic control and oversight over systemic platforms as well as the mitigation of systemic risks, such as manipulation or disinformation, and emphasises the protection of fundamental rights, especially the freedom of speech.

On the one hand, the DSA/DMA package has the potential to shake up the digital economy, especially when sector-specific rules including individual rights of affected persons follow. On the other hand, member states' public authorities play a rather subordinate rule in the proposal (for a critical analysis, see here[13]). The vague wording of the systemic risks could lead to *de facto* self-regulation and increasing responsibilities of

the platforms, which was the goal, but this leads to the strange situation that the DSA, which was drafted to limit the influence of the platforms, actually further empowers them. In addition, the DSCs are challenged with defining their role next to the Commission. All in all, however, the DSA/DMA package is pointing in the right direction of a digital future-proof Europe.

This article has originally been published on Verfassungsblog 2021/9/06, https://verfassungsblog.de/power-dsa-dma-13/, DOI: 10.17176/20210906-214352-0.

Dr. Hannah Ruschemeier is a postdoctoral researcher at the ELSI (ethical, legal, and social issues) unit at CAIS NRW and the Chair of Public Administration, Public Law, Administrative Law and European Law at the University of Administrative Sciences Speyer

[1] Washington Post Editorial Board, „Opinion: Facebook is looking a lot like a government“ (23 February 2020) *The Washington Post* https://www.washingtonpost.com/opinions/facebook-is-looking-a-lot-like-a-government/2020/02/23/2977a204-53f1-11ea-929a-64efa7482a77_story.html accessed 25 September 2021.
[2] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC”, COM(2020) 825 final.
[3] Fabian Michl, “Situativ staatsgleiche Grundrechtsbindung privater Akteure” (2018) 73 JZ 910.
[4] Bundesverfassungsgericht, Order of 11 April 2018, 1 BvR 3080/09.
[5] Frederik Ferreau, “Eine Kommunikationsordnung für Soziale Netzwerke” (4 August 2021) *Verfassungsblog* https://verfassungsblog.de/bgh-drittwirkung-fb/ accessed 25 September 2021.
[6] 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 Mar-ket (“Directive on electronic commerce”), (2000) OJ L178/1.
[7] Jakob Hanke Vela, “EU to postpone digital tax proposal” (12 July 2021) *Politico* https://www.politico.eu/article/eu-to-postpone-digital-tax-proposal/ accessed 25 September 2021.
[8] European Commission, “Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC”, COM(2020) 825 final.
[9] European 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)”, COM(2020) 842 final.
[10] Constantin van Lijnden, “Facebook, geben Sie Redefreihei!” (6 September 2018) *Frankfurter Allgemeine Zeitung* https://www.faz.net/aktuell/feuilleton/medien/facebook-darf-nicht-eigenhaendig-beitraege-loeschen-15773244.html accessed 25 September 2021.
[11] ECJ C-360/10 *Belgische Vereniging van Auteurs, Componisten en Uitgevers CVBA (SABAM) v Netlog NV* (2012) EU:C:2012:85.
[12] Aleksandra Kuczerawy, “The Good Samaritan that wasn’t: voluntary monitoring under the (draft) Digital Services Act” (12 January 2021) *Verfassungsblog* https://verfassungsblog.de/good-samaritan-dsa/ accessed 25 September 2021.
[13] Quirin Weinzierl, “Institutionalizing Parallel Governance” (18 December 2020) *Verfassungsblog* https://verfassungsblog.de/institutionalizing-parallel-governance/ accessed 25 September 2021.

Platform research access in Article 31 of the Digital Services Act

Paddy Leerssen

Over the past year, dominant platforms such as Facebook have repeatedly interfered with independent research projects, prompting calls for reform. Platforms are shaping up as gatekeepers not only of online content and commerce, but of research into these phenomena. As self-regulation flounders, researchers are hopeful for Article 31 of the proposed Digital Services Act, on "Data Access and Scrutiny" - a highly ambitious tool to compel access to certain data, but researchers also need a shield to protect them against interference with their independent projects.

Sword without a shield?

The issue of research access is becoming ever more urgent in platform governance. Over the past year, dominant platforms such as Facebook have repeatedly interfered with independent research projects, prompting calls for reform. The matter went mainstream in October 2020, when, only weeks before the US elections, Facebook tried to shut down an independent audit of their political advertising by NYU[1]. Last month, they tightened the screws even further by suspending the researchers' Facebook accounts[2], stripping them of access to the Ad Library API and Crowdtangle research tools. And closer to home, Facebook also retaliated against data collection by the Berlin-based NGO AlgorithmWatch, sending them "thinly veiled threats" of legal action[3] on the grounds that independent data collection violated the platform's Terms of Service. Platforms are shaping up as gatekeepers not only of online content and commerce, but of research into these phenomena.

As self-regulation flounders, researchers are increasingly looking to government to secure platform research access. In particular, their sights are set on Article 31 of the proposed Digital Services Act (DSA), on "Data Access and Scrutiny". A highly ambitious plan, it is to my knowledge the first legislative framework for researcher access to platform data.

What does Article 31 DSA do, and how does it constrain gatekeeper power over public interest research, and how will it help the likes of AlgorithmWatch and NYU? There are some important limitations in the current draft, and it won't actually resolve the scraping disputes we've seen over the past year. Researchers will welcome Article DSA 31 as a tool to compel access to certain data, but they also need a shield to protect them against interference with their independent projects.

Article 31 DSA in short

In short, Article 31 DSA creates a procedure for the European Commission and national authorities ('Digital Service Coordinators') to compel confidential access to platform data.

Under this framework, regulators can order access for their own monitoring and enforcement purposes (Paragraph 1) or for use by third-party researchers (Paragraph 2). Access is limited to so-called "vetted researchers", subject to various conditions such as a university affiliation, independence from commercial interests, and compliance with confidentiality and security requirements (Paragraph 4). Another important limitation is that researchers may only use this data for purposes of research into "systemic risks" as defined in Article 26 DSA. Platforms may object to data access requests in cases where they do not have the data, or access would pose "significant vulnerabilities" to security or "protection of confidential information, in particular trade secrets". This regime applies only to Very Large Online Platforms (VLOPs) with more than 45 million average monthly active recipients in the EU (Article 25(1) DSA).

All this is covered in one rather brief provision. Many technical and procedural details are left for the Commission to sort out in delegated acts (Paragraph 4), including compliance with the GDPR, and the protection of platform security and trade secrets.

There is much to like here for researchers, who have been pushing for this kind of confidential access frameworks for a while now. Still, the current draft leaves many loopholes and uncertainties that could undermine its impact in practice. And it does little to address the contractual powers that platforms wield over researchers through their Terms of Service.

Research topics: 'systemic risks' only

Article 31 DSA only applies to research related to "systemic risks" per Article 26 DSA. Admittedly this category is broad and open-ended, including catch-all concepts such as the as fundamental rights to privacy, freedom of expression and information alongside more specific issues such as "dissemination of illegal content" and "intentional manipulation of the service".

One wonders why the legislator did not opt for a more neutral, open-ended purpose such as scientific or public interest research. The present approach seems to treat research access solely as a means to enable better enforcement of the DSA. But scientific interest in platform data is by no means limited to these types of regulatory concerns. Thankfully, the concept of "systemic risks" is so broad that many researchers will still manage to fit the bill, but ideally such box-ticking exercises would not be necessary.

Research actors: academics only

Article 31 DSA only benefits "vetted researchers", defined as follows in paragraph 4:

> "*In order to be vetted, researchers shall be affiliated with academic institutions, be independent from commercial interests, have proven records of expertise in the fields related to the risks investigated or related research methodologies, and shall commit and be in a capacity to preserve the specific data security and confidentiality requirements corresponding to each request*."

There is much to unpack here, but the most important point is that access is limited to university-affiliated academics. This approach has the downside of ruling out usage by other valuable watchdogs in platform governance, such as journalists and NGOs (unless they partner with academics, of course). Critics including AlgorithmWatch[4] have already called for the university affiliation rule to be dropped. Mathias Vermeulen proposes[5] an amendment from academic to scientific researchers. Comparative research by Jef Ausloos, Pim ten Thije and I[6] has also shown that data access frameworks in other industries such as public health have made do with actor-neutral approaches, focused on scientific research *purposes* rather than actors.

But an academics-only approach also has an important upside: academics are relatively straightforward to accredit via the university system, whereas journalists and NGOs are more amorphous categories more open to abuse. The Commission will likely have less trouble deciding who qualifies as an academic, than as a journalist or NGO. Consider also how attractive Article 31 DSA might be for commercial parties, such as IP lobbyists collecting ammunition in their war against platforms, or professional advertising or financial analysts. Without proper safeguards, there is a real risk of such commercial usage crowding out public interest applications, as has already happened in other areas of transparency regulation such as US public records laws[7]. The DSA already requires researchers to be independent from commercial interests, but this test is relatively difficult to enforce in practice, especially as regards NGOs. Limiting access to universities throws up an additional barrier against co-optation by private interests.

In my view, the correct answer here depends on other aspects of Article 31 DSA that are still unclear. As I'll discuss below, important procedural aspects still need to be decided on, such as whether Article 31 DSA will produce automated and scalable solutions or instead will take a slower, smaller-scale approach focused on bespoke data grants. If barriers to access are low, and application times are short, the Article 31 DSA framework will be more attractive to non-academic watchdogs, while also being less sensitive to overcrowding from their additional usage. But if Article 31 DSA remains smaller in scale, it makes more sense to prioritize university researchers.

At this stage, my main criticism of the "vetted researchers" category is that it is too detailed and inflexible. Precisely because so much else about Article 31 DSA still needs

to be worked out in delegated decision-making, this definition is uncharacteristically, unhelpfully specific. Once the dust settles, requirements such as university affiliation and a 'proven track record' may well prove overly restrictive, or too administratively cumbersome. Why legislate on these choices now?

Will it scale? Bespoke grants versus programmatic access

Important procedural aspects of Article 31 DSA remain unclear. At present, there is no way for researchers to apply for access, and the initiative instead relies entirely on regulators to request data on their behalf. How responsive will regulators be to researcher demands? Ideally, researchers and academic institutions will be closely involved in setting the data access agenda. But in the current draft, government calls all the shots. Combined with the topical restriction to 'systemic risks', one gets the impression that the Commission sees Article 31 DSA primarily as a means to outsource regulatory monitoring burdens to universities, rather than supporting independent research for its own sake.

A related question is how repeated usage of the same resources will be handled. Once a given dataset or tool has been accessed by one researcher, does it remain available for access by others? Or must each instance of data access be decided on *de novo* in a separate procedure? Paragraph 3 stipulates that platforms "shall provide access to data [...] through online databases or application programming interfaces", suggesting that the DSA envisages the creation of automated, scalable access solutions. However, APIs and databases must only be used "as appropriate", leaving room for alternative interpretations. Overall, it remains to be seen whether Article 31 DSA will mainly produce bespoke data grants for specific recipients, or instead automated, scalable tools available to a larger pool of researchers.

Procedural delays and logjams are a central problem in other areas of transparency regulation, such as Freedom of Information laws. And they could be especially pronounced with dominant platforms, as they are technically complex, highly adverse to transparency and notoriously litigious. Judging by their recalcitrance to earlier attempts at transparency legislation, platforms will contest compelled disclosures vigorously in and outside of court. All the more important for regulators to prioritize access to general-purpose resources that serve many comers, as each victory will be hard-fought.

The Commission's delegated acts could make or break these issues, since the current draft barely specifies any procedural aspects. And that's of course presuming the Commission ever gets around to these tasks all. From earlier episodes like the GDPR we already know[8] that the Berlaymont's eyes are often bigger than its stomach, and that delegated rulemaking announced in legislation often fails to materialize in practice.

Carveouts: security, trade secrets, and "confidential information"?

One of the hardest problems created by data access regulation is managing the risk of abuse. Article 31 DSA does this by restricting access to vetted researchers, but also by creating carveouts. Platforms can refuse an access request in cases where "giving access to the data will lead to significant vulnerabilities for the security of its service or the protection of confidential information, in particular trade secrets" (Paragraph 6). We can expect platforms to litigate these carveouts to their limits. Facebook has already abused privacy law as a pretext to refuse data access[9], and security and trade secrets considerations can be put to similar ends.

Worryingly, the exemption for commercial interests doesn't just cover trade secrets as such but all "confidential information, in particular trade secrets". This protection of the confidential is almost paradoxically broad; is it not the very purpose of a research access framework to provide access to information that has not yet been disclosed – that is, confidential? Even an exemption for "trade secrets" alone is problematic; under recent CJEU case law, transparency exceptions for trade secrets have been read so broadly that they already function, in the words of Emilia Korkea-aho and Päivi Leino[10], as a "general presumption of non-disclosure" against transparency requests toward EU agencies.

Arguably, confidentiality conditions obviate the need for such exemptions. Vermeulen[11] points out that independent auditors, regulated in Article 28 DSA, have more far-reaching access rights, covering trade secrets so long as they guarantee their confidentiality. "Pre-vetted researchers must live up to the same standards and their vetting process should be conditional upon their ability to live up to those standards," Vermeulen argues, "but security reasons and trade secrets should not be a ground for a platform to refuse access to data a priori".

What about scrapers? Protecting independent data collection

It is important to note that Article 31 DSA doesn't provide any clear answers for disputes like those between Facebook and NYU or AlgorithmWatch. These disputes revolve around the independent 'scraping' of data collected with the help of volunteer-installed browser extensions. Legally, the main problem is that platforms prohibit such practices in their Terms of Service. These provisions grant platforms the power to arbitrarily restrict access and shut down unwelcome research.

What scrapers need is a guarantee that Terms of Service won't be used to shut down privacy-compliant public interest research. In the United States, the Knight First Amendment Institute is advocating for a self-regulatory solution[12] where platforms add a so-called "safe harbor" clause for public interest research in their Terms. In Europe, AlgorithmWatch[13] is now looking to the DSA to "ensure that Terms of Service cannot be weaponized against individuals or organizations that attempt to hold large platforms to account".

Of course, scraping can also be abused. Amelie Heldt, Matthias Ketteman and I have argued in an earlier blog post[14] that platforms should still be able to take action against unlawful and unethical scraping. Matthias Vermeulen has argued for a GPDR Code of Conduct[15] that clarifies the application of data protection law to independent scraping, which should help to distinguish the good from the bad and minimize any chilling effects on legitimate research.

Will we still need scraping once – if! – Article 31 gets up and running? Yes, I argue. Scraping is an important supplement to regulated access, certainly for the time being. As should be amply clear by now, disclosure regulation is highly complex and may take years or decades to succeed, while scraping is something that already happens every day. Moreover, scraping is entirely independent of platforms and can help to fact-check the official data they provide under a regulated framework. For instance, scraped data has been used to detect political advertisements[16] that platforms failed to include in their official disclosures. Regulated access may be more powerful on the longer term, since it applies systemically to all platform data, whereas scraping only observes what platforms reveal to their users. But for the time being we depend on scraping. To that end, the DSA should not only strike at platforms to compel disclosure, but shield researchers to protect independent collection.

A more theoretical account would observe that the DSA's current approach fits neatly into existing patterns of platform regulation as described in Julie Cohen's landmark account of informational capitalism, *Between Truth and Power*[17]. Policymakers are eager to construct complex new regulatory duties on and with platform services, but remain largely blind to the role of existing legal institutions in determining the baseline allocation of entitlements around platform data, such as trade secrets and Terms of Service contracts. This is how our legislators arrive at baroque new transparency rules, while leaving unquestioned the legal strictures that brought us to this problem in the first place.

This article has originally been published on Verfassungsblog 2021/9/07, https://verfassungsblog.de/power-dsa-dma-14/, DOI: 10.17176/20210907-214355-0.

Paddy Leerssen is a PhD Candidate at the University of Amsterdam and a non-resident fellow at the Stanford Center for Internet and Society.

[1] Jeff Horwitz, "Facebook Seeks Shutdown of NYU Research Project Into Political Ad Targeting" (23 October 2020) *The Wall Street Journal* https://www.wsj.com/articles/facebook-seeks-shutdown-of-nyu-research-project-into-political-ad-targeting-11603488533 accessed 25 September 2021.
[2] Laura Edelson, Damon McCoy, "Facebook is obstructing our work on disinformation. Other researchers could be next" (14 August 2021) *The Guardian* https://www.theguardian.com/technology/2021/aug/14/facebook-research-disinformation-politics accessed 25 September 2021.

[3] Nikolas Kayser-Bril, "AlgorithmWatch forced to shut down Instagram monitoring project after threats from Facebook" (13 August 2021) *AlgorithmWatch* https://algorithmwatch.org/en/instagram-research-shut-down-by-facebook accessed 25 September 2021.
[4] AlgorithmWatch, "Open letter to European Lawmakers: Use the DSA to Stop Platforms from Suppressing Public Interest Research" (August 2021) https://algorithmwatch.org/en/wp-content/uploads/2021/08/Open_Letter_to_European_Lawmakers_26.08.21.pdf accessed 25 September 2021.
[5] Mathias Vermeulen, "The Keys to the Kingdom" (27 July 2021) https://knightcolumbia.org/content/the-keys-to-the-kingdom accessed 25 September 2021.
[6] Jef Ausloos and others, "Operationalizing Research Access in Platform Governance: What to learn from other industries?" (25 June 2020).
[7] Margaret B Kwoka, "FOIA, Inc." (2016) 65 Duke Law Journal 1361.
[8] Jef Ausloos, "The Right to Erasure in EU Data Protection Law" (Oxford University Press 2020).
[9] FTC, "Letter from Acting Director of the Bureau of Consumer Protection Samuel Levine to Facebook" (5 August 2021).
[10] Emilia Korkea-aho, Päivi Leino, "Who owns the information held by EU agencies? Weed killers, commercially sensitive information and transparent and participatory governance" (2017) 54 Common Market Law Review 1059.
[11] *n 5.*
[12] Knight First Amendment Institute, "More than 200 Research Support Knight Institute Call to Facilitate Research of Facebook's Platform" (12 June 2019) https://knightcolumbia.org/content/more-than-200-researchers-support-knight-institute-call-to-facilitate-research-of-facebooks-platform accessed 25 September 2021.
[13] AlgorithmWatch, "Under Facebook's thumb: Platforms must stop suppressing public interest research" (13 August 2021) https://algorithmwatch.org/en/defend-public-interest-research-on-platforms/ accessed 25 September 2021.
[14] Amélie Heldt and others, "The Sorrows of Scraping for Science" (30 November 2020) *Verfassungsblog* https://verfassungsblog.de/the-sorrows-of-scraping-for-science/ accessed 25 September 2021.
[15] *n 5.*
[16] NYU Ad Observatory, "The Political Ads Facebook Won't Show You" https://adobservatory.org/missed-ads accessed 25 September 2021.
[17] Julie E Cohen, "Between Truth and Power" (Oxford University Press 2019).

Eyes Wide Open

Ruth Janal

The Digital Services Act must confront a gordian knot of fundamental rights and public interests with respect to various affected actors. To be effective, the new regulation must both consider the current reality of intermediary service provision and provide enough flexibility for future technological developments. It currently falls short of this aim.

Adapting the Digital Services Act to the Realities of Intermediary Service Provision

Intermediary service providers act like spiders in the web of the internet: They build the infrastructure of the internet as we know it, they bridge the divide between content provider and user – and yes, they feast financially on anything that gets caught in-between. In 2000, the EU enacted the eCommerce Directive[1] with the aim to protect intermediary service providers from liability for third party content and to thereby bolster the budding industry. Viewed through this lens, the project was a success: Within the last two decades, new services developed rapidly, and some intermediary service providers have gained an influence on the economy, public debate and our lives in ways that seemed unfathomable only twenty years ago.

Nowadays, the question is how to harness that power: Should powerful intermediaries be bound by fundamental rights in a similar way as state actors? How to ascribe responsibility for third party content without bolstering the power of very large intermediaries? Anyone trying to regulate intermediary services must not only answer those questions. They must also confront a gordian knot of fundamental rights (freedom of speech, human dignity and safety, economic rights etc.) and public interest (fair elections, public health, protection of minors etc.) with respect to various actors: users, content providers, intermediary service providers, states and other parties affected. In light of the technological developments and the legal uncertainty regarding some of the current rules, the European Commission's Proposal for a Digital Services Act[2] (DSA-proposal) is a welcome initiative. While the political debate about the regulation's policy rules has only just begun, it is of utmost importance that the new regulation both considers the current reality of intermediary service provision and provides enough flexibility for future technological developments. The proposal currently falls short of this aim. In the following, I will highlight five matters which require a better attunement to reality.

Scope of the rules

My first critique is that the scope of the proposed regulation is not tailored to the broad spectrum of internet services which are available on the market. The proposed rules apply to "providers of intermediary services", and an important subset of those rules only addresses "online platforms". Thus, the scope of the regulation hinges upon the definitions of "intermediary service" and "online platform".

Under Art. 2 (f) DSA-proposal, only services of "mere conduit", "caching" or "hosting" are considered intermediary services. This is too restrictive. There is no convincing reason to limit the scope of the regulation to services that can be qualified as one the services currently listed in Art. 12 to 14 eCommerce Directive – in particular, since those distinctions reflect the state of the internet at the turn of the millennium! While recital 27 acknowledges a range of other information society services, these services are only supposed to be covered by the proposal if they qualify as conduit, caching or hosting "as the case may be" (sic!). This distinction is neither supported by a clear policy goal, nor does it contribute to legal clarity. Most importantly, as is, the definition of "intermediary service" excludes services that automatically compile hyperlinks and snippets, such as search engines, directories and other aggregators. This would exclude one, if not the most important information service from the scope of the Digital Services Act (hello, Google!).

The obligations prescribed in chapter III, section 3 and 4 of the DSA-proposal only pertain to online platforms (section 3) or very large online platforms (section 4). According to Art. 2 (h) DSA-proposal, an online platform is the "provider of a hosting service which, at the request of a recipient of the service, stores and disseminates to the public information" (except for minor and purely ancillary features). Again, this definition is problematic, because it encompasses most host providers, including web hosting services, but excludes many services that are considered platform services under Art. 2 (2) of the European Commission's proposal for a Digital Markets Act[3]. I have two issues with this: First, it would seem reasonable to use a consistent definition in both regulations. More importantly, however, the rules of section 3 and 4 DSA-proposal need to be tailored towards the correct addressees.

This is particularly true for section 4, which contains obligations for large service providers (in particular, the obligation to implement a risk management system). The Commission's decision to ascribe particular responsibility to big players is sensible: The additional responsibilities reflect the economic power and societal influence of such large players. Smaller providers, on the other hand, might not be able to lift the economic burden of additional responsibility and might be driven out of markets that are already non-competitive. But again, the definition of providers with systemic relevance should reflect reality. The currently proposed threshold for very large service providers lies at 45 million users and is much too high: There are only four member states of the European Union with a population larger that number[4]! Furthermore, there is no reason why risk management obligations should only apply to "online

platforms", that is, host providers, and not to other providers of systemic relevance (again: hello, Google!).

Business models focusing on illegal content

Another reality check is needed with respect to the proposed rules shielding intermediaries from liability (Art. 3 et seq. DSA-proposal). These rules operate on the assumption that the intermediary service provider carries legal and illegal third-party content alike and does not seek to specifically foster illegal content. While this assumption is true for the better-known and most powerful intermediary services, the Commission ignores that there is a niche market for providers whose business model relies upon the transmission of illegal content. The liability shields do not account for intermediaries that specialize on the mediation of illegal content, or that condone the illicit intentions of a majority of their users. While recitals 18 and 20 exempt from the liability shield an intermediary service that "plays an active role" or "deliberately collaborates with a recipient of the services in order to undertake illegal activities", this exception should be incorporated in the operative provisions of the regulation, as recitals do not possess a positive operation of their own.

Also, recital 18 perpetuates the misguided definition of "active role" already contained in recital 42 of the eCommerce-Directive: "an active role of such a kind as to give [the service provider] knowledge of, or control over, that information". Since every host provider has control over the data it stores for its users, this definition fails to contribute to legal clarity. As a result, it is unclear whether automatic ad placement, indexing, recommender systems and other services lead to an "active role" of the service provider. The European Court of Justice's case law hinges upon the facts of individual cases and is not always conclusive[5] and/or convincing[6]. The Digital Services Act should react to these realities and give a list of indications that exclude the reliance on the liability exemptions.

Review

Intermediary service providers exert considerable power through their decisions to block and to delete illegal or harmful content or to suspend user accounts. While the proposal provides for a review of content moderation decisions, those rules only scratch the surface of the problem. Art. 17 and 18 DSA-proposal require online platforms to establish internal complaint-handling mechanisms, and to provide for alternative dispute settlement regarding the removal of content and the suspension of user accounts. The Commission's faith in out-of-court settlements is quite endearing, but nonetheless unwarranted[7]. The trend to outsource government functions only contributes to the private power of intermediary service providers. A rule providing for judicial redress would therefore be welcome and is needed with respect to all service providers (Art. 15 (1)(f) DSA-proposal solely entails an information obligation and is only directed towards host providers). Judicial redress is particularly important for parties

that are not in a contractual relationship with the provider, such as content providers who are faced with a blocking decision by an access provider[8].

Furthermore, the proposed review process in Art. 17 and 18 is lop-sided, as it only allows for review in cases in which platform users have been sanctioned. If, on the other hand, the platform provider has failed to take action upon a notification of illegal content (or content prohibited by terms of use), the person that flagged the content is not protected under Art. 17 and 18. The problem with such lopsided access to review is that it allows platforms to discriminate by virtue of an arbitrary enforcement of their rules[9]. Thus, the provisions might even enhance, not limit, the providers' ability to steer the public debate. Also, Art. 17 and 18 ignore the reality of the intermediaries' elaborate sanction system. Removal and suspensions are certainly not the only avenues for a platform to sanction their users. It is much more subtle to downgrade a person's content in recommender systems and timelines. It is much more effective to discontinue advertising revenue for specific content[10] (and Art. 27 (1)(b) DSA-proposal even envisages such measures). Communication may also be stifled by closing down groups. The Commission should reconsider Art. 17 and 18 in the light of these facts.

Delegation of duty with respect to misinformation and other harmful content

The proposal also does not directly confront the fact that most of the content banned via content moderation practices is so-called "harmful content". For the purposes of this post, the term harmful content is used to describe content which is legal, but may for whatever reason be considered unethical and problematic (misinformation, nudity and pornography, depictions of violence, racism, xenophobia etc.). Under the proposal, intermediary service providers are free not to carry specific content they consider harmful. Any such restrictions must rely upon clearly worded terms of use, according to Art. 12 DSA-proposal, and may give rise to the complaint mechanisms in Art. 17 and 18 DSA-proposal. While I generally agree with the premise of this rule, there is no denying that the proposal enables intermediaries with market power to repress legal content according to their terms of use. Basically, governments are thereby delegating the task of setting adequate rules for the online communication process to the intermediaries.

At the same time, Art. 26 (1) (b) and (c) of the proposal require very large online platforms to introduce a risk management system which addresses negative effects of their services on fundamental rights and the intentional manipulation of their service with an actual or foreseeable negative effect on the protection of public health, minors, civic discourse, or actual or foreseeable effects related to electoral processes and public security. Thus, very large intermediaries are not only entitled to define permissible content, they may also be pressured to suppress certain content, even though the content is legal.

In my view, the EU and Member States should take a stronger stance on harmful content, such as misinformation. This includes rules prohibiting individuals from spreading misinformation and from coordinating misinformation by virtue of inauthentic uses of intermediary services. As long as lying and misleading the public is not illegal, intermediary services are in principle entitled to carry such content – and their actions to limit the spread of such content may arguably constitute an infringement of free speech[11]. The proposal should also specifically require service providers to undertake steps to combat misinformation, for example, by monitoring groups that practice malicious compliance[12], by setting disincentives to harmful content, by suspending users and content across platforms[13], by detecting new registrations of suspended users and via efforts to detect inauthentic use. Art. 28b of the Audiovisual Media Service Directive[14] might function as a prompt, as could the EU's Assessment of the Code of Practice on Disinformation[15]. At the very least, and in light of Art. 17 and 18 DSA-proposal, the proposal should clarify that service providers are entitled to remove content and suspend users for the purpose of combatting coordinated harmful use, even if the specific individual content is permissible under the terms of service.

The adverse incentives of advertising and recommendation systems

Speaking of misinformation and harmful content: As *Zeynep Tufekc*i has correctly noted, "we're building a dystopia just to make people click on ads"[16]. Internet users have become used to expecting services without financial remuneration. This leads intermediary service providers to focus on user engagement and data hoarding, in order to sell more ads and finance their seemingly gratuitous services. Unfortunately, user engagement is driven to a significant extent by misinformation, extremist content and general outrage. Recommender systems that rely heavily on user engagement thus push problematic content. One way to break this vicious circle is to address revenue streams and the platforms' focus on user engagement. While the proposal takes some steps in this direction, I do not think those steps go far enough.

Art. 24 DSA-proposal requires online platforms to guarantee some advertisement transparency to the ad recipient, while Art. 30 DSA-proposal commands very large online platforms to create repositories, which reveal information about the advertisements they display (content, time period, users targeted, person on whose behalf it was displayed). In my view, this is putting the cart before the horse. Yes, advertisements may be misleading, but the Unfair Commercial Practices Directive[17] provides an avenue to deal with such ads. To combat misinformation, it is necessary to look at the content which is financed by virtue of these ads (both illegal and harmful content). Particularly Facebook and Google have managed to convince advertisers – without any real proof – that their data troves allow them to efficiently target consumers. Transparency for advertisers regarding the environment in which their ads are displayed is sorely lacking, and advertisers are resorting to brand safety companies[18] to receive valiant information. A mere database of advertisements will not help solve this problem, nor will the information requirements suggested in Art. 5 (g) and 6 (g) DMA-

proposal[19]. Rather, large online platforms should inform both advertisers and the public on the context in which specific ads are displayed and on the trustworthiness of the sponsored content. At least then it wouldn't come as a surprise to advertisers[20] if they found themselves financing extremist content[21] and misinformation – and the public would have an avenue to lobby companies for responsible marketing strategies.

With respect to recommendation systems, Art. 29 DSA-proposal requires very large online platforms to provide their users with some information regarding the functionalities of the recommendation system and with recommendation-options not based on profiling. However, as experience with the GDPR has shown, one cannot expect individual users to solve systemic problems. Apart from Art. 29 DSA-proposal, the proposal solely relies upon platform risk management to address recommendation systems (Art. 26 (2), 27 (1) (a) DSA-proposal). This is insufficient. The proposal should contain a rule requiring recommendation systems of very large online platforms to not focus on user engagement alone and to prioritize quality content. Also, real-time information regarding the content which was most recommended, displayed and shared via the intermediary service is needed. Currently, tools which allow such insights are either reverse engineered, such as the project Citizen Browser[22], or offer limited insights on a voluntary basis only (i.e. Facebook's Crowd Tangle[23]).

Conclusion

As I have argued above, the institutions of the European Union need to take a closer look at the realities of intermediary service provision before enacting the Digital Services Act. This concerns the roles different types of service providers play in the information age, the definition of providers with systemic relevance and the different ways content is promoted, ranked and paid for. Also, the proposal features a remarkable retreat from traditional state functions: Instead of granting affected parties a right to judicial redress, the proposal only provides service users with a right to complaints mechanisms and to alternative dispute resolution systems. Private actors with considerable market power are allowed to define what constitutes harmful use and thus to banish legal content from the public debate. In a way, the proposal treats powerful providers as mini-governments and allows them to cement their influence on the public debate.

But just as it is easier to destroy than to build, it is easier to criticize legislation than to draft it. There are no easy fixes for illegal and harmful content online. Unsurprisingly, the European Commission's proposal is not a sword which cuts the gordian knot of fundamental rights in the information age. And while I do believe that the proposal should be further adapted to the realities of intermediary service provision, the Commission is to be commended for at least taking a stab at that gordian knot.

This article has originally been published on Verfassungsblog 2021/9/07, https://verfassungsblog.de/power-dsa-dma-15/, DOI: 10.17176/20210907-214133-0.

Ruth Janal is a Professor for Civil Law, IP Law and Commercial Law at Bayreuth University.

[1] 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 Mar-ket ("Directive on electronic commerce"), (2000) OJ L178/1.
[2] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[3] European 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)", COM(2020) 842 final.
[4] Wikipedia, "List of European Union member states by population" https://en.wikipedia.org/wiki/List_of_European_Union_member_states_by_population accessed 25 September 2021.
[5] ECJ C-682/18 and C-683/18 *Frank Peterson v Google LLC, YouTube Inc., YouTube LLC, Google Germany GmbH* and *Elsevier Inc. v Cyando AG* (2021) EU:C:2021:503.
[6] ECJ C-324/09 *L'Oréal SA and others v eBay International AG and others* (2011) EU:C:2011:474.
[7] Daniel Holznagel, "The Digital Services Act wants you to 'sue' Facebook over content decisions in private de facto courts" (25 June 2021) *Verfassungsblog* https://verfassungsblog.de/dsa-art-18/ accessed 25 September 2021.
[8] ECJ C-314/12 *UPC Telekabel Wien GmbH v Constantin Film Verleih GmbH, Wega Filmproduktionsgesellschaft mbH* (2014) EU:C:2014:192.
[9] Jessica Guynn, "Facebook while black: Users call it getting 'Zucked,' say talking about racism is censored as hate speech" *USA Today* (24 April 2019) https://eu.usatoday.com/story/news/2019/04/24/facebook-while-black-zucked-users-say-they-get-blocked-racism-discussion/2859593002/ accessed 25 September 2021.
[10] Ben Krischke, "YouTube dreht Gunnar Kaiser den Geldhahn zu - und kassiert Schlappe vor Gericht (30 July 2021) *Meedia* https://meedia.de/2021/07/30/gericht-hat-entschieden-youtube-muss-demonetarisierung-von-gunnar-kaiser-aufschlusseln/ accessed 25 September 2021.
[11] Bundesverfassungsgericht, Order of 22 May 2019, 1 BvQ 42/19.
[12] Ben Collins, Brandy Zadrozny, "Anti-vaccine groups changing into 'dance parties' on Facebook to avoid detectio" (22 July 2021) *NBC News* https://www.nbcnews.com/tech/tech-news/anti-vaccine-groups-changing-dance-parties-facebook-avoid-detection-rcna1480 accessed 25 September 2021.
[13] Kari Paul, "'A systemic failure': vaccine misinformation remains rampant on Facebook, experts say" (21 July 2021) *The Guardian* https://www.theguardian.com/technology/2021/jul/21/facebook-misinformation-vaccines accessed 25 September 2021.
[14] Directive 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive), (2010) OJ L095/1).
[15] European Commission, "Assessment of the Code of Practice on Disinformation – Achievements and areas for further improvement", SWD(2020) 180 final.
[16] Zeynep Tufekci, "We're building a dystopia just to make people click on ads" (September 2017) *TED* https://www.ted.com/talks/zeynep_tufekci_we_re_building_a_dystopia_just_to_make_people_click_on_ads accessed 25 September 2021.
[17] Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council (Unfair Commercial Practices Directive) amended by Directive (EU) 2019/2161 of the European Parliament and of the Council of 27 November 2019, (2005) OJ L149/22) and (2019) OJ L328/7.

[18] Matt Skibinski, "Special Report: Top brands are sending $2.6 billion to misinformation websites each year" *NewsGuard* https://www.newsguardtech.com/special-reports/brands-send-billions-to-misinformation-websites-newsguard-comscore-report/ accessed 25 September 2021.
[19] *n 3*.
[20] *n 18*.
[21] Jamie Grierson, "Google summoned by ministers as government pulls ads over extremist content" (17 March 2017) *The Guardian* https://www.theguardian.com/technology/2017/mar/17/google-ministers-quiz-placement-ads-extremist-content-youtube accessed 25 September 2021.
[22] The Markup – Citizen Browser, https://themarkup.org/series/citizen-browser accessed 25 September 2021.
[23] "Inside Facebook's Data Wars" (14 July 2021) *The New York Times* https://www.nytimes.com/2021/07/14/technology/facebook-data.html accessed 25 August 2021.

II

The Digital Markets Act (DMA)

The Scope of the DMA

Teresa Rodríguez de las Heras Ballell

The combination of the features characterising gatekeepers in the Digital Markets Act's is likely to create significant power imbalances in the market and lead to unfair practices that the proposal aims to prevent and repair. A service-based approach, over a provider-based one, as well as a functional description of core platform services would enhance the effectiveness of the DMA in the achievement of its policy goals.

Pivotal for success, critically assessed

The Digital Markets Act[1] (DMA) deploys an ex ante regulatory strategy aimed to ensure contestability of digital markets across the Union and to prevent unfair practices in the digital sector, where certain actors operate as 'gatekeepers'. Therefore, the concept of the gatekeeper is pivotal in the delimitation of the scope, and its correct definition is instrumental to the success of the proposal. But there are other elements of the scope to consider.

The full achievement of the policy goals inspiring the proposal, its perfect compatibility and complementarity with the competition rules and other acts of Union law, the guarantee that innovation is preserved and that no barriers to market entry are artificially raised for competitive new entrants, require a thoughtful, precise, scope-delimiting definition. Should the scope be vague, the criteria designating gatekeepers be ambiguous or inadequate, or the Commission decisions unpredictable or discretionary, at best, the entire system fails and, at worst, the regime will produce undesired effects on the market. Therefore, the feasibility, efficacy, and success of the proposal to address Big Tech actors' power is contingent on its scope and its definitions.

The scope-delimiting solution of the DMA pivots on three elements: (i) the definition of the core platform service, (ii) the concept of the gatekeeper, and (iii) the substantial connection with the Union market. These elements embody the policy goals of the proposal: to capture those providers that, even if they are not necessarily dominant in competition law terms, have an impact on the internal market due to their considerable economic power, and their role as a gateway for a large number of users to markets, services, or infrastructures. The combination of the features characterising gatekeepers is likely to create significant power imbalances in the market and lead to unfair practices that the proposal aims to prevent and repair.

I argue that the list-based definition of core platform services is not optimal for guaranteeing a technology-neutral, structure-agnostic adaptability of the DMA to future

challenges. A list of selected services may instil rigidity in the proposal in the face of new emerging models. Simultaneously, the current list of selected services does not succeed in ensuring terminological consistency and conceptual coherence with other Union acts. The risk of overlaps, gaps, or conflicts among applicable rules should be prevented and minimized. Therefore, I propose an alternative option for definitions, based on a functional description of core platform services.

As regards the designation of gatekeepers, whether the proposal aims to adopt a service-based approach or a provider-based one is not clear. A service-based approach should prevail and be expressly articulated in the determination of both the quantitative and the qualitative criteria.

Core platform services

The Regulation shall apply to 'core platform services' (Art. 1.2 DMA), defined as any digital service included in the exhaustive list enumerated by Article 2.2 DMA: online intermediation services, online search engines, online social networking services, video-sharing platform services, number-independent interpersonal communication services, operating services, cloud computing services, advertising services. Only these services qualify.

In the scoping process, the decision to select such specific services was based on their widespread and common use, their importance for connecting business users and end users, and, as per current market conditions, a higher risk of weak contestability and unfair practices. The merit of this drafting option is primarily that it provides predictability and legal certainty to the market players, while also reducing the sphere of discretion of the Commission in designating gatekeepers under the Regulation.

Nonetheless, the formula chosen to define which services fall under the Regulation invites some critical considerations.

An exhaustive list of core platform services

First, although the list of selected services seems to be quite complete today, given the constant development of the market, the absence of a functional definition of core platform services may lead to undesired results. On the one hand, the rapid transformation of the market and the emergence of innovative business models could render the list outdated and obsolete in the (near) future. Unless the listed services prove to be sufficiently broad to embrace not only analogous services, but also other new services sharing similar characteristics and raising equivalent policy concerns, the Regulation might lack future-proof adaptability. In particular, it is doubtful whether the DMA intends to adopt a technology-neutral approach: is the DMA structure-agnostic? It has been questioned, for example, whether the current list would include distributed ledger technology-based networks, which are gaining popularity and significant scale for a varied array of purposes and sectors. The central role of the provider of core platform services

might mean excluding from the scope decentralized/distributed models. However, in the near future, they could become relevant in magnitude and gatekeeping power.

The DMA does rightfully provide for a review mechanism in Article 17. But its design neither guarantees total adaptability nor a prompt reaction to market evolution: the Commission 'may' conduct a market investigation, it 'may' propose the addition of new core platform services. The investigation must be concluded within 24 months, including a proposal to amend the Regulation, as delegated acts cannot enlarge the scope. The Regulation must be amended every time – itself a lengthy process. Before an amendment is agreed and becomes effective, the Regulation would not apply to those services not included in the list of core platform services, independently of their potential to impact on the market contestability. The risk of asymmetric regulation of the digital markets should be prevented.

To counter this risk, it might be worth considering the inclusion of a functional definition of core platform services, replacing either the entire list, or adding it as a final general clause. Already, the Recitals provide clear guidance on the characteristics and features of the core platform services the proposal aims to address (Recitals 2, 3 and 4). They could inspire a functional definition. Certainly, a general clause or a functional definition may compromise the desired legal certainty and cloud the clarity that the current wording and scope ensures; however, the gains on generality, adaptability, and coherence counterbalance the losses.

Terminological consistency

Second, terminological and conceptual consistency with other Union instruments is highly desirable, but not fully assured at the moment. To delimit the scope of application, the Digital Services Act[2] (DSA) employs the well-established legal concepts of 'intermediary services' and 'information society services', whereas the Platform to Business Regulation[3] (P2B) also adds the concept of 'online intermediation services' to the EU's repertoire. In addition, the DSA attempts to formulate its own comprehensive definition of online platforms. The DMA's scope departs from this sound terminological background.

The services listed in the DMA as core platform services are not consistent with the entrenched EU regulatory terminology for digital services. Such a disparity has consequences beyond the mere terminological fragmentation: It may negatively affect the conceptualization of digital services and digital markets, hinder a smooth complementarity among Union acts, and cause unexpected policy contradictions or interpretation issues among the applicable instruments.

The perimeters of the DMA's scope

Third, due to the terminological disparities, it is uncertain to which extent the DMA's scope of application is intended to go beyond the online intermediation services of the

P2B Regulation and the online platform services of the DSA. Comparison is not easy, as the variables to outline the perimeters are not equivalent.

One might wonder whether all or most of the core platform service providers under the DMA amount to online platforms as defined in the DSA. Social networks are clearly online platforms (Recital 1 DSA), even if they are independently defined by the DMA at Article 2(7). There are no strong reasons to define them differently and on the basis of the specific content, format, or purpose of use. Social networks can evolve in the form and the means of interaction, and they can easily overlap. For example, video-sharing platforms lie at the intersection of many interactive formats of use and regulatory regimes. While video-sharing platforms and some online intermediation services providers (such as online marketplaces) may also fall under the DSA's definition of online platform; concurrently, video-sharing platform providers[4] are *inter alia* also subjected to the applicable rules of Audiovisual Media Services Directive, as amended in view of changing market realities.

Further, by using the concept of 'online intermediation services' (Art. 2.5 DMA), the proposal applies the concept as defined by the P2B Regulation. However, there are no reasons why the DMA should restrict its scope to business-to-consumer transactions, as the P2B Regulation does, and, therefore, the use of this term as defined by the Regulation might not be convincing.

A business-agnostic, technology-neutral functional definition of core platform services, underpinned by the basic concepts and the consolidated terminology of the Union regulation on digital services, would enhance the coherence of the entire legislative package, and greatly alleviate inconsistencies, contradictions, or misinterpretations.

Listing the services which qualify as core platform services in the Recitals, as an illustration of the functional definition laid down in the subsequent provision, can strike a proper balance between the desired proximity to the market, the recognition of business models and the necessary level of abstraction for robust legal rules.

The concept of gatekeeper: a service-based or a provider-based approach

Article 3 DMA sets out the quantitative and the qualitative criteria for the Commission to designate a provider of core platform services as a 'gatekeeper'.

As is, it is not clear whether the DMA adopts a service-based approach or a provider-based approach. A service-based approach entails that all the criteria for the designation of a gatekeeper are applied to and determined by the provision of each individual service. Under a provider-based approach, the spotlight is on the provider as a whole, independently of the services provided. If the thresholds are applied to each core platform service, a company can be provider of multiple core platform services and be concurrently designated as a gatekeeper in some or all of them. Hence, large companies are not necessarily to be designated a gatekeeper unless the relevant criteria are met in relation to the provision of a core platform service, and only to that extent. That would

mean that the criteria to designate gatekeepers are to be applied under a service-based approach (Art. 3.3 DMA). However, the reference to 'undertakings' in the estimation of the quantitative criteria may lead to a different conclusion (Art. 3.2 DMA). The use of the concept of an economic unit within the meaning of competition law does not seem appropriate under this new regulatory strategy.

The importance of clarifying the approach is crucial to avoid unintended consequences and to disproportionately prevent new entrants from accessing the market in reasonable and competitive conditions. For example, non-platform traditional businesses are particularly concerned about the implications of a provider-based approach. New entrants running incipient core platform models might be captured too early, if the relevant criteria for estimating gatekeeping potential apply to the whole non-platform business. Inadvertently, the DMA would be raising entry barriers for new entrants to the platform business and consolidating the entrenched position of incumbents.

Recitals 15 to 28 DMA reveal that the underlying policy is aligned with the above-proposed service-based approach, but the wording of the main provisions may lead to undesired interpretations. Both in Article 3(c) DMA and other related provisions, an explicit mention of a service-by-service analysis could provide clarity.

Further, a clarifying definition of the concept of a provider of a core platform service as a distinct and separate term from 'undertaking' would be advisable. Although the intra-group dynamics may be relevant in the determination of the obligations, the definition of a provider of a core platform service should be neutral in terms of legal form and internal organization: An entity or entities or parts of entities which provide core platform services. In effect, the definition would be service-centred and service-defined. The relevant qualitative criteria and quantitative thresholds would then be assessed and calculated per core platform service. Otherwise, the entry of or the scaling-up of non-platform traditional companies in the platform business might unintentionally be hampered, even if their core platform services were not significant enough to create a risk to contestability or of unfairness.

Conclusion

The decision to delimit the scope of the DMA on the basis of an exhaustive list of core platform services has the merit of providing legal certainty and predictability to the market. However, it constrains the adaptability of the proposal to the evolution of the market and the emergence of future business models. The review mechanism laid down in Article 17 DMA will not be agile enough to keep the DMA duly accommodated to the upcoming challenges of the platform economy, thereby risking that it will fall short of its objective. Also, the list of selected services to qualify as core platform services neither ensures terminological consistency nor conceptual coherence with other relevant instruments of the Union. That could mean overlap, incompatibility among applicable rules, interpretation issues, or undesired gaps. In these gaps, Big Tech's power may continue to grow, whereas smaller actors may be hampered by uncertainty.

The use of a functional definition of core platform services would be a preferable alternative option. In determining the qualitative and quantitative criteria for the designation of a core platform service provider as a gatekeeper, it is my proposal that a service-based approach would be more effective to achieve the policy goals inspiring the DMA, without inadvertently raising barriers to market entry or capturing new entrants to the platform business too early. A service-based approach would ensure that the Regulation does accurately target the relevant actors, if they provide core platform services, if they act as gatekeepers, and if they hold economic power to cause imbalances in the market, without further organizational, structural or legal considerations. The strategical design of the business model, the internal structure of the provider, or the legal form adopted should not divert the regulation from its main policy goals. A service-based approach is structure-agnostic, design-neutral, and does not risk business innovation and market competition.

This article has originally been published on Verfassungsblog 2021/8/30, https://verfassungsblog.de/power-dsa-dma-02/, DOI: 10.17176/20210830-233002-0.

Teresa Rodríguez de las Heras Ballell is a Professor of Commercial Law at the University Carlos III of Madrid. She is also a Member of the Expert Group for the EU Observatory on the Online Platform Economy.

[1] European 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)", COM(2020) 842 final.
[2] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[3] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users online intermediation services, (2019) OJ L186/57.
[4] European Commission, "Guidelines pursuant to Article 13(7) of the Audiovisual Media Services Directive on the calculation of the share of European works in on-demand catalogues and on the definition of low audience and low turnover", (2020) OJ C223/3.

Why End-User Consent Cannot Keep Markets Contestable

Inge Graef

A central source of Big Tech gatekeepers' power is their encompassing access to individuals' personal data. The prohibition of Article 5(a) of the proposed Digital Markets Act, therefore, is a welcome attempt to limit the private power over data held by gatekeeping platforms. However, end-user consent cannot be regarded as an adequate safeguard for keeping data-driven markets competitive.

A suggestion for strengthening the limits on personal data combination in the proposed Digital Markets Act

A central source of Big Tech gatekeepers' power is their encompassing access to individuals' personal data. By combining personal data across the range of services they provide, gatekeepers are able to create increasingly precise profiles of individuals. Their control over vast amounts and sources of data may not only erode the privacy interests of individuals but can also strengthen gatekeepers' competitive advantage over business users and rivals.

The prohibition of Article 5(a) of the proposed Digital Markets Act[1] (DMA), therefore, is welcome as an attempt to limit the private power over data held by gatekeeping platforms. This provision requires a gatekeeper to refrain from combining personal data sourced from its core platform services with personal data from other services offered by the gatekeeper or third parties, unless the end-user provided consent under the General Data Protection Regulation[2] (GDPR). The prohibition is based on the remedy imposed by the German Bundeskartellamt in its 2019 Facebook decision[3].

However, end-user consent cannot be regarded as an adequate safeguard for keeping data-driven markets competitive. To undo the competitive harm resulting from Facebook's practices, it is submitted here that the Bundeskartellamt should have imposed a more far-reaching remedy. For the same reason, the DMA should not rely on end-user consent as a mechanism to keep markets contestable, where gatekeepers wish to combine personal data. Rather, gatekeepers should only be able to combine personal data across services under the DMA when this is necessary to perform a contract.

The Reasoning in the Bundeskartellamt's Facebook Case

In its 2019 decision, the Bundeskartellamt found that Facebook had violated the German competition rules, by forcing end-users to agree that their social network data would be combined with personal data collected within Facebook's other services, such

as WhatsApp and Instagram, and with personal data collected by Facebook on third-party websites. If end-users did not agree to these terms, they could not use Facebook's social networking service. To assess whether Facebook's conduct met the thresholds of abuse, the Bundeskartellamt relied[4] on the data protection rules of the GDPR as a standard, against which it determined that Facebook had violated German competition law.

As part of its reasoning, the Bundeskartellamt concluded that end-user consent was not freely given[5], as required under Article 4(11) GDPR, due to Facebook's dominant position and the absence of alternative social networks on the market. The combination of personal data was also not found necessary for the provision of a social network service to the end-users. And finally, Facebook's legitimate interests in combining personal data for commercial purposes did not outweigh end-users' interests with respect to the protection of their personal data. For these reasons, there was no lawful ground for combining personal data under Article 6(1) GDPR. By violating the GDPR, Facebook, in the view of the Bundeskartellamt, also exploited end-users and excluded competitors in violation of the German competition rules.

The reasoning of the Bundeskartellamt is controversial[6], especially with regard to the question whether it is desirable for a competition authority to intervene against anti-competitive conduct that also violates data protection rules, and to substantially reason on the latter grounds. In the interim proceedings on appeal, the Oberlandesgericht[7] in Düsseldorf and the Bundesgerichtshof[8] reached diverging conclusions on the legality of the Bundeskartellamt's decision. The latest development is the Oberlandesgericht in Düsseldorf's referral of questions[9] to the Court of Justice in Luxembourg, on the Bundeskartellamt's interpretation of the GDPR.

Irrespective of the intervention's desirability, the key question is whether the remedy chosen by the Bundeskartellamt to put an end to Facebook's infringement is effective to address the competitive harm.

Why the Remedy in the Bundeskartellamt's Facebook Case Cannot Address Competitive Harm

As a result of the remedy imposed by Bundeskartellamt, Facebook is only allowed to combine personal data from its various services and third-party websites with the voluntary consent of the end-user. The inspiration for this remedy is drawn from the GDPR, where consent is one of the lawful grounds for processing personal data under Article 6. After the Bundeskartellamt's decision, end-users are no longer required to consent to their personal data being combined as a precondition for using Facebook's social network. Even if end-users do not consent to the combination of personal data across services, Facebook must allow them to use its social network.

Although this remedy empowers end-users by giving them more control over their personal data, it is questionable whether the imposition of end-user consent as a

precondition for the combination of personal data is sufficient to silence the competition concerns. The effectiveness of the remedy of consent in promoting competition is completely dependent on individual users' choices. This fallacy is all the more relevant now that the DMA is copying the Bundeskartellamt's Facebook remedy in Article 5(a) DMA and is applying it to all situations where gatekeepers want to combine personal data across different services.

In fact, the remedy in the Facebook case does not go beyond ensuring compliance with the GDPR. Arguably, the outcome illustrates that competition law was merely used to enforce data protection law. By limiting the remedy to consent under the GDPR, the Bundeskartellamt makes itself vulnerable to critics who claim that, as a competition authority, it was not competent to enforce the GDPR. Had it imposed a stronger, alternative remedy to address the competitive harm beyond the data protection harm, this might have eliminated doubts about its competence. Even though it relied on the GDPR to establish a violation of the German competition rules in its substantive assessment, the Bundeskartellamt was not bound to a data protection remedy, but could instead have adopted a competition remedy to address the competitive harm. Rules from other legal regimes, such as intellectual property law, have already been used as an indicator[10] for establishing an infringement of competition law. The key condition is that the breach of another legal regime causes competitive harm. Although the Bundeskartellamt pointed to competitive harm in the form of exploitation of end-users and exclusion of competitors caused by the violation of the GDPR, such competitive harm cannot be remedied through consent, whose effectiveness depends on the choices of individual users.

End-user consent under the GDPR cannot address competitive harm due to data externalities[11]. These externalities imply that the choices of one person may affect other persons with similar characteristics. If person A consents to her personal data being exchanged between services, the combined dataset about her behavior and preferences may also provide more detailed insights about persons B, C and D who, for example, have similar preferences and share demographic characteristics. As explained, the Bundeskartellamt remedy makes the extent to which the exploitation of end-users and exclusion of competitors occurs dependent on the individual choices of end-users. This is not a responsibility that individual users should be expected to carry, especially given the competitive and collective harm that the Bundeskartellamt identified, which exceeds the harm to individual end-users that data protection law aims to address.

If the majority of Facebook's users still agrees to having their personal data combined, the remedy will only have a limited effect on the protection of overall competition and consumer welfare. Since the Bundeskartellamt was not limited to remedies within data protection, it could have gone a step further, by prohibiting Facebook from combining personal data, regardless of whether end-users consent. Such a measure – while certainly controversial – would have better addressed the competitive harm in the market and the externalities that individual end-users do not and should not be expected to

take into account when deciding whether to consent to the combination of their personal data.

A Shortcoming in the DMA

For the same reasons, the DMA should impose stricter requirements on the combination of personal data and should not rely on consent per the GDPR. The DMA's goal of ensuring "contestable and fair markets in the digital sector" goes beyond protecting the individual relationship between end-users and data controllers, on which the GDPR focuses. The evident risk behind the current phrasing of Article 5(a) DMA is that gatekeepers can trick users into agreeing[12] to the combination of personal data, without realizing the potential consequences for themselves and others.

In Article 5(a), the DMA falls short of its stated objective of imposing stricter requirements on gatekeepers in order to make markets fairer and more contestable. The European Data Protection Supervisor recalled in its opinion on the DMA[13] (in par. 24 and footnote 26) that other digital platforms, not qualifying as gatekeepers, must already obtain consent from end-users to combine personal data for the purposes of profiling and tracking under the GDPR. In other words, Article 5(a) DMA does not depart from the current interpretation of the GDPR for these purposes, because the requirement of end-user consent already applies to all data controllers under the GDPR, irrespective of their market position.

An Alternative Condition for Combining Personal Data in the DMA

A stronger and more reliable condition for combining personal data, rather than consent, could be Article 6(1)(b) GDPR, which states that the processing of personal data is lawful when it is "necessary for the performance of a contract" to which the end-user is a party. Such an approach would offer stronger guarantees than consent[14] because this lawful ground for the processing of personal data would only allow gatekeepers to combine personal data to the extent that this is indispensable for the performance of a contract, such as the provision of a service.

One example of a service requiring the combination of personal data could be a new application, bringing together personal data from a gatekeeper's email service and map service, to advise a user on how to best organize her travel movements. Where the combination of personal data only increases the level of personalization of the service, but is not strictly necessary for the provision of the service, gatekeepers should not be allowed to combine personal data. Although this may seem far-reaching, the GDPR's purpose limitation principle already limits the exchange of personal data across services offered by the same provider, if this results into personal data being processed for a different purpose than for which it was originally collected. Because of the larger impact of their practices on the market, the same should apply a fortiori to gatekeepers under the DMA. Even though one may argue that this approach harms consumers in the short term, due to the limits on personalization, the restrictions imposed on

gatekeepers also provide room for other market players to attract consumers to their services, with the prospect of more consumer choice in the longer term.

Where the combination of personal data is an unavoidable prerequisite for the performance of a contract, the merging of data should be possible: it brings value to end-users and to the market in the form of new services that would otherwise not have existed. End-users will retain control over their personal data, due to their choice whether or not to receive a service from a gatekeeper.

However, monitoring is necessary to ensure that gatekeepers interpret[15] the condition in a way that the combination of personal data only happens if strictly necessary for the performance of a contract they have concluded with end-users. In particular, the combination of personal data with the sole aim of increasing personalization[16], profiling end-users and improving targeted advertising should fall outside of the notion of performance of a contract. These are precisely the practices that the DMA should restrict, in order to control the private power held by gatekeepers and to open up competition to the benefit of rivals as well as to protect the long-term interests of consumers.

Unless Article 5(a) DMA is amended to relieve individual end-users of the responsibility to decide on the desirability of combining personal data across services, there is a risk that gatekeepers can continue exploiting their strong competitive advantage resulting from the ties between the range of services they offer to the detriment of consumers, businesses and the European digital single market.

This article has originally been published on Verfassungsblog 2021/9/02, https://verfassungsblog.de/power-dsa-dma-08/. It is a variation of part of a Dutch language paper written by the author entitled “Het reguleren van het gebruik van data door digitale platforms: gaat de voorgestelde Digital Markets Act ver genoeg?”, which is forthcoming in the journal Markt & Mededinging.

Inge Graef is Associate Professor of Competition Law at Tilburg University and is affiliated with the Tilburg Institute for Law, Technology, and Society (TILT) and the Tilburg Law and Economics Center (TILEC).

[1] European 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)”, COM(2020) 842 final.
[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016) OJ L119/1.
[3] Bundeskartellamt, Decision under Section 32 (1) German Competition Act of 6 February 2019, B6-22/16.
[4] Bundeskartellamt, “Bundeskartellamt prohibits Facebook from combining user data from different sources” (7 February 2019) https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2019/07_02_2019_Facebook.html.accessed 25 September 2021.

[5] European Data Protection Board, "Guidelines 05/2020 on consent under Regulation 2016/679 – Version 1.1." (13 May 2020).
[6] See https://devcpi.com/wp-content/uploads/2019/03/EU-News-Column-March-2019-3-Full.pdf.
[7] Oberlandesgericht Düsseldorf, order of 26 August 2019, Kart 1/19 (V).
[8] Bundesgerichtshof, order of 23 June 2020, KVR 69/19.
[9] Oberlandesgericht Düsseldorf, order of 24 March 2021, Kart 2/19 (V).
[10] ECJ C457/10P *AstraZeneca v European Commission* (2012) EU:C:2012:770.
[11] Daron Acemoglu and others, "Too Much Data: Prices and Inefficiencies in Data Markets" (2019) NBER Working Papers 26296.
[12] Rupprecht Podszun, "Should gatekeepers be allowed to combine data? – Ideas for Art. 5(a) of the draft Digital Markets Act" (8 June 2021) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3860030 accessed 25 September 2021.
[13] European Data Protection Supervisor, "Opinion 2/2021 on the Proposal for a Digital Markets Act" (10 February 2021).
[14] European Data Protection Board, "Guidelines2/2019 on the processing of personal data under Article 6(1)(b) GDPR in the context of the provision of online services to data subjects" (9 April 2019).
[15] Timothy Lamb, "Initial Reflections on the Draft Digital Markets Act" (May 2021) https://antitrustlair.files.wordpress.com/2021/05/initial-reflections-on-the-digital-markets-act-2.pdf accessed 25 September 2021.
[16] Inge Graef, "Consumer sovereignty and competition law: From personalization to diversity" (2021) 58 Common Market Law Review 471.

How to Challenge Big Tech

Jens-Uwe Franck • Martin Peitz

The European Commission's proposal for a Digital Markets Act is meant to complement EU competition law, in order to guarantee contestable digital markets. However, from a policy point of view, the current self-restriction to behavioural remedies in competition law and merger control, as well as the focus on behavioural ex ante regulation via the DMA, is at best a half-hearted and at worst a misguided way to effectively address the Big Tech challenge. We argue in favour of a competition law toolkit with extended options to use structural measures to tackle entrenched market dysfunctionalities.

Internationally, there is growing discomfort about the market position of some large digital players that serve as matchmakers and gatekeepers, controlling entire ecosystems. In Europe and the U.S., "Big Tech" is associated with the names of Google, Amazon, Facebook, Apple, and Microsoft – now widely famous under the acronym "GAFAM" – and possibly a few others. Those Big Tech players are accused of foreclosing or absorbing potential competitors, erecting barriers to entry and leveraging their entrenched market positions. While the immediate effect on consumers is often difficult to assess, the claim is that there is long-term harm to innovation and consumers.

The European Commission has proposed the Digital Markets Act (DMA[1]) as a regulatory tool that is meant to complement EU competition law, in order to guarantee contestable digital markets. However, from a policy point of view, the current self-restriction to behavioural remedies in competition law and merger control, as well as the focus on behavioural *ex ante* regulation via the DMA, is at best a half-hearted and at worst a misguided way to effectively address the Big Tech challenge.

We argue in favour of a competition law toolkit with extended options to use structural measures to tackle entrenched market dysfunctionalities: expanded and strengthened merger control; extended possibilities to respond to infringements of competition law and equivalent provisions with structural remedies; and the availability of forced divestiture, possibly after a market investigation.

The Digital Gatekeeper Challenge

An increasing part of economic and social activity is facilitated by digital players and channelled through the internet, and a small number of firms have taken key "gatekeeper" positions. GAFAM have become private regulators dictating terms and conditions to participants in their ecosystems. Even if users are uncomfortable with those terms, there are often few viable alternatives to some of the services offered. Increasingly, GAFAM's position looks to have become entrenched for a number of services.

Strong network effects increase the value of a digital service for consumers and business users, and, because of coordination problems and inertia, switching to newcomers is unattractive. It is a bit like a meritocracy trap[2]: Big Tech firms make more-attractive value propositions and become more sophisticated in extracting rents, and challengers have to overcome more and more hurdles.

The EU's Regulatory Response

Regulating firms with power relative to other businesses in a vertical relationship or entrenched market power is a natural response. This is indeed the approach the EU has taken. The EU lawmaker has established across-the-board transparency rules in its Platform-to-Business Regulation 2019/1140[3]. These are meant to improve business users' position vis-à-vis the digital platforms. The EU lawmaker also targets a small number of particularly powerful players with an entrenched market position. With the proposed DMA[4], it seeks to prohibit certain business practices when adopted by them.

To illustrate, if a platform obliges its business users not to offer lower prices elsewhere, business users cannot divert consumers through price. This limits platforms' incentives to compete on fees or other conditions they offer to their business users. End users may suffer from higher prices or lower quality. This concern goes beyond Big Tech and applies to other platforms in strong positions with respect to specific user groups, such as hotel booking platforms vis-à-vis independent hotels or event ticketing platforms vis-à-vis concert organizers. Thus, the rationale for singling out a few firms is not obvious in the case of some of the proposed obligations and prohibitions in the proposed DMA. The raison d'être of an intervention is not contingent on a gatekeeper position, as presupposed by the DMA proposal.

Things look different if the risks of exploitation and foreclosure increase with the scope of operations and market entrenchment, thanks, in particular, to overwhelming network effects. Here, the DMA approach is broadly suitable – that is, to specifically address gatekeeper platforms and to implement remedies that aim at keeping markets open or opening them up.

Behavioural Remedies and Their Shortcomings

At the EU level, we see, first of all, fines and behavioural remedies by the Commission based on findings of an infringement of Article 102 TFEU (abuse of market dominance) against Google (Alphabet) (Google Shopping[5], Android[6], and AdSense[7]), as well as pending investigations against Apple (App Store Practices (music streaming)[8], App Store Practices[9], and Mobile payments[10]), Amazon (Amazon Marketplace[11] and Amazon – Buy Box[12]) and – again – Google (ad tech and data-related practices[13]). Moreover, merger control may give the option to regulate market conduct via behavioural remedies so that combined resources (data) may not readily be used to erect new market barriers. In the Google/Fitbit[14] merger proceedings, the Commission made extensive use of this. For instance, Google had to commit to not using the health and wellness data collected from Fitbit devices for Google Ads (including search advertising and display advertising).

Lawyers consider structural remedies – as opposed to behavioural remedies – to be the more intrusive measure. They may be seen as surgery instead of permanent drug treatment. Yet, structural remedies appear to be more in line with the idea that the state trusts market forces within an economic order it has formed, to guarantee the functioning of markets. Thus, in aggregate, "surgery" may be regarded as preferable, as it ultimately amounts to more economic freedom for all market players – including those that are subject to regulation due to their economic power.

In line with our view, the British Competition and Markets Authority (CMA), the Australian Competition and Consumer Commission (ACCC) and the Bundeskartellamt have issued on 20 April 2021 a "Joint statement on merger control enforcement"[15], stating that the "increasing complexity of dynamic markets and the need to undertake forward-looking assessments require competition agencies to favour structural over behavioural remedies."

One structural remedy that is hotly debated in the U.S. is the "breakup" or, to use a term that sounds less dramatic, forced divestitures. Sometimes, such forced divestitures simply correct a merger that has turned out to be problematic. While a reinforced merger policy clearly cannot deal with the problems from the past, it may help in the future. Thus, a discussion of structural remedies in response to competition problems should start with merger policy

Merger Policy for Big Tech

Big Tech has acquired a large number of start-ups over the last decade. In digital markets it is difficult to foresee how these start-ups would have developed if they had stayed independent or had been acquired by some other firm. Currently, to block a merger, the Commission has to argue a case showing that the notified concentration will have anti-competitive effects. Given the uncertainties and the competition authorities' lack of information, this is often an almost impossible mission.

Strengthening competition authorities' power to prohibit mergers could mean to lower the required standard of proof, or giving them the power to reverse the burden of proof with regard to the expected effects on competition in clearly specified scenarios – for instance, if one of the merging firms has a powerful entrenched position. Such a position may be identified by a market investigation or by applying criteria as established in the proposed DMA[16] or section 19a of the German Competition Act[17].

Various reform approaches point in this direction. In France, the Senate has approved a legislative initiative[18], currently pending in the National Assembly, that would shift the burden of proof in merger cases involving (designated) large digital gatekeepers ("*entreprises structurantes*"): When the competition authority initiates an in-depth examination of a notified transaction, it is the undertaking that must provide evidence that the transaction is not likely to harm competition. Likewise, in the U.S., the House Judiciary Committee recently approved a bill that would ban acquisitions by (designated) large digital platforms, unless they can prove that the merger will not harm actual or potential competition.

The French, German and Dutch governments ("Friends of an Effective Digital Markets Act"[19]) lament that Article 12 of the DMA proposal lacked ambition. They demand that the existing EU merger framework should be modified for DMA gatekeepers: Acquisitions of low-turnover but high-value targets should be captured and the substantive test should be adapted to more effectively address cases of "potentially predatory acquisitions". This is water to our mill.

Market Structure in Digital

Ultimately, the choice over whether we live in an environment with a few firms controlling large ecosystems or a more fragmented digital world is political. Since innovations yet unknown will benefit unforeseen digital activities, our working hypothesis is that a more fragmented world is likely to deliver more innovation than a world with few ecosystems, controlled by heavily regulated firms.

Absent the ability to impose divestiture obligations and to run a stricter merger policy, the DMA and its envisaged regulatory approach toward Big Tech may still help in opening up space for new and independent digital players. By analogy, this happened in a number of regulated industries, for example telecommunications, in which privatized incumbent firms were subject to more stringent regulation than newcomers were.

Regulation via the DMA or, possibly, via behavioural remedies imposed on the occasion of merger proceedings, seems to be a very indirect way of achieving this outcome. Enabling the European Commission to impose divestiture obligations as the result of a market investigation and, looking forward, to block digital conglomerate mergers more easily are more direct paths to a healthier digital world. In light of institutional constraints, this may be wishful thinking, but at least an open discussion in the Member States would be helpful. The option of stricter merger control and forced divestiture should not be taken off the table.

Divestiture Initiatives

Forced divestitures are not unheard of in Europe. In West Germany, after World War II, mandated unbundling, such as that of IG Farben, was a powerful beacon to herald in the new paradigm of guaranteeing competition by means of regulatory intervention – if necessary, also by intervention in the market structure. This post-war period of competition law in West Germany was based on Allied decartelization laws inspired by U.S. antitrust law.

In the U.S., divestiture obligations are accepted as a legitimate remedy in the competition toolbox and its availability under section 2 of the Sherman Act has been recognised by the U.S. Supreme Court. Certainly, this remedy is not exactly routinely used, but it is an option. Very recently, in its complaint[20] filed against Google on 20 October 2020, the U.S. Department of Justice requests the court to "enter structural relief as needed to cure any anticompetitive harm". Moreover, politically, "unbundling Big Tech" is not seen as a far-fetched objective of competition policy. Rather, after recent debates in the House on a package of six tech-focused bills, Dan Bishop, a Republican U.S.

Representative for North Carolina, remarked, "I will tell you, I'm not 100% there to break up Big Tech, but I'm close."[21]

Under German law, similar to EU law, structural remedies are hardly ever used, as they can only be imposed in case of competition infringements "if there is no behavioural remedy which would be equally effective, or if the behavioural remedy would entail a greater burden for the undertakings concerned than the structural remedies"[22]. Neither in the EU nor in Germany can divestiture be ordered as an (objective) instrument of market regulation. The last attempt to add such an instrument to the competition toolbox – initiated by the Federal Ministry of Economic Affairs and supported by the Monopoly Commission[23] – got bogged down in 2010. The debate at the time[24] focused on conceivable targets (remarkably, Big Tech was not really on the radar yet), on fundamental questions of competition policy, and on uncertainties about what leeway EU law and fundamental rights left to the German legislature.

Since 2010, however, the rise of the digital platform economy and of concentration within it has continued. With this ongoing fundamental transformation of our economy, it would seem careless not to have an open mind to reconsidering structural instruments that were previously rejected as being too harsh for the addressees or too burdensome for the authorities to be implemented.

What Can We Ultimately Expect from the DMA?

In response to structural competition problems, it is only natural and indeed consistent to consider structural remedies, including breakups of digital conglomerates. Time will tell whether GAFAM will have to divest some of their activities. The more immediate question in the EU is who is willing to invest political capital to initiate a serious debate on strengthened merger control and forced divestitures as a regulatory instrument. A cautious move in this direction is the attempt by the rapporteur[25] of the European Parliament to amend Article 16 of the DMA proposal[26] in such a way that, first, the choice between behavioural and structural remedies is to be made based not on "proportionality" but on "effectiveness" and, second, that for structural remedies to be imposed it need not be shown that "equally effective behavioural remedies" are either not available or "more burdensome for the gatekeeper concerned". In addition, there may still be hope that the initiative of the "friends of an effective DMA" to strengthen merger control will find fertile soil. However, we fear that the EU will, in the end, continue to restrict itself to playing games of behavioural remedies and regulation. We would be happy to be proved wrong.

This article has originally been published on Verfassungsblog 2021/9/06, https://verfassungsblog.de/dsa-dma-power-12/, DOI: 10.17176/20210906-214440-0.

Jens-Uwe Franck is Professor of Law at the University of Mannheim and Senior Member of the Mannheim Center of Competition and Innovation—MaCCI. Hde advises the Federal Ministry for Economic Affairs on issues related to the DMA.

Martin Peitz is Professor of Economics at the University of Mannheim (since 2007) and a director of the Mannheim Centre for Competition and Innovation—MaCCI.

---

[1] European 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)", COM(2020) 842 final.
[2] Roge Karma, „'The Meritocracy Trap,' explained" (24 October 2019) *Vox* https://www.vox.com/policy-and-politics/2019/10/24/20919030/meritocracy-book-daniel-markovits-inequality-rich accessed 25 September 2021.
[3] Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business of online intermediation services, (2019) OJ L186/57.
[4] *n 1.*
[5] European Commission, Case AT.39740 Google Search (Shopping) (2010-2017).
[6] European Commission, Case AT.40099 Google Android (2015-2018).
[7] European Commission, Case AT.40411 Google Search (AdSense) (2016-2019).
[8] European Commission, Case AT.40437 Apple – App Store Practices (music streaming) (2020 ongoing).
[9] European Commission, Case AT.40716 Apple – App Store Practices (2020 ongoing).
[10] European Commission, Case AT.40452 Apple – Mobile payments (2020 ongoing).
[11] European Commission, Case AT.40462 Amazon Marketplace (2019 ongoing).
[12] European Commission, Case AT.40703 Amazon – Buy Box (2020 ongoing).
[13] European Commission, Case AT.40670 Google – Adtech and Data-related practices (2021 ongoing).
[14] European Commission, Case M.9660 Google/Fitbit (2020)
[15] Competition & Markets Authority, Australian Competition & Consumer Commission, Bundeskartellamt, "Joint Statement on merger control enforcement" (2021).
[16] *n 1.*
[17] German Act Against Restraints of Competition § 19a.
[18] Progress of Libre choix du consommateur dans le cyberespace, https://www.senat.fr/dossier-legislatif/ppl19-048.html#timeline-1 accessed 25 September 2021.
[19] Governments of France, Germany, and the Netherlands, "Strengthening the Digital Markets Act and Its Enforcement" (2021).
[20] US Department of Justice and others, Complaint in Case 1:20-cv-03010 *US and others v. Google LLC* (10 October 2020).
[21] Lauren Feiner, "House committee passes sweeping tech antitrust reforms, but their future remains murky" (24 June 2021) *CNBC* https://www.cnbc.com/2021/06/24/house-committee-passes-broad-tech-antitrust-reforms.html accessed 25 September 2021.
[22] German Act Against Restraints of Competition § 32.
[23] Monopolkommission, "Gestaltungsoptionen und Leistungsgrenzen einer kartellrechtlichen Unternehmensentflechtung" (27 April 2010).
[24] Bundeskartellamt, "Entflechtung als Instrument des Kartellrechts: Neue Instrumente im GWB?" (October 2010).
[25] European Parliament Committee on the Internal Market and Consumer Protection, "Draft Report on the proposal for a regulation of the European Parliament and of the Council Contestable and fair markets in the digital sector (Digital Markets Act)" (1 June 2021).
[26] *n 1.*

III

Enforcement

Private enforcement and the Digital Markets Act

Rupprecht Podszun

> *For the Digital Markets Act to function properly – that is, to dismantle overwhelming private power – enforcement capacities of private actors should be strengthened at the outset: Competitors and customers should be integrated into the enforcement system as complainants, informants and litigants. The digital giants will not tumble because of government intervention but because of innovative competitors and stronger customers that can rely on the framework set by governments. Private power needs to be cured with private empowerment.*

The Commission will not be able to do this alone

The Google Cases made Margrethe Vestager and her team at the European Commission heroes in the fight against the insolences of Big Tech. And rightly so: The Directorate General for Competition deserves the praise for taking on some of the most powerful companies in the world, for chartering new territory and for persisting in the still on-going uphill battle for the regulation of Big Tech. But they had great helpers – even more than that: instigators – that sent them on the mission.

This contribution serves as a memorial to these actors – which is all the more necessary since they were forgotten in the Digital Markets Act (DMA). For the DMA to function properly – that is, to dismantle overwhelming private power – enforcement capacities of private actors should be strengthened at the outset: Competitors and customers should be integrated into the enforcement system as complainants, informants and litigants. Without explicit rules on this form of "private enforcement" the high ambitions of the DMA are likely to remain unfulfilled. The digital giants will not tumble because of government intervention but because of innovative competitors and stronger customers that can rely on the framework set by governments. Private power needs to be cured with private empowerment. This should, ideally, be reflected in the procedural rules.

How it all started

To find out who the masterminds behind the landmark Google Shopping decision[1] of the European Commission were, you need to turn to paragraph 39 of that 755-paragraph-long decision:

> "*On 3 November 2009, Infederation Ltd. ("Foundem") lodged a complaint against Google with the Commission. […] On 22 January 2010, pursuant to Article 12 of Regulation (EC) No 1/2003, the Bundeskartellamt (Germany) exchanged information with the Commission on a complaint against Google lodged by Ciao GmbH ("Ciao"). […] On 2 February 2010, eJustice.fr ("eJustice") lodged a complaint against Google with the Commission.*"

It goes on like this for several pages. If you, well, *google* Foundem today, you find a dead former price comparison portal and much information about its battle for life, turned into an antitrust fight. Foundem and the other companies that followed suit got the Commission going. They called for help in 2009 and 2010, yet it took the Commission until 2017 to reach a decision (that is under review by the courts[2]). That is quite a while in digital times. However, without the first-hand information from market players, there may not have been any Google case at all.

Antitrust cases strongly rely on the information provided by market actors. From my own days as a case officer in the *Bundeskartellamt*, the German competition watchdog, I remember the dependence on market actors: You sift through the large number of complaints to detect infringements in the first place; and once you have opened a case you are completely dependent on information provided by experts in the respective trade – usually customers and competitors of the undertaking under investigation.

The Commission wants to do it alone

The draft DMA contains very few words on the role of private parties in taming the gatekeepers. In Art. 19, undertakings are subjected to requests for information. In Art. 20, the Commission is empowered to interview persons who may contribute to the investigations (if these persons consent). That is it – a very basic involvement of third parties.

This restraint towards private enforcement and the participation of competitors or customers in DMA proceedings is a mistake: The Commission will not be able to deal with gatekeeper regulation alone.

The "Friends of an Effective Digital Markets Act" – the governments of France, Germany and the Netherlands – came to the same conclusion in their May 2021 non-paper[3]. They did not only ask for better involvement of national agencies and the Member States, but explicitly favour "private enforcement of the gatekeeper obligations." In a joint paper from June 2021[4], the national competition agencies also mentioned the important role and deterrent effect of private enforcement.

The DMA in its current version ignores the role of private parties for setting the framework for fair and contestable markets. Private enforcement is not mentioned. The enforcement regime, as it stands, relies on automatic compliance by the gatekeepers and on monitoring and enforcement by the Commission. That is a confident expectation: Will some of the most powerful undertakings in the world really subject themselves

automatically to obligations set in the DMA? Will the Commission detect problems that may arise from a different understanding of the words – or blatant non-compliance?

The role of private parties

The role of private market actors in administrative proceedings is usually threefold: Firstly, they solve the information deficit of the agency. Secondly, they initiate, drive and control proceedings through their formal participation. Thirdly, they monitor compliance after proceedings and claim damages in case of loss. There is a fourth function that I will turn to later.

The first three, mentioned here, are functions of private actors that are established in traditional competition law. I am hesitant to praise competition law proceedings as a model for the involvement of private parties, however, as it is still very burdensome for private actors to get involved in EU competition cases.

Complainants have a weak position in Commission proceedings. They may complain, but there are no time limits for the Commission to react, no duty to take up a case, and the Court's practice in dealing with complaints that got a formal rejection decision from the Commission gives enormous leeway to the Commission. Access to information, the possibility to have a hearing, the right to complain and the right to claim damages – yes, these exist, and third parties certainly have an impact on competition proceedings, but their role remains weak.

In competition law, all these rights, although weak, were established, developed and spelt out as rules of procedure, rules for damages, rights to complain etcetera, in hard-fought court battles or in Commission guidelines. They are achievements built over years. However, this "acquis" is not directly applicable to the DMA. With the draft law as it stands, the fight begins anew.

The DMA is not a piece of competition law legislation (at least that is what the Commission claims, and while many of my colleagues wish to see the DMA in the realm of traditional antitrust[5], I side with the Commission here). The whole enforcement apparatus, developed for the enforcement of Art. 101 and 102 TFEU, is thus not applicable in DMA cases. In effect, the Commission ventures into a new field of direct application of EU rules by an EU administrator to undertakings without a similar set of accompanying laws and standards or best practices. (Just consult the legislation pages[6] on the DG COMP website to get an impression of the body of law that nowadays serves to implement two provisions in the TFEU.) I doubt that DMA enforcement can do without this.

The pros of private enforcement

But is gatekeeper regulation a matter for private enforcement at all?

For a German competition lawyer, that is a no-brainer: Yes! We are nurtured with ordoliberal superfood from day one, before getting a Hayek diet, which means that we believe that the spontaneous market order is mirrored by a private law society (as *Franz Böhm* once famously described it in ORDO[7]). Where private actors can establish

a market order (with the help of courts), they do not need to rely on state interventionism.

Apart from a sentimental belief in such concepts, economists would argue with the efficiency and the effectiveness of private actors' involvement: They have superior market knowledge, they jump at the pressing issues, they are able to reduce bureaucratic costs. The Court of Justice repeatedly pointed at the effectiveness of European law to justify private enforcement. Deterrence and compensation are strengthened if private sheriffs are around.

In European legal doctrine, the private pillar of market regulation is well-established. Readers of *Verfassungsblog* do not need a reminder of Van Gend & Loos[8], but the wording of the Court of Justice is so inspiring, still today, that it justifies the quote:

> "*...the Community constitutes a new legal order of international law for the benefit of which the states have limited their sovereign rights, albeit within limited fields, and the subjects of which comprise not only Member States but also their nationals. Independently of the legislation of the Member States, Community law therefore not only imposes obligations on individuals but is also intended to confer upon them rights which become part of their legal heritage.*"

Regulating gatekeepers serves the public interest by securing welfare and democracy. It also serves the individual rights of (now dead) companies such as Foundem or Ciao and consumers. The rights conferred upon users, in turn, will become part of a new "*digital* legal heritage".

The Commission would ease its own enforcement burden and would give due recognition to market participants if it revised the chapter on enforcement by including, in particular, an article on the handling of complaints and incoming information. For Foundem and the like, time limits would have been vital. Complainants report that at present, in competition proceedings, it is not just unclear whether the Commission will pick up a case, but also when. The whole idea of the DMA, meanwhile, is to speed up enforcement. Nevertheless, the DMA leaves it up to the Commission when to start enforcement action. Streamlining these internal procedures with the help of third parties would probably solve many of the problems associated with enforcement. Therefore, third parties should be included as parties to the proceedings with a formal standing, including access to file and the right to appeal. The Commission should also clarify that damages claims are possible as so-called follow-on claims, to the effect that private litigants can base their claims on Commission findings that are binding for courts.

Getting a right right

The statement from *Van Gend & Loos* seems to suggest that private enforcement is automatically possible, once directly applicable and very concrete obligations are set. The authors of the DMA probably took it as a given. In its Q&As[9] on the DMA, for example, the Commission states that infringements of DMA obligations may result in damages actions in national courts for the companies affected.

Two caveats: Firstly, damages are just one part of private involvement, and a late one, as damages are usually the final element of an enforcement action. Litigation on damages may come years after the infringement, often too late for companies that are severely battered. The other aspects of involvement are not covered.

Secondly, the problems with damages claims in competition law show what it takes to get an individual right right: The devil is in the details. Despite of serious efforts of the European Court of Justice in the landmark cases of *Courage* and *Manfredi*, and a whole set of rules in the 2014 Damages Directive[10], actually getting compensation for victims of cartels is still very hard. Without precedents, patience and supportive legislation there is little hope to succeed.

Decentralise enforcement

There is a fourth aspect of private enforcement that I wish to add: Private parties should be able to claim injunctive relief or prohibition orders against infringements by gatekeepers. This would mean that enforcement could become independent from the European Commission. An alternative path to enforce the obligations of the DMA would open up.

At present, the DMA reads as if it was the exclusive privilege of the Commission to run enforcement actions against gatekeepers. It is unclear whether a national court would even accept an application for prohibiting the violation of a DMA obligation from a private party. Would a competitor like Foundem be able to turn to the Düsseldorf District Court and ask for an injunction against Google's self-preferencing, based on Art. 6 (1) (d) DMA? *Van Gend & Loos* or *Courage* may point to that direction. The Commission, however, does not seem to envisage this. At least, it does not mention this possibility and does not take any precautions for this case (as it did for competition law in Regulation 1/2003[11], where it offers coordination mechanisms for decentralised enforcement).

If there is no alternative to public enforcement by a Commission unit, I have twofold fears:

First, the Commission may easily be overburdened with the workload of gatekeeper regulation. Imagine, the 80 or so Commission staff who must deal with 18 obligations for 5 to 10 gatekeepers with several core platform services each. These corporate groups will be able to mobilise the best legal and economic advice. Imagine just a couple of these cases going to the European Court. In addition, the Commission may wish to run an update of the DMA according to its draft Art. 10. What will be left of enforcement after three years (apart from heavily-stressed Commission officials)?

A second fear is that the political agenda may change. What if a successor of Margrethe Vestager is less keen on taming the tech titans? What if priorities within the Commission shift? Who keeps up enforcement? Private actors seeking injunctions in court and national competition agencies could step in.

Evolutionary gatekeeper regulation

The price to be paid for more actors being involved in enforcement is fragmentation (something that does not go down too well with Art. 114 TFEU, admittedly). This may be cured by channelling private enforcement to specialised European panels, instead of national courts, as Philip Marsden and I suggested last year[12]. "Fragmentation" may even be an opportunity: Private enforcement as an equal second pillar to Commission enforcement opens up a field for regulatory evolution in a decentralised network. This is exactly what we need when venturing into new territories – competition for the best solution.

Foundem, Ciao, and the others that started all this made one mistake: They trusted public enforcement by the European Commission, which took too long. Had they relied on the power of private enforcement, taking Google to court[13], the case would have been resolved much quicker. The mistake to rely too heavily on public enforcement should not be repeated.

This article has originally been published on Verfassungsblog 2021/9/01, https://verfassungsblog.de/power-dsa-dma-05/, DOI: 10.17176/20210901-112941-0.

Rupprecht Podszun holds the Chair for Civil Law, German and European Competition Law at Heinrich Heine University Düsseldorf and is an Affiliated Research Fellow with the Max Planck Institute for Innovation and Competition. He runs the competition law blog www.d-kart.de and is a podcaster with economist Justus Haucap ("Bei Anruf Wettbewerb").

---

[1] European Commission, Case AT.39740 Google Search (Shopping) (2010-2017).
[2] Google Inc., Action in Case T-612/17 *Google and Alphabet v Commission* (11 September 2017).
[3] Governments of France, Germany, and the Netherlands, "Strengthening the Digital Markets Act and Its Enforcement" (2021).
[4] European Competition Network, "Joint paper of the heads of the national competition authorities of the European Union: How national competition agencies can strengthen the DMA" (23 June 2021).
[5] Jürgen Basedow, "Das Rad neu erfunden: Zum Vorschlag für einen Digital Markets Act" (29 January 2021) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773711 accessed 25 September 2021.
[6] European Commission, "Antitrust and Cartel Legislation" https://ec.europa.eu/competition-policy/antitrust/legislation_en accessed 25 September 2021.
[7] Böhm, "Privatrechtsgesellschaft und Marktwirtschaft" (1966) 17 ORDO 75.
[8] ECJ C-26/62 *van Gend & Loos v Netherlands* (1963).
[9] European Commission, "Digital Markets Act: Ensuring fair and open digital markets" https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2349 accessed 25 September 2021.
[10] 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, (2014) OJ L349/1.
[11] 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, (2003) OJ L1/1.
[12] Philip Marsden, Rupprecht Podszun, "Restoring Balance to Digital Competition – Sensible Rules, Effective Enforcement" (2020).
[13] Rupprecht Podszun, "Private Enforcement and platform regulation: Two GAFA-cases – and what they tell us about the Digital Markets Act" (10 June 2021) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3862497 accessed 25 September 2021.

Private Enforcement for the DSA/DGA/DMA Package

Peter Picht

The package consisting of the Digital Markets Act, the Digital Services Act, and the Data Governance Act is about empowering authorities vis-à-vis powerful private market players. Private enforcement is absent in this package, despite its great potential: By engaging in rule enforcement, individuals and companies help to confine key market players' (unlawful use of) economic power, while also counterbalancing a tendency for state agencies to become the sole decision makers on when and how to sanction what they consider undue conduct.

Competition Law Lessons and Beyond

1. Public Enforcement Powers Under the D-Package

Akin to other pieces of regulatory legislation, and more than some of them, the package consisting of the Digital Markets Act[1] (DMA), the Digital Services Act[2] (DSA), and the Data Governance Act[3] (DGA) ("D-Package") is about empowering authorities vis-à-vis puissant private market players. This purpose calls for state enforcement (often also called "public enforcement") powers. Indeed, the D-Package contains a number of public enforcement mechanisms, such as the EU Commission's investigation, sanctioning, and monitoring competencies under Art. 18 et seq. DMA; the powers of the Members States' "competent authorities" to ensure compliance with the DGA per its Art. 13; or the system of interlocking measures by Digital Service Coordinators and the Commission according to Art. 38 et seq., Art. 50 et seq. DSA.

2. Shortcomings of Public Enforcement

However, experiences *inter alia* with state enforcement of competition law caution against too exclusive a reliance on state enforcement: Watchdog resources are limited, and the administrative selection of enforcement priorities may be impaired by the fact that it is not driven by the genuine competitive interests of a market participant. State enforcement of competition law in a multi-layer system of Member State and Union-level agencies and courts can be quite slow and badly synced. The already vivid discussion on how to coordinate the competencies of national competition authorities and the EU Commission under the DMA (see, e.g., the ECN's joint paper[4] on the matter), as well as a glance at the stark contrast between enforcement approaches in the DMA (Commission-focused) and the DSA (Member State-focused, but with the possibility for the Commission to step in), forebode rather more than less difficulties under the D-Package. On a more fundamental level, increasing state enforcement powers may induce an adverse impact on citizens' rights and freedoms. This risk is, arguably, higher in some domains of the D-Package (e.g. removal of content from online platforms

pursuant to the DSA; comprehensive, real-time access to personal and non-personal data under the DMA) than in many a traditional competition law focus.

3. The Rise of Private Enforcement

These and further aspects have caused support for, and of late a steadily increasing relevance of, private enforcement (PE) in EU competition law. Its core element are lawsuits in which companies or individuals harmed by anti-competitive practices seek redress. Where, for instance, customers bought a product at prices inflated by a cartel between producers, they could seek compensation of their damages consisting of (mainly) the delta between the prices actually paid and the hypothetical prices in an undistorted competitive environment. Such lawsuits are brought before civil courts, at the initiative and – initially, subject to later compensation – the cost of the respective claimant. They require, thus, no direct involvement of competition agencies, even though they very frequently rely on findings of infringement made in public enforcement proceedings. Certain developments outside the EU, especially in the US, have kindled fears that PE could be abused, for instance by pressurizing purported infringers into making unjustified settlement payments to avoid the nuisance, bad publicity and costs that even dubious PE litigation may cause. However, such fears have, so far and overall, not materialized in the EU. Elements of its legal framework, preventive in that respect (e.g. loser pays principle for litigation costs, no punitive damages), would loom large in D-Package enforcement as well. At the same time, PE of competition law has made progress – not least through the EU Damages Directive[5] (2014/104/EU) – in solving intricate issues any PE regime faces, such as the principle of full redress, though without overcompensation; quantification of damages and passing-on defense; distribution of liability within a group of perpetrators; access to evidence; the binding effect of state enforcement decisions; and a coherent limitations regime.

PE can make an important contribution to realizing the D-Package's goals (cf. 5. below). Although some of the present approaches to these issues in competition law PE are certainly debatable, the Package should draw on competition law experiences in setting up a PE regime, but it should also try to further improve PE mechanisms beyond the state reached in traditional competition law.

4. Unsatisfactory Rules on PE in the D-Package

Alas, in their present state, the D-Package drafts contain little to this effect. They neither comprise stand-alone provisions on PE nor explicit references allowing for the application of PE legislation outside the Package (such as the Damages Directive). On the contrary, certain language which rather accentuates that the Package is distinct from competition law (such as Art. 9(2) DGA or the exclusive reliance on Art. 114 TFEU as the DMA's legal basis) is fueling a vivid debate on whether competition law's PE mechanisms – and, for that matter, to which extent competition law provisions as a whole – are applicable at all in the realm of the Package (see, e.g., the contributions by Basedow[6], Leistner[7], Podszun et al.[8]).

5. Ways Forward

To remedy this uncertainty, the EU Commission must at least complement the Package Acts with a reference to the Damages Directive that permits the Package to plug, *mutatis mutandis*, into competition law PE.

A – very worthwhile – attempt to improve D-Package PE beyond a mere, unspecific transplant from competition law would, however, require more than that. Among other elements, it should include:

- Fostering PE routes complementary to those under competition law, in particular contract and unfair competition law (cf. also Basedow[9], Leistner[10], though with a more critical view on such additional routes). This implies the availability of a broad range of remedies beyond damages, such as (preliminary) injunctions, contract adaptation, disgorgement of profits, data-specific remedies, but also checks on the abusive enforcement of such remedies. However, legal prongs other than competition law lack, as yet, Union-wide PE harmonization in the style of the Damages Directive. Furthermore, the (sometimes piece-meal) principles developed for the interaction between competition, unfair competition and contract law PE regimes in the realm of traditional competition law cannot necessarily be transplanted to D-Package scenarios without alterations. In consequence, such a multi-prong PE approach must include further guidance, especially to Member State courts which ought not be left to their conjecture. A structured framework for the exchange of practice experiences between these courts would enhance the coordinative effect of such guidance.
- Having "third-party beneficial data intermediaries" (including data sharing service providers in the sense of the DGA), which act in the interest of data subjects and (professional) data recipients under the Package, and assist PE claimants in their ventures. Such intermediaries could contribute, in particular, the expert knowledge on D-Package matters they will likely acquire, but they may also actively intervene in PE proceedings. In a similar vein, regulation should require addressees of obligations under the D-Package, in particular DMA Gatekeepers and "very large online platforms" in the sense of the DSA, to contribute to a workable PE regime, for example, by way of transparency obligations or support of PE actions against third-party offenders using such platforms/Gatekeeper services.
- Moving from a PE function that largely consists in follow-on actions (as is today's reality in competition law) to a more equal, reciprocal role of state enforcement and PE as the first mover approach whose results instruct the respective other enforcement prong. Arguably, only the addition of substantial standalone, first mover PE would fully realize the decentralized Package enforcement via PE. First mover PE may even serve as a valuable filter indicating to watchdogs where to hunt and providing them with helpful information in form of evidence from PE litigation. As said before, market participants may, from their

first-hand experience, know better than state agencies about particularly severe infringements and particularly valuable information for proving them. The proposals made heretofore could further this goal, but also additional elements, including early-on remedies besides damages; rules on burden of proof and information access, which reduce dependence on competition watchdog files for substantiating PE claims; support by intermediaries; reasonable limitation periods; mechanisms which help to overcome claimants' rational apathy, such as the bundled enforcement of individual claims by a third party agent; the creation of specialized alternative dispute resolution bodies (cf. also Podszun et al.[11]). Alternative dispute resolution mechanisms could be particularly well-suited to generate a cross-jurisdictional impact necessary to effectively police digital players acting on a global scale.

- Shielding safe harbours under the Package against PE "surges" – measures duly taken in the fulfilment of Package obligations, or the exercise of Package rights, must, in the main, not generate PE liability. This caveat could, for instance, apply to the provision and reception of data pursuant to Art. 6 (g)-(j) DMA, with regard to an alleged anti-competitive information exchange; to measures aiming at the prevention of unlawful data access or transfer pursuant to Art. 11(5), (7) DGA with regard to an alleged obstruction of competing or dependent undertakings; to mere conduit, caching or hosting activities exempted from liability under Arts. 4-6 DSA with regard to violations of civil, (unfair) competition, or other prongs of law such activities may allegedly constitute.

- Using as a PE opportunity the fact that Gatekeepers (and other key digital market players) are powerful rule-makers for their digital environments. Of course, it must be ensured that Gatekeeper rules align with the goals of state (law) and society, ultimately performing a role subsidiary to them. Subject to this condition, however, Gatekeeper-set rules can support PE, especially when it comes to harm afflicted by one user of Gatekeeper services to another. Where, for instance, the terms and conditions in Gatekeepers' contracts implement appropriate conduct and transparency obligations on their users and business partners, they can serve as workable PE grounds besides state law.

- Conceptualizing, on the doctrinal level, a legal framework that coherently incorporates the aforesaid components of a workable PE regime. This challenging task likely requires a combination of selective references to the Damages Directive and other pieces of legislature, substantial guidance for Member State courts (including inter-court dialogue), and genuine, explicit PE provisions in the D-Package. Provisions in the Acts of the D-Package should, *inter alia*, specify the obligations whose violation gives rise to a broader or narrower set of PE remedies. For damage claims to result from the violation of one of the D-Package's extensive anti-circumvention rules (e.g. Art. 11 DMA), for instance, the fulfilment of qualifying requirements, such as a perpetrator's intent, seems appropriate at least in the early stages of D-Package enforcement. Furthermore, the

D-Package itself offers the preferable place for addressing alternative dispute resolution mechanisms keyed to its particularities.

6. PE and Power

The difficulties of developing PE into a vivid, though well-ordered component of the D-Package are yet another symptom for the lack of a sufficiently robust, harmonized legal framework for such private legal action in Europe. At the same time, improving this aspect of the Package offers the serendipitous chance of a catalytic effect for PE in Europe. This includes PE's potential to contribute to the checks and balances on economic and political power: By engaging in rule enforcement, individuals and companies help to confine key market players' (unlawful use of) economic power. And by taking such enforcement in their own hands, they counterbalance a tendency for state agencies to become the sole decision makers on when and how to sanction what they consider undue conduct. Balancing state as well as corporate power looms particularly large in the digital realm as its technologies – and potentially the control market players or the state exercise through them – increasingly permeate all parts of life and society. All in all, D-Package PE presents an opportunity we should not miss.

This article has originally been published on Verfassungsblog 2021/9/03, https://verfassungsblog.de/power-dsa-dma-09/.

Prof. Dr. Peter Georg Picht, LL.M. (Yale), holds a chair for economic law at Zurich University, heads the University's Center for Intellectual Property and Competition Law, and is an Affiliated Research Fellow with the Max Planck Institute for Innovation and Competition.

[1] European 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)", COM(2020) 842 final.
[2] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[3] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act)", COM(2020) 767 final.
[4] European Competition Network, "Joint paper of the heads of the national competition authorities of the European Union: How national competition agencies can strengthen the DMA" (23 June 2021).
[5] 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, (2014) OJ L349/1.
[6] Jürgen Basedow, "Das Rad neu erfunden: Zum Vorschlag für einen Digital Markets Act" (29 January 2021) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3773711 accessed 25 September 2021.
[7] Matthias Leistner, "The Commission's vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act – A critical primer" (22 March 2021) *SSRN* https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3789041 accessed 25 September 2021.
[8] Philipp Bongartz and others, "The Digital Markets Act: Moving from Competition Law to Regulation for Large Gatekeepers" (2021) 10 Journal of European Consumer and Market Law 60.
[9] *n 6.*
[10] *n 7.*
[11] *n 8.*

Enforcement of the DSA and the DMA – What did we learn from the GDPR?

Suzanne Vergnolle

In trying to overcome the cross-border enforcement's pitfalls of the GDPR, the Commission's proposals for a Digital Services Act and Digital Markets Act are largely expanding the Commission's enforcement powers. Unfortunately, what is touted as a solution for cross-border enforcement issues, might lead to new difficulties and challenges due to the risks of the centralization of power with the Commission.

Remember May 2018, when our mailboxes were full of emails explaining how companies were, as they put it, "better protecting our privacy"? For privacy experts, it was a moment of achievement and excitement: the long-awaited General Data Protection Regulation[1] (GDPR), was *finally* entering into application. This regulation is often presented as a "success story"[2], or as a "model for policymakers"[3]. Unfortunately, the hopes surrounding its effectiveness have gradually allayed. Data protection experts are still desperately waiting to see tangible improvements for peoples' privacy.

Some[4] attribute this to failures from European governments, which are underfunding and understaffing their national data protection authorities (DPAs), while others[5] lament the impracticality of the GDPR's vague language. Most commentators, however, agree on one thing: the one-stop-shop[6] mechanism instituted by the GDPR is ineffective or, at least, broken. The past years have unveiled this mechanism as a slow and inefficient system, which even the European Commission recognized[7] in 2020. We should hope that the Commission is trying, in its most recent regulatory proposals, to avoid repeating the same mistakes.

At a first glance, it might seem so. Both the Digital Services Act[8] (DSA) and the Digital Markets Acts[9] (DMA) put forward new enforcement mechanisms avoiding bottleneck national investigations seen with the GDPR. In a nutshell, the DSA framework organizes the exemption from liability for providers of intermediary services (Article 1 § 1 DSA[10]), and the DMA provides harmonized rules "ensuring contestable and fair markets in the digital sector" (Article 1 DMA[11]).

Both proposals are essentials because they aim at fostering innovation, growth, and competitiveness notably by bridling concentration of private power. However, their success is contingent to a solid and effective enforcement. Otherwise, their principles and rules might remain a toothless tiger and face the same disillusion and criticisms[12] than the GDPR.

In trying to overcome the cross-border enforcement's pitfalls of the GDPR (Part I), the Commission's proposals are largely expanding the Commission's enforcement powers.

By doing so, the institution is fully applying the adage: "you are never as well served as when you serve yourself." Unfortunately, the solutions for cross-border enforcement put forward in both proposals (Part II) might lead to new difficulties and challenges, notably because of the risks of the centralization of power with the Commission.

I. Issues with cross-border enforcement in the GDPR

One reason explaining why the GDPR garnered such attention is the level of fines DPAs can impose on organizations. Article 83 sets forth fines of up to 10 or 20 million euros, and 2% or 4% of the entire global turnover of the preceding fiscal year, depending on the violation.

As of late August 2021, at least 760 fines have been imposed, corresponding to more than 1 billion euros[13]. However, they are unevenly spread out across the European Union. The Irish Data Protection Authority (DPC) has only issued a few fines (less than 10) since 2018[14]. This is concerning as most Big Tech companies have their main establishment in Ireland, making the DPC their lead authority. Per the one-stop-shop mechanism[15], a single lead supervisory authority located in the Member State in which an organization has its "main" establishment must coordinate cross-border complaints and investigations into that organization's compliance with the GDPR. Most of the high-profile cases include cross-border processing of personal data, triggering the application of the one-stop-shop. Currently, a backlog of at least 28 cases[16] against Big Tech firms is under investigation by the Irish DPC. Only two have led to a decision and a fine, increasing the frustration from other DPAs[17] and widespread criticism from NGOs[18] to Members of the European Parliament[19].

A case against WhatsApp illustrates well the difficulties of GDPR's enforcement. When Facebook purchased WhatsApp in 2014, it assured[20] nothing would change for its user's privacy. However, in 2016, WhatsApp announced[21] modifications to its privacy policy, organizing a data sharing with Facebook. The change drew widespread regulatory scrutiny across Europe and some national authorities adopted a decision[22] before the entering into force of the GDPR. Since then, the Irish DPC has been the lead authority investigating the company's compliance with the regulation. In December 2020, the DPC sought feedback from other DPAs on its draft decision but was unable to find a consensus with the other authorities.

Thus, when in early 2021 WhatsApp made another unclear change to its privacy policy[23], regulators' attention sparkled again across Europe. In an emergency proceeding, the Hamburg DPA (the city where Facebook has its German headquarters) banned Facebook from processing WhatsApp users' data. The DPA also put pressure on the European Data Protection Board (EDPB) to intervene and make its emergency order "a binding decision" for all Member States. On July 15, 2021[24], the EDPB denied the emergency nature of the situation and charged the Irish DPC to conduct an investigation, without providing any timeline to do so, infuriating civil society organizations and the Hamburg DPA[25], unable to take matters into its own hands. However, on July 28, 2021, while addressing the merits of the objections of DPAs on the Irish draft decision, the

EDPB required the DPC[26] to adopt its final decision within one month, which finally happened on September 2, 2021[27]. To sum up, a decision impacting the privacy of millions of data subjects takes years to see the light and might not even be addressing the most recent issues of the company's behavior. This case well illustrates how convoluted and ineffective GDPR's enforcement mechanism is.

Originally presented as a necessary tool to foster efficient and coherent GDPR interpretation, the one-stop-shop mechanism has already proven to induce delays in procedure and widespread frustration. It also shows that the inactivity of one single authority can act as a bottleneck and put at risk the rights of all data subjects across Europe. This paralysis may, in part, have informed the recent Court of Justice decision[28] clarifying that non-lead DPAs can initiate legal proceedings before the courts of their own Member States against a company with its main establishment elsewhere in the EU.

If only one lesson is drawn from the GDPR's enforcement scheme it should be that a system centralizing its oversight around one institution should make sure the chosen institution is up for the tasks.

II. Solutions for cross-border enforcement in the DSA and the DMA

Enforcement of the DSA and the DMA might be easier since the scopes of the initiatives are much smaller than the GDPR. In fact, while the GDPR applies indifferently to the public and private sector, the two proposals are only targeting some private organizations (online intermediaries services[29] for the DSA and gatekeeper providers of core platform services[30] for the DMA). Also, while the GDPR applies to all processing of personal data, the DSA mainly targets regulation of online content and the DMA sets out obligations to ensure "contestable and fair markets"[31] across the Union.

As for enforcement, even though the two legislative initiatives adopt different approaches, they both give the European Commission a central role. Another common feature is the various timelines set out by the two initiatives to avoid latency and inertia, which appears as a lesson drawn from the GDPR.

The DMA enforcement mechanism

The enforcement's provisions of the DMA are sitting in Chapter V[32] (especially Article 25 and seq. DMA). Every step – investigation, monitoring, and enforcement powers – is centralized with and conducted by the Commission, granting minimal involvement to Member States. Per article 32 DMA[33], the "Digital Markets Advisory Committee" is a comitology committee[34] whose members will be representatives from the Member States, with referral capacity under Article 33 DMA[35], according to which three or more Member States can request the Commission to open a market investigation. In effect, Member States' role is limited to an advisory function.

As noted by some commentators[36], this centralized approach is rather unusual in the area of EU digital and economic regulation. Whether the Commission puts in place adequate staffing to tackle, all by itself, the extent of the DMA's tasks is yet to be seen. One of the consequences could be a sub-optimal level of enforcement, effectively

reproducing the bottleneck scheme seen with the GDPR. Unfortunately, the DMA does not offer alternative legal action or safeguards to avoid such an outcome. Article 35[37] merely provides the European Court of Justice a limited right to review some of the Commission's decisions (the ones imposing fines or periodic penalty payments).

The DSA enforcement mechanism

Even though the DMA's enforcement relies solely on the Commission, which is *per se* questionable, it has the benefit of providing a clear system. This is not the case for the DSA's enforcement, which involves various actors[38] alongside the Commission in a maze of responsibilities.

Each Member State needs to appoint a Digital Services Coordinator[39] who is responsible for supervising the intermediary services established in their Member State. All providers of intermediary services must designate a "single point of contact" for direct communication or, if they do not have an establishment in the Union, designate a legal representative in one of the Member States in which they offer services (Articles 10 and 11 DSA[40]). Similarly to the one-stop-shop mechanism of the GDPR, the Digital Services Coordinator (DSC) of the provider of intermediary services' main establishment (Coordinator of establishment) has sole jurisdiction (Article 40[41] DSA). However, unlike in the GDPR, the DSA provides strict deadlines for the Coordinator of establishment to answer a request of investigation and enforcement from another DSC or the Board of Member States Digital Services Coordinators (Board). Article 45 § 4[42] DSA requires the Coordinator of establishment to provide its assessment "without undue delay and in any event **not later than two months** following receipt of the request". If this time limit is not met, or if the DSC or the Board does not agree with the assessment, it can refer the matter to the Commission, which shall assess the matter **within three months**. Then, the Commission can send back the matter to the Coordinator of establishment for review, after which it has **two months** to "take the necessary investigatory or enforcement measures". To illustrate, if a matter is referred to the Coordinator of establishment on January 1st, and it passes through all stages, a decision should be made at the latest on August 1st. In comparison, it took more than three years to Luxembourg's DPA to reach a decision against Amazon[43] under the GDPR's enforcement system.

A different enforcement regime is organized for very large online platforms, over which the Commission has direct supervision powers and can, in the most serious cases, impose fines of up to 6% of the global turnover of a service provider. For these platforms, the Commission is the central and main regulator[44]. The Board has a purely advisory role, leaving the Member States outside of this system. If some commentators[45] hope this system may foster efficiency and speediness in oversight procedures and rightly compare it to what already exists in competition law, a more cautious commentator might be alarmed by the risks surrounding such centralization. Excluding Member States from the most serious cases and providing a monopolistic role to the Commission may led to dangerous consequences.

A critical evaluation of enforcement solutions in the DSA and the DMA

If the enforcement mechanisms laid down in the DSA and DMA avoid some of the issues of delays and inertia existing in the GDRP's cross-border enforcement system, they are not exempt of criticisms. Many Member States, including France, Germany, and the Netherlands, have already expressed[46] concerns that the DMA might have negative effects on existing national competition law regimes and their enforcement. In this regard, they asked for clarification on the articulation between the DMA and national competition law. They also asked to grant greater power to Member States.

Foremost, the centralization of power around the European Commission is problematic. First, as discussed above, the DMA places a heavy enforcement burden on the Commission who will need to gather and analyze an enormous amount of data[47], particularly during the launch phase. To be able to meet the extent of its responsibilities, the Commission will have to expand the number of its officials, but also its skillset to include *inter alia* computer and data scientists. The latter absence of technical know-how is already been considered[48] one of the reasons behind GDPR's enforcement failures.

Also, the enforcement powers provided to the Commission put the European separation of powers at stake. Traditionally, the Commission is presented as the executive arm of the European Union. However, its footprint has been expanding both in the legislative and judicial branches – a trend that continues with the DSA and the DMA. Both enforcement mechanisms are highly reliant on the Commission and don't provide an enforcement role to national judiciaries (under Article 41 § 3[49] of the DSA, they are left with a power to renew order restricting access of recipients of the service, which only happens after exhaustion of many other actions). By allowing itself to adopt "non-compliance decisions" (Article 58[50] DSA and Article 25[51] DMA) and impose heavy fines to the organizations (Article 59[52] DSA and Article 26[53] DMA), the Commission is more than the executive arm of the European Union; it is also applying its law and punishing law-breakers, like a court would do. Another element highlighting this role are the procedural rights recognized to the services and gatekeepers, such as the right to be heard and access to the file (Article 63[54] DSA and Article 30[55] DMA). Because the courts are often under-dimensioned or less specialized, it is becoming common in the digital sector to grant enforcement powers outside the court system.

To sum up, the Commission drafted the two initiatives (as the executive branch), will contribute to the legislative discussions (as an involved negotiator), and will be a key actor of their enforcements (as a judge). Such centralization of power can cause long-term democratic problems. As Montesquieu put it: "power curbs power" and it is of the utmost importance to make sure that power is distributed between institutions so they can operate as checks and balances and make sure there is no abuse or corruption of power. Unfortunately, the current system does not enable this.

Also, because the Commission was not created as a judiciary institution, it is not equipped or organized to take up that role. If the regulation stays as it is the Commission will need to drastically evolve or put at risk the enforcement of both regimes. We would not want latency, inertia, and blind eyes to become a common feature of the enforcement of European Digital Regulations.

In conclusion, what did we learn from the GDPR? Apparently, not enough. Both the DSA and DMA are centralizing most of their enforcements around one institution, the Commission. To avoid facing similar issues of latency and inertia, it seems crucial to better involve Member States, while providing a swift timeline for their contribution, and probably provide the judicial power with a bigger role. Fortunately, the proposals being still under negotiation, lots of refinements could still be made.

This article has originally been published on Verfassungsblog 2021/9/03, https://verfassungsblog.de/power-dsa-dma-10/.

Dr. Suzanne Vergnolle is a Post-Doctoral Fellow at the Swiss Institute of Comparative Law and the University of Lausanne.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), (2016) OJ L119/1.
[2] European Commission, "GDPR the fabric of a success story" (June 2020).
[3] Trevor Butterworth, "Europe's tough new digital privacy law should be a model for US policymakers" 23 May 2018 *Vox* https://www.vox.com/the-big-idea/2018/3/26/17164022/gdpr-europe-privacy-rules-facebook-data-protection-eu-cambridge accessed 25 September 2021.
[4] Brave, "Europe's governments are failing the GDPR" (April 2020) p 3.
[5] Chris Jay Hoofnagle and others, "The European Union general data protection regulation: what it is and what it means" (2019) 28 Information & Communications Technology Law 65.
[6] European Commission, "What happens if my company processes data in different EU Member States?", https://ec.europa.eu/info/law/law-topic/data-protection/reform/rules-business-and-organisations/enforcement-and-sanctions/enforcement/what-happens-if-my-company-processes-data-different-eu-member-states_en accessed 25 September 2021.
[7] European Commission, "Data protection as a pilar of citizens' empowerment and the EU's approach to the digital transition – two years of application of the General Data Protection Regulation" (communication), COM(2020) 264 final.
[8] European Commission, "Proposal for a Regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC", COM(2020) 825 final.
[9] European 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)", COM(2020) 842 final.
[10] *n 8* p 44.
[11] *n 9* p 33.
[12] Adam Satariano, "Europe's Privacy Law Hasn't Shown Its Teeth, Frustrating Advocates" (27 April 2020) NY Times https://www.nytimes.com/2020/04/27/technology/GDPR-privacy-law-europe.html accessed 25 September 2021.
[13] GDPR Enforcement Tracker, https://www.enforcementtracker.com/?insights accessed 25 September 2021.

[14] Irish Data Protection Commission, "Annual Report 2020" (2021) p 48.
[15] *n 6*.
[16] Scott Ikeda, "Outgoing Privacy Commissioner Calls GDPR 'Broken,' Says That Basic Model 'Can't Work'" (1 July 2021) *CPO Magazine* https://www.cpomagazine.com/data-protection/outgoing-privacy-commissioner-calls-gdpr-broken-says-that-basic-model-cant-work/ accessed 25 September 2021.
[17] *n 16*.
[18] Access Now, "Three years under the EU GDPR – An implementation progress report" (May 2021).
[19] Samuel Stolton, "MEPs rue lack of GDPR sanctions issued by Irish data authority" (26 March 2021) *Euractiv* https://www.euractiv.com/section/data-protection/news/meps-rue-lack-of-gdpr-sanctions-issued-by-irish-data-authority accessed 25 September 2021.
[20] WhattsApp Blog, "Facebook" (19 February 2014) https://blog.whatsapp.com/facebook/?lang=en access 25 September 2021.
[21] WhattsApp Blog, "Looking ahead for WhatsApp" (25 August 2016) https://blog.whatsapp.com/looking-ahead-for-whats-app?lang=en accessed 25 September 2021.
[22] Michaela Ross, "Facebook, WhatsApp Fined by Spain for Failure to Obtain Consent" (16 March 2018) *Bloomberg Law* https://news.bloomberglaw.com/business-and-practice/facebook-whatsapp-fined-by-spain-for-failure-to-obtain-consent accessed 25 September 2021.
[23] Raphaël Grably, "Pour Whatsapp, le profit aux dépens de la confidentialité des données" (10 February 2021) *BFM Business* https://www.bfmtv.com/tech/pour-whats-app-le-profit-aux-depens-de-la-confidentialite-des-donnees_AD-202102100095.html accessed 25 September 2021.
[24] European Data Protection Board, "Urgent Binding Decision 01/2021 on the request under Article 66(2) GDPR from the Hamburg (German) Supervisory Authority for ordering the adoption of final measures regarding Facebook Ireland Limited" (12 July 2021).
[25] Hamburg Commissioner for Data Protection and Freedom of Information, "Press Release: Data exchange between WhatsApp and Facebook remains unregulated at European level" (15 July 2021) https://datenschutz-hamburg.de/assets/pdf/2021-07-15_EDSA_FB_en.pdf accessed 25 September 2021.
[26] European Data Protection Board, "EDPB adopts Art. 65 decision regarding WhatsApp Ireland" (28 July 2021) https://edpb.europa.eu/news/news/2021/edpb-adopts-art-65-decision-regarding-whatsapp-ireland_en accessed 25 September 2021.
[27] Irish Data Protection Commission, "Data Protection Commission announces decision in WhatsApp inquiry" https://www.dataprotection.ie/en/news-media/press-releases/data-protection-commission-announces-decision-whatsapp-inquiry accessed 25 September 2021.
[28] Heidi Waem, Simon Verschaeve, "EU: What's left of the GDPR's one-stop-shop? CJEU clarifies competences of non-lead data protection authorities" (5 July 2021) *DLA Piper* https://blogs.dlapiper.com/privacymatters/eu-whats-left-of-the-gdprs-one-stop-shop-cjeu-clarifies-the-competences-of-non-lead-data-protection-authorities/ accessed 25 September 2021.
[29] *n 8* p 45.
[30] *n 9* p 37.
[31] *n* 9 p 34.
[32] *n 9* p 48.
[33] *n 9* p 54.
[34] European Commission, "Comitology" https://ec.europa.eu/info/law/law-making-process/adopting-eu-law/implementing-and-delegated-acts/comitology_en accessed 25 September 2021.
[35] *n 9* p 55.
[36] Damien Geradin, "DMA proposal: Should there be a greater role for the Member States?" (7 April 2021) *The Platform Law Blog* https://theplatformlaw.blog/2021/04/07/dma-proposal-should-there-be-a-greater-role-for-the-member-states/ accessed 25 September 2021.
[37] *n 9* p 55.
[38] Crowell & Moring, "Digital Services Act: The European Commission Proposes An Updated Accountability Framework For Online Services (12 January 2021) https://www.crowell.com/NewsEvents/AlertsNewsletters/all/Digital-Services-Act-The-European-Commission-Proposes-An-Updated-Accountability-Framework-For-Online-Services accessed 25 September 2021.
[39] *n 8* p 68.
[40] *n 8* p 50.
[41] *n 8* p 69.
[42] *n 8* p 74.

[43] Stephanie Bodoni, "Amazon Gets Record $888 Million EU Fine Over Data Violations" (30 July 2021) *Bloomberg* https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach accessed 25 September 2021.
[44] Ben Wagner, Heleen Janssen, "A first impression of regulatory powers in the Digital Services Act" (4 January 2021) *Verfassungsblog* https://verfassungsblog.de/regulatory-powers-dsa/ accessed 25 September 2021.
[45] *n 47*.
[46] Governments of France, Germany, and the Netherlands, "Strengthening the Digital Markets Act and Its Enforcement" (2021).
[47] Damien Geradin, "The DMA proposal: Where do things stand?" (27 May 2021) *The Platform Law Blog* https://theplatformlaw.blog/2021/05/27/the-dma-proposal-where-do-things-stand/ accessed 25 September 2021.
[48] *n 4*.
[49] *n 8* p 71.
[50] *n 8* p 81.
[51] *n 9* p 50.
[52] *n 8* p 81.
[53] *n 9* p 51.
[54] *n 8* p 83.
[55] *n 9* p 53.

Max Planck Institute for Innovation and Competition Research Paper Series

ISBN 978-3-00-070284-6