Edited by
Joris van Hoboken, João Pedro Quintais, Naomi Appelman,
Ronan Fahy, Ilaria Buri & Marlene Straub

Putting the DSA into Practice

Enforcement, Access to Justice and Global Implications

Verfassungsbooks
ON MATTERS CONSTITUTIONAL

Contents

Imprint	3
Title	4
Foreword	6
Contents	17
Will the DSA Work?: On Money and Effort	20
Between Preservation and Clarification: The Evolution of the.	36
The DSA Fails to Reign in the Most Harmful Digital Platform.	52
Why the DSA Could Save Us From the Rise of Authoritarian.	64
A Regulator Caught Between Conflicting Policy Objectives:.	76
Platform Oversight: Here is what a Strong Digital Services Co.	92
Fundamental Rights Impact Assessment in the DSA	108
An Intersectional Lens on Online Gender-Based Violence and.	122
Now What: Exploring the DSA's Enforcement Futures in Rela.	136
If You Build it, They Will Come: The DSA ``Procedure Befor.	152
Remedying Overremoval	168
Contextualisation over Replication: The Possible Impacts of t.	184
Regulating Influence, Timidly	200
The DSA as a Paradigm Shift for Online Intermediaries' Due.	212
The European Union's New DSA and the Rest of the World	228

DOI 10.17176/20230208-093135-0
ISBN Print 978-3-757517-96-0

Verfassungsblog gGmbH
Großbeerenstr. 88/89
10963 Berlin
verfassungsblog.de
info@verfassungsblog.de

Cover design by Carl Brandt
© 2023 belongs to the authors

This work is licensed under the Creative Commons Attribution-ShareAlike 4.0 International License. To view a copy of this license, visit creativecommons.org/licenses/by-sa/4.0/.

This book was realized thanks to funding by the Digital Legal Studies initiative, an interuniversity research program on law and digital technologies in the Netherlands, and the Institute for Information Law (IViR). The DSA Observatory is supported through funding by the Open Society Foundations and the Civitates initiative for democracy and solidarity in Europe. The work of João Pedro Quintais in this book is further funded by his VENI Project "Responsible Algorithms: How to Safeguard Freedom of Expression Online" funded by the Dutch Research Council (grant number: VI.Veni.201R.036).

Edited by
Joris van Hoboken, João Pedro Quintais, Naomi Appelman,
Ronan Fahy, Ilaria Buri & Marlene Straub

Putting the Digital Services Act into Practice

Enforcement, Access to Justice, and Global Implications

Verfassungsbooks
ON MATTERS CONSTITUTIONAL

Foreword

Coinciding with the European Union (EU)'s Digital Services Act (DSA)'s publication in the Official Journal of the European Union on 27 October 2022, the University of Amsterdam's DSA Observatory and Verfassungsblog hosted an online symposium, on "Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications". The contributions are collected in this publication.

The DSA is intended as the EU's landmark piece of legislation for addressing illegal and harmful content and activity online. Its official publication marks the end of a years-long drafting and negotiation process and opens a new chapter: that of its enforcement, practicable access to justice, and potential to set global standards. This symposium critically interrogates the DSA's portrayal as Europe's new "Digital Constitution", intended to affirm the primacy of democratic rulemaking over the private transnational ordering mechanisms of Big Tech. While it extends the e-Commerce Directive's core principles for the regulation of online services that handle third-party content and codifies existing self-regulatory practices initiated by online platforms, it also introduces significant legal innovations: a tiered system of due diligence obligations for intermediary services, the regulation of content moderation through terms of service enforcement, systemic risk assessment obligations for the most widely used platforms and search engines, and access to data for researchers. In sum, with the DSA, the EU aims once again to set a global standard in the regulation

of the digital environment. But will the DSA be able to live up to its expectations, and under what conditions?

Throughout this publication, you will encounter leading experts' answers to these and related questions and will be left with even more. If there was a central theme throughout the contributions, it would be that the DSA is only the beginning of what will be an uphill battle. The contributions focus on the predicted outcome of the DSA in three main themes: (i) the implementation and enforcement of the DSA; (ii) access to justice in relation to content moderation processes; and (iii) international impact and what standards the DSA may be furthering globally.

Implementation and enforcement of the DSA

A crucial aspect of the success of the DSA relates to the application of its due diligence requirements in practice and the effective implementation of its enforcement framework. The enforcement framework includes a combination of new regulatory authorities at the national (Digital Services Coordinators) and EU level (as part of the European Commission). As underlined by many experts (particularly civil society and academics), these elements will be decisive as to whether the DSA will deliver on its goals, and whether its rules will be capable of meaningfully protecting fundamental rights. In the long run, the question of legitimacy will be particularly important. Will the national authorities in charge of overseeing the regulation of content moderation processes, an area perhaps even more

contested than online privacy, be broadly accepted by market players and the general public?

As shown by the General Data Protection Regulation (GDPR), ambitious substantive rules are nothing but a "paper tiger" without effective enforcement. Serious failures in the GDPR's enforcement have clearly influenced the debate around the DSA's enforcement chapter. In effect, the DSA opts for more centralized enforcement against the most powerful platforms by the European Commission and includes strict deadlines for Digital Services Coordinators and the Commission to act.

At the national level, the EU member states must decide how to position and equip their national regulators. Dealing with this hot potato of regulatory competence will not be easy, as the DSA cuts across media law, telecommunications regulations, consumer protection, data protection, intellectual property and criminal law. Some countries may decide to create new regulatory agencies in the process, while others may allocate the relevant oversight tasks to (a possible combination of) existing agencies. Pragmatism, path dependency and national particularities may open a plethora of institutional approaches to putting the DSA into action.

Given the profound fundamental rights implications of the DSA, the choice of further developing the European Commission into the most important regulatory authority for online content governance deserves continued debate and scrutiny. In the area of platform regulation, the Commission is not an independent regulatory authority, but the executive branch of

the EU, which put forward the DSA proposal and played an active role in its negotiation and finalization. As the Commission might be assigned enforcement functions in future pieces of legislation, the DSA's supervision and enforcement architecture raises constitutional issues relating to independence and the separation of powers, which are also highly relevant beyond the DSA debate.

Other stakeholders (users, researchers and civil society organizations) are also given a significant role to play in the DSA enforcement architecture. Vetted researchers, for instance, will be able to gain access to platform data to investigate relevant harms and dynamics connected to platforms' operations. One of the most relevant questions concerns whether the DSA provides these actors with adequate tools to contribute meaningfully and effectively to the enforcement of its rules, particularly from a fundamental rights perspective.

Finally, the DSA also regulates content moderation practices based on terms of service and requires intermediaries to moderate transparently, proportionately, and with due regard to the fundamental rights and interests of users and other stakeholders. The precise interpretation of this new provision, which builds on the horizontal effect of fundamental rights between users and online services, will involve complex balancing requirements and an interplay between national constitutional safeguards and the EU.[1]

Access to justice and content moderation

One of the main policy goals of the DSA is to create a safer online environment. It is one thing for the DSA to provide new mechanisms to address online harms, it is another for those to deliver on their promise in practice. Whether this goal is met will depend on whether the DSA succeeds in offering adequate access to justice to people confronted with online harm. In this regard, codification of the notice and takedown and complaint mechanisms can be seen as a step forward. However, it is an open question to what extent this offers sufficient remedies, given the breadth of online harms the DSA addresses. For example, whether the DSA can provide individual or collective opportunities to contest terms and conditions remains to be seen. The matter is further complicated by the fact that substantial barriers to justice often prevent meaningful access to complaint and redress mechanisms or remedies. Ultimately, effective remedies against online harm and abuse will remain dependent on the platform's implementation of the DSA requirements, and on national particularities of procedural law more generally.

Even though it is clear that the impact of online harms is spread unevenly, it is still insufficiently understood what online harms are faced by different (marginalized) groups, how these harms differ and intersect, and where access to justice and opportunities for the contestation of platform practices are needed. In particular, various types of unlawful content (such as harassment or racism), as well as over-removals or

bans, disproportionately harm marginalised communities. For the DSA to succeed in contributing to a healthy digital environment for all, it will be essential to understand these different needs, and involve civil society organisations representing these interests in the implementation and enforcement debate.

International implications of the DSA

Finally, EU regulation has an undeniable impact beyond European borders. The so-called "Brussels effect" – the ability of the EU to shape global standards by exercising its regulatory power – has been a distinctive feature of earlier EU law, particularly of the GDPR. Since its announcement, discussions about the DSA proposal have been accompanied by the awareness that the DSA may have a profound regulatory resonance on a global level. US-based platform regulation experts and policymakers have thus followed the DSA debate closely, perhaps not least because the largest platforms more heavily regulated under the DSA mostly originate from Silicon Valley.

The same issues and societal risks that the DSA seeks to address are affecting – perhaps even more significantly, and with additional complexities – countries outside the EU borders. The possible adoption of DSA standards outside the EU raises the question of whether these rules, if implemented, could help advance the platform regulation efforts elsewhere, as well as promote fundamental rights and other democratic values. At the same time, the DSA's approach could pose risks

in less democratic countries, particularly in light of the civil society critiques of some aspects of the DSA, including the centralization of certain enforcement powers.

The line between the safeguarding of fundamental freedoms and democratic values online versus regulatory competition with other regions is thin. A question which thus accompanies discussions on the DSA's extraterritorial effects is, fundamentally, why the EU is attempting to set international standards, and whether it does so mindful of possible collateral effects.

A preview

In the days after the DSA was officially published, the necessity and urgency of its rules became abundantly clear. Among other events, Elon Musk bought Twitter, raising questions about the implications of platform ownership and discretion in governance. Against this backdrop, more than a dozen expert authors spanning policy, academia, and civil society across five continents critically addressed some of the questions sketched out above, while raising many more. Martin Husovec lays the foundations: he foregrounds that the DSA's success depends primarily on societal structures that the law can only foresee and incentivize but cannot build; only people can. Husovec explores how people – from consumer protection groups to research communities – can be supported in building bottom-up enforcement structures. Conversely, Folkert Wilman looks at the DSA through the lens of the Court of Justice of the European Union (CJEU)'s top-down jurisprudence on the e-Commerce Directive. It may appear as if the

DSA had simply preserved and codified the status quo made by case law. However, in terms of the intermediary liability framework, a notable evolution has taken place. Despite such evolution, Sebastian Becker Castellaro and Jan Penfrat contend that the DSA misses the bigger picture: not even the most carefully designed content moderation policy will protect us from harmful online content, as long as we do not address the dominant, incredibly damaging surveillance business model of most large tech firms. As such, they argue, the DSA is useful but falls short of its stated goal. Alexandra Geese disagrees. She similarly identifies the business models of dominant social media platforms as drivers of the rise of authoritarian regimes worldwide – algorithmically amplified into visibility and success – but is optimistic that the DSA tackles the information asymmetry which allows platforms to polarize and for online harms to spread. The crucial legal tools she highlights are audits, risk assessments and researcher access to data. The European Commission's role as a central enforcement authority, meanwhile, is cause for concern.

Ilaria Buri shows that while the DSA's design clearly learned from the experience with enforcing the GDPR, this role by the Commission - already dealing with conflicting policy objectives - raises fundamental questions about the institutional separation of powers. In this context, Julian Jaursch shows why it is crucial that member states get their design choices for strong Digital Services Coordinators right, and what they must take into account. With a strong Digital Services Coordinator, Jaursch shows, the DSA's enforcement – hence its overall suc-

cess – stands and falls. Alessandro Mantelero scrutinises the fundamental rights impact assessments foreseen by the DSA; the risk-based approach adopted is not supported by adequate models, and existing frameworks from human rights impact assessments contexts are limited when extended to the digital context. In her contribution, Asha Allen invokes intersectionality in the risk assessment context. Although the DSA highlights the risk of online gender-based violence, however, its approach to addressing such risks must adopt an intersectional methodology, without which mitigation measures and access to remedies will fail to provide the necessary mechanisms for those most acutely impacted by these rights violations.

"Now what?" asks Catalina Goanta; how shall we approach the DSA's omissions? She explores native advertising in the influencer economy on digital platforms and highlights how it currently falls in a grey area, between the DSA and sectoral regulation. Pietro Ortolani explores the DSA's "Procedure Before Substance" approach to content moderation. Rather than pursuing any major harmonization of the substantive law applicable in this very broad and porous area, the DSA concentrates on proceduralising access to justice on and off digital platforms. Whether this approach will pay off is unknown. Aleksandra Kuczerawy turns to a central lesson the DSA has learnt from the e-Commerce Directive. The Regulation codifies three avenues for access to justice in the case of unwarranted content restrictions, to be used in sequence or separately: internal complaint-handling mechanisms, out-of-court dispute settlement and judicial redress. While they appear comprehensive

on paper, the practice may be another story. Tomiwa Ilori looks at the DSA from a pan-African perspective and treats it with cautious optimism. Although the DSA's precedents may have a Brussels Effect in Africa, it will only be positive insofar as local contexts are foregrounded in the transposition. Relatedly, Nayanatara Ranganathan shows that while the DSA has set its sights on recommender systems and "influence", it sidesteps the crucial operative question that characterizes online advertising: how and why advertisements reach who they reach. Nicolo Zingales looks at the DSA's meta-regulatory approach to regulate self-regulation among very large online platforms. Even though this shift should be welcomed for enabling reflexive and adaptive regulation, we must also be weary of its risk of collapsing in the absence of well-resourced and independent institutions. Finally, Daphne Keller considers "the good", "the bad" and "the future" of how the DSA will be received outside of the EU. While the procedural turn may set positive impulses, the rest of the world should see the DSA as no more than a starting point.

Together, these contributions provide a much-needed first critical reflection on the core aspects of the DSA, the centrepiece of EU platform regulation, that is bound to play a crucial role in the governance of online content moderation and fundamental rights in years to come.

The editors

References

1. On this topic, see João Pedro Quintais and Naomi Appelman and Ronan Fahy, "Using Terms and Conditions to Apply Fundamental Rights to Content Moderation" (2022) German Law Journal <https://ssrn.com/abstract=4286147>.

Contents

Will the DSA Work?: On Money and Effort
Martin Husovec 19

Between Preservation and Clarification: The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law
Folkert Wilman 35

The DSA Fails to Reign in the Most Harmful Digital Platform Businesses - But It Is Still Useful
Sebastian Becker and Jan Penfrat 51

Why the DSA Could Save Us From the Rise of Authoritarian Regimes
Alexandra Geese 63

A Regulator Caught Between Conflicting Policy Objectives: Reflections on the European Commission's Role as DSA Enforcer
Ilaria Buri 75

Platform Oversight: Here is what a Strong Digital Services Coordinator Should Look Like
Julian Jaursch 91

Fundamental Rights Impact Assessment in the DSA
Alessandro Mantelero 107

An Intersectional Lens on Online Gender-Based Violence and the DSA
Asha Allen 121

Now What: Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising
Catalina Goanta 135

If You Build it, They Will Come: The DSA "Procedure Before Substance" Approach
Pietro Ortolani 151

Remedying Overremoval
Aleksandra Kuczerawy 167

Contextualisation over Replication: The Possible Impacts of the DSA on Content Regulation in African Countries
Tomiwa Ilori 183

Regulating Influence, Timidly
Nayanatara Ranganathan 199

The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence: Hail To Meta-Regulation
Nicolo Zingales 211

The European Union's New DSA and the Rest of the World
Daphne Keller 227

Martin Husovec

Will the DSA Work?

On Money and Effort

The Digital Services Act (DSA) is an ambitious project. It constrains private power to protect the freedom of individuals. Arguably, it is based on ordoliberal thinking that if competition does not discipline private power enough to facilitate individual freedoms, the state must intervene to prescribe basic rules of the game to constrain it; competition can do the rest. Wisely, the DSA shifts away from the unproductive debate about liability for third-party content as the only policy lever to achieve change. Instead, it moves the conversation to accountability for how systems enabling risks are being designed.

The DSA has many components but, in its essence, it is a digital due process regulation bundled with risk-management tools. It creates universal due process guarantees, invites transparency to private decision-making and institutionalizes constant risk management by larger players. Europeans gain enforceable procedural rights owed to them by private parties operating the digital ecosystem. Regulators gain tools to hold such providers accountable for what science tells us goes wrong with their designs. Victims, NGOs, and industries gain tools to better enforce their rights at scale.

But will these tools work?

The rulebook is there. It is a tremendous achievement. But setting the rules of the game does not mean we also master its outcomes. The real struggle begins now. My main concern about the DSA resides also in its strength – it relies on *societal structures* that the law can only foresee and incentivize but cannot

build; only people can. These structures, such as local organisations analysing threats, consumer groups helping content creators, and communities of researchers, are the only ones to give life to the DSA's tools. They need to be built bottom-up and sometimes locally in each Member State. If their creation fails, the regulatory promises might turn out to be a glorious aspiration. How to avoid that?

Here is my to-do list.

We need a vibrant community of specialized trusted flaggers, consumer associations, dispute resolution bodies, content moderation professionals and content creators. We need their joint efforts to standardize what makes sense. We need to educate Europeans about their new rights and scientists about their newly gained tools to conduct research. We need to invest money and energy. And finally, we need a mixture of private and public enforcement to make the DSA a success story. Let me address each of these points one by one.

Local trusted organisations

Why are local organizations key? Let me illustrate this with the example of trusted flaggers (Article 22). The DSA grants them preferential treatment when they notify problematic content – but only if they have a track record of quality – that is precision in targeting what is illegal.

The unique European challenge for the DSA is that such organizations must almost always be local. Excellent German

consumer organisations are unlikely to help Spanish-speaking consumers. Devoted Dutch anti hate speech groups will not have the skills to find and notify Romanian content. Skilled Estonian groups fighting against hybrid threats will not help in Slovakia. Thus, the capacity needs to be built up across all Member States to fight all the unique challenges of today, ranging across various forms of extremism, terrorism, war propaganda, hate speech and beyond.

For quality and predictability to emerge from chaos, local organisations are indispensable. Without trusted flaggers, there will be fewer trusted notices and fewer good decisions. But we should also be honest. To achieve quality in the enforcement through such local players, they cannot operate on a shoestring budget. Various actors must help facilitate their work: service providers by providing them with the right interfaces and help with standardization of how notices are exchanged (Articles 16(1), 44(1)); local authorities and citizens by investing and supporting their work; researchers by providing them with the right tools and insights.

It should be in everyone's interest to help such organisations in their efforts to improve and grow. No one was helped by the wasteful practices of the past when the low quality of notices was a crime without punishment. The DSA is a chance to reward betterment: helpful notifiers get carrots, bad actors get sticks (Article 21(5), Article 22(1), Article 44(1) *versus* Articles 23(2), Article 22(6), Article 21(5)).

It is not enough to invest in regulators. Member States and citizens must also invest in their *local* civil society. The legis-

lators were warned very early about this. We cannot look away from the problem of funding and simply hope for the best.

Individuals must actively use the tools

This brings me to the role of individuals. I do not expect that all Europeans will read the DSA provisions before going to sleep – though, as the famous GDPR app shows, it can be therapeutic.

But it is inescapable that only those Europeans who are aware of their rights can properly enforce them. The DSA assumes active individuals. The DSA gives recipients of some services a right to understand how content moderation decisions are made, obtain an explanation of each decision, appeal it internally within the service and get a second opinion from experts (Articles 17, 20, 21). Users and notifiers can also ask for help from consumer associations and other non-profit groups (Article 86). They gain various tools of transparency to demystify how impactful digital services operate and make content moderation decisions. For instance, they can browse through explanations given to those whose content is removed (Article 17(5)) and view aggregate statistics (Articles 15, 24, 42); for VLOPs, parents will be able to read the reports about how they mitigate risks posed to their children (Article 42(4)). Granted, average parents will not read such reports. But many devoted journalists (and perhaps some academics) can read it for them.

The DSA tries to overcome the prototypical problem of user apathy by empowering users to defend themselves by two means. First, it grants them a fast, cheap, and much more

credible remedy than just internal re-assessment. Second, it invites consumer associations to assist them when seeking redress.

If the internal content moderation processes fail, the affected users or notifiers can obtain a second expert opinion issued by out-of-court dispute settlement bodies (Article 21). Where some people see "de facto courts",[1] I see a second external expert opinion. On the micro level, the dispute settlement bodies give users a fast and cheap remedy to seek redress by asking external experts. On the macro level, due to its payment structure, this regime incentivizes providers to make fewer mistakes because each mistake costs them money and reputation. When these small costs pile up, they might become significant to force changes in providers' systems and rules.

And let's be clear. The DSA does *not* take away all the power from platforms. It does mostly *not* limit what legal content can be prohibited by providers under their community guidelines – that is a power that providers retain. Thus, if providers do not like how out-of-court bodies read their rules, they can change them and make them clearer. But once they put the rules in black and white, they cannot claim to be orange without actually changing them. The DSA limits only some grossly unfair policies (Article 14). Thus, if vague clauses serve only to enforce grossly unfair outcomes, there is now a stick that can be relied upon by individuals.

All the talk about out-of-court bodies as de facto courts in my view clouds the most important point of their existence. If regulators do a good job in monitoring and certifying these

bodies – which is undoubtedly crucial, the DSA can constrain a private power in a significant way without limiting a platform's rulemaking. It promises individuals to get an interpretation of these rules by someone who has *not* written them and has no clear stake in individual outcomes. Impenetrable jargon in the terms and conditions will not be the provider's advantage anymore (Article 14). Moreover, the DSA embeds consumer associations in such processes (Article 86). It thereby allows more expertise to enter the conversation in the open, and even gives organisations tools to defend individuals who lack means and expertise – whether as notifiers or content creators (Articles 86 and 90).

To be sure, the goal of this tool is not to eradicate mistakes – to disagree is part of human nature. Even if it works it can only minimize mistakes, reduce their arbitrariness, and improve the legitimacy of the underlying decision. But for activities on such an industrial scale, this is probably the best outcome we can hope for.

Without active individuals who invoke their rights, none of this will work. Consumers and other groups can do a lot to empower individuals by making them aware of their rights.

The DSA's heroes: Researchers

The success of the DSA's risk management rulebook for very large online platforms (VLOPs) and very large online search engines (VLOSEs) is probably the most open-ended. But instead of emphasizing how amazing the regulators must be – which

is surely true – I want to put the spotlight on my DSA heroes: the researchers.

While regulators are crucial, they will do little if they do not have sparring partners among researchers who help them to distinguish yellow press headlines from real causes of problems.

The DSA tries to create a tool to manage all kinds of risks. Systemic risks stemming from content moderation, recommender systems, advertising and other parts of the design of services must be reviewed for how they de-risk the distribution of illegal content, impact fundamental rights and some other protected interests (Article 34). By trying to be future-proof, the risk management mechanism remains very broad and gives out little detail about methods by which to investigate systemic risks. Moreover, unlike in other narrow sectors, here the relevant risks are to an individual, communities and society at large – so basically everything we cherish.

Starting from scratch can overwhelm and disorientate regulators as to what the enforcement priorities should be and how to deal with them. And this is where researchers are key.

Researchers can help to identify what counts as a risk (Article 40(4)). In effect, they help to shape the agenda[2] for regulators and providers of digital services. They also monitor and assess those risks, their causes and contributing factors, and suggest methods and tools to mitigate them. Their suggestions have direct relevance to providers' compliance with the DSA. To be able to do so, they require special access to any data held by providers on a project basis (Article 40(8)). Such

access cannot be easily refused by providers or regulators (Article 40).

The DSA thus changes the norm:[3] now researchers pick their projects and platforms, not the other way around. And once the research shows some risks, their causes, or suggests a way forward, it cannot be ignored by providers or regulators (Articles 40(4)).

But this tool's Achilles heel lies also in funding. The researchers engaging in such data-intensive projects need money to be able to conduct them properly and independently. If the only funding available to do research comes from the industry, even if remotely, we have a problem.

European academia needs specific grants for researchers who want to make use of the data opened up by the DSA. However, the financial support must be equally independent of the authorities that act as regulators. Researchers cannot act as a check on the abuse of state power exercised by regulators if they also need funding from the same authorities.

If the funding to conduct the risk-mitigation research is indispensable, controlling the funding means controlling the access to data. Thus, if the only funding comes from regulators or the industry, we risk again that *someone* will set research priorities for us.

DSA as a baseline, not the only standard

When celebrating the due process rights in the DSA, we should not forget about its blind spots too. Infrastructure providers are subject to only very light due diligence obligations. Superusers, such as influencers, and trusted content creators, such as journalists, academics, and others, are not offered stronger rights although they might need them. But this per se is not an issue as long as the DSA's due diligence obligations are not perceived as the final world – the golden standard that may not be exceeded. Many, not all, blind spots can be overcome by DSA-plus agreements or practices. To the extent that they are not anti-competitive, they should be encouraged.

Let me offer an example. To individual users acting as content creators, such as influencers, artists, bloggers, and hobbyists, the DSA grants rights to defend their life's work. Such content will be soon protected by due process requirements against allegations made by others.

Until now, the incentives were mostly lined up in the opposite direction[4] – that is to remove their content whenever there is a potential legal risk. The DSA prescribes the steps and processes for platforms to follow. If a notice is received, it must be examined, decided, and explained with care (Articles 14, 17, 20). This does not necessarily always mean by humans, but with an eye on the accuracy of the aggregate decisions. But the DSA still assumes that most of the content is equally important and that all mistakes are equally problematic. For the universal due process obligations, this stance is understand-

able. However, it should not imply that content creators might not be afforded stronger procedural rights. Why shouldn't investigative journalists in war zones be better protected against abuse or takedown?

While the DSA does not explicitly provide incentives for content creators to team up, if they set up organizations, they can collectively negotiate to gain extra procedural rights for their content as trusted sources.[5] The DSA provides a place for such agreements in the Codes of Conduct, which have regulatory relevance (Articles 45, 37(1), 35(1), and even Article 14).

The DSA should be a (baseline) standard, not the only standard. It should be a trigger for co-regulation and competition on top of the basic rules.

Private and public enforcement

Finally, and importantly, enforcement will not happen overnight. Public authorities need resources, and the European Commission needs strong partners in the Member States. There will always be too few officials chasing too many problems. But coordination among member States can help to pool resources and avoid needless duplication. For instance, the Russian war propaganda, using the same techniques across the continent, is surely better fought together, even though the local threats can slightly differ. The regulatory initiatives around the GDPR suggest that the cooperation of national authorities in the digital space is possible. There is no reason to doubt that the same can happen around the DSA. However, the vastness of

challenges covered by the DSA should not be underestimated. The DSA offers baseline expectations, toolkits, and vocabulary – but it will take many experts with different skills to construct a healthy digital public sphere.

That being said, I still think that without private enforcement, the DSA risks, at least in some areas, causing similar dissatisfaction as GDPR enforcement. The DSA has undoubtedly learnt from the GDPR's shortcomings in many ways, such as its institutional design and stronger risk-auditing systems. However, if I am right that there will always be too few officials chasing too many problems, the only way to complement the limited public enforcement is by going to the courts as plaintiffs. The DSA facilitates only some private enforcement actions, such as those against unfair interfaces (Article 25 DSA), or by non-profit groups (Article 90). The good news is that it does not fully pre-empt private enforcement on the national level. In my view, due diligence obligations thus *can* give rise to the corresponding rights of individuals on the national level, and often they *should*. There is an important role left for the national parliaments which can introduce explicit private claims making various due diligence obligations directly actionable. The DSA mostly deals with public enforcement of due diligence obligations and is less concerned with how to convert them into legally enforceable claims of individuals. The care is owed to individuals, but it is less clear how individuals, not regulators, can enforce the DSA's promises. For instance, if a user's account is terminated against all the rules, the DSA only formulates expectations of care, but not a private claim through

which the concerned individual can go to court. Sometimes the legal vehicle to do this already exists in the national law, such as contracts and torts; in other cases, they must be created.

Conclusion

I know that there is a lot of hope that the DSA can serve as a model abroad. But I think we first need to prove that it can work where it was drafted. This brief essay shows that there are many points where the DSA can fail – trusted flaggers, out-of-court settlement bodies, consumer organisations, researchers, national regulators, and obviously, the European Commission. But every point of failure is also an opportunity that mostly did not exist before the DSA. All these shiny tools have one thing in common – without investing our time and money, they can not work as intended.

References

1. Daniel Holznagel, "The Digital Services Act wants you to 'sue' Facebook over content decisions in private de facto courts" (*Verfassungsblog*, 24 June 2021) <https://verfassungsblog.de/dsa-art-18/> accessed 17 January 2023.
2. Mathias Vermeulen, "Researcher Access to Platform Data: European Developments" (2022) 1(4) Journal of Online Trust and Safety 1 <https://doi.org/10.54501/jots.v1i4.84> accessed 17 January 2023.
3. "The Clash Between Facebook and Independent Researchers" (*The Journal, The Wall Street Journal*, 8 September 2021) <https://www.wsj.com/podcasts/the-journal/the-clash-between-facebook-and-independent-researchers/8fda97fc-203d-4632-bc86-f81c0cbe5faf> accessed 17 January 2023.
4. Martin Husovec, "Why There Is No Due Process Online?" (*Balkinization*, 7 June 2019) <https://balkin.blogspot.com/2019/06/why-there-is-no-due-process-online.html> accessed 17 January 2023.
5. Martin Husovec, "Trusted Content Creators" (2022) 9(52) LSE Law Policy Briefing Papers <https://doi.org/10.2139/ssrn.4290917> accessed 17 January 2023.

Folkert Wilman

Between Preservation and Clarification

The Evolution of the DSA's Liability Rules in Light of the CJEU's Case Law

The Digital Services Act (DSA)[1] contains remarkable new rules on matters like content moderation, risk assessment and enforcement. Whilst such rules may be the most eye-catching in current discourse, it should not be forgotten that rules on liability remain a key feature of the DSA's approach to platform regulation.

Recital 16 explains that the DSA seeks to preserve the intermediary liability framework of the e-Commerce Directive (ECD),[2] but also to clarify certain elements, having regard to the case law of the Court of Justice of the EU (CJEU). This essay examines the balance that the EU legislator sought to strike between these two considerations, i.e. preservation and clarification. It does so by focusing specifically on the effect given to the CJEU's case law regarding the ECD's intermediary liability framework.

When assessing the rules in question, it is evident that the DSA's emphasis has been on preservation. However, as this essay will show, that does not mean that nothing at all has changed. In fact, a closer look reveals that in some respects a notable evolution has taken place. That holds true, in particular, in relation to the rules relating to the contested issues of how active a service provider can be without disqualifying *a priori* for the liability exemptions and of "Good Samaritan protection".

Continuity, confirmations and innovations

Articles 4, 5 and 6 of the DSA contain almost literal copies of the conditional liability exemptions found in Articles 12, 13

and 14 ECD for "mere conduit", "caching" and "hosting" services respectively (jointly called "intermediary services" in the DSA). This copy/paste approach is the clearest example of the EU legislator seeking to ensure continuity when it comes to liability rules.

In addition, the DSA contains various provisions that are mainly confirmations of what was already known. Take for instance Recital 17 DSA, which states that the DSA's rules do not offer a positive basis for liability. Thus, where the conditions of the liability exemptions have not been met, the intermediary service provider concerned is not necessarily liable. Rather, whether such liability exists is to be assessed separately under the applicable rules of EU or national law. This already followed from the CJEU's 2010 ruling in *Google France*[3] (see para. 107).

Recital 17 also clarifies that the DSA's liability exemptions relate to any type of liability and to any type of illegal content. In other words, they apply in principle regardless of the nature (civil, criminal or administrative; direct or indirect), origin (EU or Member State) and specific field (defamation, intellectual property, hate speech, etc.) of the "underlying" law that makes the content in question illegal and subject to liability. Whilst only implicit in the CJEU's case law available to date, this has never been fundamentally contested (see F. Wilman, The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US, 2020, pp. 20-21; with further references).[4] Clarifications like the above ones are hardly spectacular. Yet they are still helpful. Including them increases legal

certainty and facilitates the practical application of the DSA. They also help ensure continuity in the transition from the ECD to the DSA.

At the other end of the spectrum, the DSA contains some liability-related provisions that are largely new. One could think, in particular, of the special rule of Article 6(3) DSA regarding the liability under consumer protection law of particular types of hosting service providers; namely, online platforms that allow consumers to conclude distance contracts with traders (simply put: B2C online marketplaces). Admittedly, this rule takes account of prior CJEU case law, in particular *Wathelet*.[5] However, that case did not deal with the ECD's liability exemptions. Thus, whilst Article 6(3) constitutes a notable innovation, it cannot be said to result from earlier case law. Rather, the provision should be seen as an expression of the EU legislator's intention to better protect consumers (see Recital 24 and Article 1(1) DSA).

Service providers' active role

Neutrality as the core criterion

The first of the rules on which this essay concentrates relates to the scope of the intermediary liability regime. The central issue here is how active a service provider may be in providing its service for that service to still qualify as an intermediary service falling within the scope of that regime. The issue

arises especially in relation to the liability exemption for hosting services, contained currently in Article 14 ECD and in the near future in Article 6 DSA.

The CJEU has expressed itself quite extensively on the matter, most notably in *Google France* (para. 112-114),[6] *L'Oréal v. eBay* (para. 112-113)[7] and *YouTube* (para. 105-106; note that this latter judgement dates from after the adoption of the DSA proposal).[8] In this case law, the CJEU formulated the core criterion: to qualify, service providers should take a neutral position in relation to their users' content. That means that they should not play an active role of such a kind as to give them knowledge of or control over that content. This case law has now been codified in Recital 18 DSA.

The CJEU's case law is contested, however. It is based on the application of Recital 42 of the ECD regarding the activity in question being "of a mere technical, automatic and passive nature" to hosting services. This is a reading that many consider mistaken (e. g., Peguera, p. 682).[9] Others argue that the business models of many hosting service providers mean that they are not neutral (e. g., Savin, p. 2).[10] That being so, it is unsurprising that not everybody is thrilled with this decision to codify it (see e. g., Buiten, p. 371).[11] Before concluding that this decision was mistaken, it is however worth noting the following three points.

Subtle changes

First, there are a few subtle changes. Most notably, whilst the DSA repeats many of the ECD's recitals relating to the liability

rules, it does not repeat Recital 42 ECD. Specifically, Recital 18 DSA mentions *mere technical* and *automatic* processing when giving effect to the core criterion of neutrality, but it does *not* refer to the controversial requirement of *passivity*. In other words, the DSA follows the CJEU's ruling in *L'Oreal v. eBay*, which does not refer to Recital 42 ECD and passivity either, rather than *Google France* (and *YouTube*), which do.

In addition, Recital 19 DSA emphasises the different nature of mere conduit, caching and hosting activities. In doing so, it follows *McFadden* (para. 61-63).[12] This indicates that the same criterion may be used for all three types of services, but that it should be applied taking account of the differences between them. Furthermore, Recital 21 DSA about the service provider being "in no way involved" with the user's content remains applicable, like under Recital 43 ECD, only in relation to mere conduit and caching. That suggests that a provider of hosting services *can* be involved, to some extent, with that information, without necessarily disqualifying itself from the liability exemption.

All this confirms what could already be deduced from the CJEU's core criterion itself: intermediary service providers – and especially hosting service providers – *can* play an active role to some extent, provided the role is not such as to give them knowledge of or control over the content that they transmit or store for their users. Thus, passivity is not required and it is inaccurate to cast the discussion about the scope of Article 6 DSA in terms of "active or passive".

Application

Second, it is reasonable to assume that retaining the CJEU's core criterion also means retaining the elements of its case law that few found problematic. That is, the statements dealing with the actual *application* of the criterion. Think in particular of the clarifications provided in *L'Oréal v. eBay* (para. 115-116) that storing offers for sale, setting the terms of service, being remunerated for the service and providing general information to users do not make a hosting service provider (in the case at hand, an online marketplace) "too active". The ruling also clarifies that this would be different, however, where a provider optimises the presentation of the offers for sale or promotes those offers.

In this regard, it is worth bearing in mind that introducing an entirely new criterion – apart from the question of what that criterion should be – might well have led to renewed uncertainty about the application of existent case law. Neutrality may have its shortcomings, such as that it offers little inherent clarity. Yet it does not seem fundamentally unsuited for distinguishing intermediary service providers, which are subject to the DSA's special rules on liability, from content providers, which are subject to the "ordinary" rules of liability for the content that they provide.

Different context and purpose

Third, the concept of "intermediary service provider" may well change by virtue of its transposition from the ECD to the DSA.

Under the ECD, being qualified as such only offers advantages for service providers; especially the availability, in principle, of the liability exemption.

Under the DSA that is different. Said advantages remain but qualifying as an intermediary service provider also means being subject to a range of due diligence obligations, which are set out in other parts of the DSA (namely, its Chapter III). It is hard to imagine that a service provider could escape the application of those obligations simply by making itself "too active".

This difference may not only affect how keen service providers are on qualifying as intermediary service providers, but it could also alter the interpretation of the concept itself. For it is settled case law that terms of EU law are to be interpreted in the light of not only their wording but also their context and the objectives pursued. As the latter have changed – see, for instance, the DSA's aim of protecting fundamental rights, including consumer protection (Article 1(1) DSA)) – this may well affect the CJEU's interpretation of the concept in future cases brought under the DSA, despite the concept having been worded and explained similarly as under the ECD.

"Good Samaritan" protection

What's not new...

The second rule to be considered here is the "Good Samaritan" clause, laid down in Article 7 DSA. It holds, in short, that intermediary service providers are not to be deemed ineligible for the liability exemptions of Articles 4, 5 and 6 DSA solely

because they either take voluntary own-initiative measures to tackle illegal content or take measures to comply with EU or national law.

This rule is related to the previous topic: intermediary service providers may be hesitant to take such voluntary measures out of fear of being seen as too actively involved with their users' content, which, in turn, could mean that they are excluded from the scope of the DSA's liability exemptions. Article 7 aims to clarify that such fear is unfounded, provided however the intermediary service provider concerned acts in good faith and diligently. As explained in Recital 26 DSA, in this manner the clause seeks to remove a disincentive for the taking of such voluntary measures.

As regards the taking of such voluntary measures, Article 7 corresponds to what the CJEU stated in *YouTube* (para. 109). In that judgement, The CJEU held that the fact that a service provider voluntarily implements technological measures aimed at detecting certain illegal (in the case at hand, copyright-infringing) content among the content uploaded by its users does not mean that it plays an active role giving it knowledge of and control over the content within the meaning of the above-mentioned case law. The European Commission had earlier already made similar statements in non-binding documents, such as its 2018 Recommendation on illegal content online (Recital 26).[13]

As regards the taking of measures to comply with the law, this seems like little more than stating the obvious. That said, some might still find it helpful to be reassured in this man-

ner that compliance with, for instance, the DSA's due diligence obligations does not lead to the service provider in question becoming "too active". That conclusion would also seem to follow, by the way, from the statement in its Recital 41 that the DSA's due diligence obligations are independent of the question of liability.

... and what is

However, some elements of Article 7 DSA *are* new; most notably, the conditions of good faith and diligence. There are good reasons for including these conditions. In particular, voluntary measures taken by intermediary service providers are not socially beneficial *per se*. Even when sincerely meant to tackle illegal content, they can cause considerable damage if not enacted diligently. For instance, the large-scale removal of content that is wrongly considered illegal comes to mind.

The conditions of good faith and diligence are clearly open norms. That may be hard to avoid, considering the many different situations in which Article 7 could apply. Nonetheless, the resulting flexibility comes at the expense of clarity. It will be principally up to the CJEU to determine, in time, what these conditions entail exactly.

Although therefore not entirely clear, it would be unfair to say that Article 7 simply swaps the uncertainty as to *whether* such voluntary measures can be taken for uncertainty as to *how* those measures are to be taken. That is so, especially in view of clarifications provided in Recital 26 DSA, for instance as regards service providers taking reasonable measures to ensure

that any automated tools used are as reliable as possible. In essence, it seems that respecting the diligence requirements found elsewhere in the DSA, combined with a dose of common sense and reasonableness, should normally go a long way in ensuring that the conditions are met. That holds true all the more so given that setting the bar too high would imply the risk that Article 7 will fail to achieve the above-mentioned objective.

Other criticisms

Other criticisms of Article 7 (see e. g., Kuczerawy, 2021)[14] seem less well founded. For instance, there is no reason to consider that the *actual success* of the voluntary measures taken in tackling illegal content is relevant in this context. That is to say, good faith and diligence quite clearly do not imply a requirement that the measures must have been fully successful. When it comes to tackling illegal content, 100% effectiveness is neither realistic nor necessarily required (cf. *UPC Telekabel Wien*, para. 58-63).[15]

Furthermore, it is true that Article 7 does not address the possibility that an intermediary service provider may *obtain actual knowledge or awareness* of illegal content, within the meaning of Article 6 DSA, as a consequence of the voluntary measures that it enacts. But that is for good reason and is unlikely to act as a serious disincentive. For where that occurs, the intermediary service provider has an obvious course of action to avoid losing the benefit of the liability exemption.

Namely, expeditiously removing the illegal content in question. In this regard, it should be recalled that a hosting service provider only risks losing said benefit if a *specific* item of illegal content, of which it obtains knowledge but which it may have failed to remove expeditiously, is *clearly illegal*, in the sense that the illegality can be established without a detailed legal examination (cf. *YouTube*, para. 111-116; these parts of the judgement are relating to notices, but the same is likely to hold true in relation to own-initiative investigations; see also Article 14(3) DSA).

Conclusion

The DSA retains the key features of the ECD's intermediary liability regime, but it also contains several clarifications. The latter range from uncontroversial statements to largely new rules, with an interesting group of provisions – notably those on the service providers' active role and "Good Samaritan" actions – somewhere in between. The clarifications tend to build on existing CJEU case law and will, no doubt, over time generate new case law, fleshing out what they entail precisely. That being so, whilst the DSA's rules on matters like due diligence, risk assessments and enforcement may be most eye-catching, it would be a mistake to ignore the subtle yet noteworthy evolution that the DSA brings about for liability-related matters.

This essay has been written in a personal capacity and none of the statements made therein can be attributed to the author's employer.

References

1. See the draft Regulation on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act), 7.9.2022, available via: https://www.europarl.europa.eu/doceo/document/TA-9-2022-0269-FNL-COR01_EN.pdf.
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 L 178/1.
3. Case C-134/02 *Joined Cases C-236/08 to C-238/08, Google France* EU:C:2010:159, [2010] OJ C134/2.
4. Folkert Wilman, *The Responsibility of Online Intermediaries for Illegal User Content in the EU and the US* (Edward Elgar 2020) 20 <https://www.elgaronline.com/view/9781839104824.xml>.
5. Case C-149/15, *Sabrina Wathelet v Garage Bietheres & Fils SPRL* EU:C:2016:840, [2016].
6. Case C-134/02 *Joined Cases C-236/08 to C-238/08, Google France* EU:C:2010:159, [2010] OJ C134/2 paras 112-114.
7. Case C-324/09 *L'Oréal SA and Others v eBay International AG and Others* EU:C:2011:474, [2011] paras 112-113.
8. Joined Cases C682/18 and C683/18 *Frank Peterson v YouTube Inc. and Others and Elsevier Inc. v Cyando AG* EU:C:2021:503, [2021] paras 105-106.
9. Miquel Peguera, "The Platform Neutrality Conundrum and the Digital Services Act" (2022) 53 IIC 681,682 <https://link.springer.com/article/10.1007/s40319-022-01205-7> accessed 18 January 2023.
10. Andrej Savin, "The EU Digital Services Act: Towards a More Responsible Internet" (2021) Copenhagen Business School Law Research Paper Series No. 21-04 1,2 <https://ssrn.com/abstract=3786792>.
11. Miriam Buiten, "The Digital Services Act: From Intermediary Liability to Platform Regulation" (2021) 12(5) JIPITEC 361, 371 <https://www.jipitec.eu/issues/jipitec-12-5-2021/5491>.
12. Case C-484/14, *McFadden v Sony Music Entertainment Germany GmbH* EU:C:2016:689, [2016].
13. Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online [2018] OJ L 63/50.

14. Aleksandra Kuczerawy, "The Good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act" (*Verfassungsblog*, 12 January 2021) <https://verfassungsblog.de/good-samaritan-dsa/> accessed 18 January 2023.
15. Case C314/12, *UPC Telekabel Wien v Constantin Film Verleih and Others* EU:C:2014:192, [2014] paras 58-63.

Sebastian Becker and Jan Penfrat

The DSA Fails to Reign in the Most Harmful Digital Platform Businesses - But It Is Still Useful

The Digital Services Act (DSA) adopted by the European Parliament on 5 July 2022 was lauded by some as creating a "constitution for the internet"[1] and a European response to the "digital wild west".[2]

Together with many other civil society organisations, European Digital Rights (EDRi)[3] has been working extensively with the EU's institutions to ensure that the new regulation not only fulfils this promise but, by doing so, protects the fundamental rights of people and reaffirms the open internet as a public good. To some extent, we have succeeded. But the DSA is far from perfect and much will depend on how well the new regulation is going to be implemented and enforced.

This essay argues that while the DSA has just been crafted carefully enough to avoid major damage to digital rights in the EU, it has focussed so much on *who* must delete what kind of content within which time frame, that it missed the bigger picture: no content moderation policy in the world will protect us from harmful online content as long as we do not address the dominant, yet incredibly damaging surveillance business model of most large tech firms.

This essay builds its legal and policy observations on EDRi's DSA research and advocacy work of the past three years.

Freedom of expression online and the role of online platforms

One of the main pillars of the DSA is the new content moderation framework for online platforms such as Facebook,

YouTube and Twitter. This framework consists of a conditional liability regime that follows the logic of the EU's Electronic Commerce Directive (ECD)[4] and the jurisprudence[5] of the Court of Justice of the European Union. Just as under the ECD, online platforms can only be held liable for user-generated content if they have "actual knowledge" of the illegality of that content, and – just as under the ECD – the DSA continues to prohibit EU Member States to impose any obligation for platforms to generally monitor user content.

These principles aim to protect freedom of expression by ensuring that online platforms are not incentivised to over-police people's online speech. Therefore, the EU's decision to uphold the conditional liability regime and combine it with a mandatory "notice-and-action" system that should enable users to flag illegal content and complain about the platforms' inaction are considered by many civil society organisations to be welcome steps in the right direction. This is particularly true when compared to the various dangerous proposals that were put forward by some EU member states and Members of the European Parliament: from 24-hour removal deadlines from the moment of flagging to mandatory and generalised content surveillance by platform companies. Many of those dangerous proposals would have almost entirely dismantled free expression rights of all platform users.

However, the DSA's strong focus on the comprehensive regulation of user-generated online content has also somewhat obstructed the view on the bigger questions: Why does harmful or illegal content spread so expansively on social media in

the first place? What responsibility do online platforms' algorithms play in the distribution and promotion of online content? And what are the commercial incentives that guide the development of those algorithms?

These questions motivated EDRi's digital rights advocacy early on, aimed at understanding the commercial interests of large online platform providers and at highlighting their role in actively distributing and amplifying different kinds of online content, including through and funded by surveillance-based online advertising.

Big Tech is broken by design and by default

When online platforms moderate and recommend online content, they can do so based on various rules and factors. This includes their own terms and conditions, applicable law in the country where a given piece of content was posted from, as well as what kind of content maximises the platform's profits. The larger the profits, the stronger the incentive to let them guide content moderation and recommendation practices.

EDRi[6] and many other organisations and researchers have[7] shed light[8] on how companies such as YouTube's Alphabet Inc (US$ 76 billion net income in 2021) and Facebook's Meta Inc (US$ 39 billion in 2021) continuously optimise their content recommendation algorithms in view of maximising their profits.

But it is not only the company's size that matters.

The business models of most of the largest tech firms are built around what we call "surveillance-based advertising"[9] - digital ads that target people based on personal, often very sensitive data that those firms extract from us all. It is "extracted" because while this data is sometimes explicitly provided by users, it is most often information inferred from our observed behaviour online: every website we visit, every article we read, apps we install, product we buy, our likes, our comments, connections, and many more sources of metadata are being combined into the largest commercial collection of individual profiles that humankind has ever seen.

All of this just to enable companies to fill our screens with advertising micro-targeted at us, trying to convince us to buy more stuff.

Deception as a service

In theory, under the EU's General Data Protection Regulation (GDPR),[10] this type of data collection for marketing purposes is only legal with people's consent. Yet, many companies deploy deceptive designs in their user interfaces. Those include, for example, consent pop-ups that do not offer users meaningful ways to reject tracking, that trick users into clicking "accept", or do not provide the necessary information about how personal data would be used for advertising.

These deceptive designs[11] (or dark patterns) are currently deployed on 97% of the 75 most popular websites and apps according to a 2022 study.[12] Hence, they continue to play a

central role[13] in the surveillance-driven advertising business. Companies are of course fully aware of what they are doing: in its 2018 annual report[14], Facebook stated that the regulation of deceptive design "could adversely affect [their] financial results". Both Meta and Google have joined other tech firms in firmly opposing any deceptive design regulation in the DSA.

Not least thanks to civil society's advocacy, the final DSA does recognise the negative impact that deceptive interface designs have on users' privacy rights, but heavy corporate lobbying has led it to contain only very limited restrictions: While Article 25 prohibits interface designs that "deceive or manipulate the recipients of their service or in a way that otherwise materially distorts or impairs the ability of the recipients of their service to make free and informed decisions", this prohibition only applies to online platforms (such as Facebook, Tiktok, Youtube, or Twitter), not to websites that embed, say, Google ads. More crucially, the prohibition does not apply to practices covered by GDPR and the Unfair Commercial Practices Directive (UCPD)[15] – a limitation that will exclude all consent pop-ups for personal data collection.

Tracking-free ads instead?

Knowing that the DSA was unlikely to solve these problems, more than 20 Members of the European Parliament, 50+ civil society organisations, and many ethical tech firms banded together in the Tracking-Free Ads Coalition (EDRi is a supporter)[16], to achieve more substantive change: an end to surveillance-based advertising altogether.

This attempt sparked a colossal counter-lobbying campaign[17] that included full-page newspaper ads from Facebook[18], social media ads micro-targeted at MEPs, as well as Brussels' billboards and other ad spaces[19] covered all with a single message: European SMEs need surveillance-based online advertising to reach customers. Without them, the EU economy basically falls apart.

As a result, the DSA addresses surveillance-based ads only with half-baked restrictions in Article 26. It prohibits providers of online platforms to "present advertisements to recipients of the service based on profiling" as defined by GDPR, as well as to use "special categories of personal data referred to in Article 9(1)" of the GDPR.

Just as with deceptive interface designs, those restrictions only apply to online platforms as defined in the DSA, but not to websites, apps or other intermediary services that embed Google ads, for example. Worse, the DSA limits the prohibition to ads shown by platforms *to their own users*. Providers are therefore free to micro-target such ads to anywhere else on the web, if they offer this kind of service. This does not respond to the actual and current ad tech ecosystem.[20] In practice, the prohibition in the DSA will not cover things like cookies and tracking banners that appear as advertisements on most webpages thanks to Google ads services.

Even worse still, Article 26 does not address the use of proxy data for sensitive characteristics. While a platform will not be allowed to target ads based on the sensitive category "race", they can simply replace it with a generic proxy "interested in

African-American culture" or "K-pop". While targeting based on health data, for example based on pregnancy, won't be allowed anymore, a platform can simply use a category based around "interest in baby toys". As long as those proxies cannot be construed as "revealing" sensitive data (which would be prohibited again), anything goes. As a result, this DSA provision is unlikely to protect people from the discrimination[21] and abuse of personal data[22] that the ad industry enables.

A semi-positive conclusion

Despite all the shortcomings touched upon above, EDRi holds that the DSA is a positive step forward. That is because, while not ambitious enough, it has – maybe for the first time in Europe – enabled politicians and the public to debate and understand the harms inflicted by the data-driven advertising models that many of the largest tech firms would rather keep hidden from public view.

Now it is known that Google is not a search engine provider and Facebook never was a social media company. They are global commercial surveillance corporations.

The biggest contribution of all debates around the DSA is that next time around, lawmakers and the public are already aware.

References

1. Alexandra Geese, "Europe Calling 'DSA Deal: A constitution for the internet!'" (*Alexandrageese.eu*, 29 April 2022) <https://en.alexandrageese.eu/video/europe-calling-dsa-deal/> accessed 27 October 2022.
2. EPP Group, "New sand strong rules for online platforms to end 'digital Wild West' created by Silicon Valley." (*EPP Group*, 19 January 2022) <https://www.eppgroup.eu/newsroom/news/new-rules-for-online-platforms-to-end-digital-wild-west> accessed 27 October 2022.
3. European Digital Rights (EDRi) <edri.org> accessed 27 October 2022.
4. Directive 2000/31/EC of the European Parliament and of the Council of 8th 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.
5. Case C-682/18 and C-683/18 Frank Peterson v Google LLC & others [2021] OJ 2021/503.
6. EDRi, "Targeted online: an industry broken by design and by default" (March 2021) <https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf> accessed 27 October 2022.
7. Article19, "EU: Regulation of recommender systems in the Digital Services Act" (*Article19*, 14 May 2021) <https://www.article19.org/resources/eu-regulation-of-recommender-systems-in-the-digital-services-act/> accessed 27 October 2022.
8. Access Now, "Who should decide what we see online" (*Access Now*, 20 February 2020) <https://www.accessnow.org/who-should-decide-what-we-see-online/> accessed 27 October 2022.
9. EDRi, "Targeted online: an industry broken by design and by default" (*EDRi*, March 2021) <https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf> accessed 27 October 2022.
10. 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

11. Deceptive Design, "About this site" (*deceptive.design*) <https://www.deceptive.design/about-us> accessed 28 October 2022.

12. Francisco Lupiáñez-Villanueva and others, *Behavioural Study on Unfair Commercial Practices in the digital environment: dark patterns and manipulative personalization* (Directorate-General for Justice and Consumers [European Commission] 2022) <https://data.europa.eu/doi/10.2838/859030> accessed 27 October 2022.

13. Catherine Armitage, Johnny Ryan and Ilaria Buri, "Online Advertising: These Three Policy Ideas Could Stop Tech Amplifying Hate - DSA Observatory" (*DSA Observatory* 5 July 2021) <https://dsa-observatory.eu/2021/07/05/online-advertising-these-three-policy-ideas-could-stop-tech-amplifying-hate/> accessed 22 November 2022.

14. Facebook Inc., "ANNUAL REPORT PURSUANT TO SECTION 13 OR 15(d) OF THE SECURITIES EXCHANGE ACT OF 1934 For the fiscal year ended December 31, 2020" (January 2021) <https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/4dd7fa7f-1a51-4ed9-b9df-7f42cc3321eb.pdf> accessed 27 October 2022.

15. Directive 2005/29/EC of the European Parliament and of the Council of 11 may 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) no 2006/2004 of the European Parliament and of the Council [2005] OJ L 149/22.

16. Tracking-free Ads Coalition <trackingfreeads.eu> accessed 27 October 2022.

17. Corporate Europe Observatory, "Big Tech's last minute attempt to tame EU tech rules" (*Corporate Europe Observatory*, 23 April 2022) <https://corporateeurope.org/en/2022/04/big-techs-last-minute-attempt-tame-eu-tech-rules> accessed 27 October 2022.

18. Frederik Zuiderveen Borgesius, "Sigh." (*Twitter*, 21 November 2021) <https://twitter.com/fborgesius/status/1462518361619849222>, accessed 27 October 2022.

19. Jan Penfrat, "Example of how Facebook tries to influence policymakers in Brussels via @POLITICOEurope with their not-so-subtle nonsense advertising" (*Twitter*, 10 November 2021) <https://twitter.com/ilumium/status/1458371612542218245> accessed 27 October 2022.

20. Global Disinformation Index, "Follow the Money – How disinformation has become a big business" (*Global Disinformation Index*, 2 April 2019) <https://www.disinformationindex.org/blog/2019-4-2-follow-the-money-how-disinformation-became-a-big-business/> accessed 28 October 2022.

21. Frederike Kaltheuner, "How online ads discriminate. Unequal harms of online advertising in Europe" (Gail Rego ed, *EDRi*, June 2021) <https://edri.org/wp-content/uploads/2021/06/EDRi_Discrimination_Online.pdf> accessed 27 October 2022.

22. EDRi, "Targeted online: an industry broken by design and by default" (*EDRi*, March 2021) <https://edri.org/wp-content/uploads/2021/03/Targeted-online-An-industry-broken-by-design-and-by-default.pdf> accessed 27 October 2022.

Alexandra Geese

Why the DSA Could Save Us From the Rise of Authoritarian Regimes

The rise of extremist right-wing governments, as observed recently in Italy, is closely linked to the business models of large digital platforms such as Facebook and YouTube. Their algorithms polarise debates and stir up emotions because that enables them to keep people on their screens for longer and show them advertising. Our time is their money. But what does that mean for democracy?

The profit-making polarisation of debates favours angry content eliciting hate and fear.[1] In political terms, those emotions are usually targeted by right-wing extremist movements and parties who thrive on spreading anger and fear. As a consequence, messages shared on the internet by right-wing extremists go viral and then quickly enter the mainstream via conservative media or politicians. A recent example is German CDU leader Friedrich Merz calling Ukrainian refugees "social tourists", picking up a typical right-wing extremist narrative depicting war refugees as greedy people going after German taxpayers' money. People who consistently counter such speech are often attacked with coordinated hate posts. A case in point is the Austrian political scientist Natascha Strobl,[2] who is regularly forced to leave Twitter to shield herself from threats and insults. Such pile-ons also silence people in the political centre.

The Swedish democracy researcher Staffan Lindberg and colleagues from the V-Dem Institute see a clear link between polarisation and the success of autocrats[3] – something that three years ago was considered a bold theory and has now become reality. Nobel Peace Prize winners like Maria Ressa are calling for

restrictions to be placed on tech companies' destructive polarisation power with a 10-point plan;[4] the UN Secretary-General Antonio Guterres tweeted:[5] "Social media platforms based on a business model that monetises anger & negativity are causing untold damage to societies. Hate speech & misinformation are proliferating. Our data is being bought & sold to influence behaviour. We need regulatory frameworks to change this."

The European Union's Digital Services Act ("DSA") is this framework.

No more: "Too big to regulate"

The Act initiates a paradigm shift in the thinking about the regulation of digital technology in general, and of social networks, in particular. The following considerations are inspired by Shoshana Zuboff, emeritus Harvard professor and author of the ground-breaking book "The Age of Surveillance Capitalism".

The first fundamental change is that the DSA breaks with the previous paradigm whereby tech companies shaped the world largely unhindered. Their global nature, their financial might, and their ability to reach billions of people and thereby influence public opinion seemed to make regulatory attempts impossible or ineffectual. The Act now puts an end to that futility. Democracy is alive and has the clear intention to set its own rules that Big Tech companies also must abide by. This is an important point because the previously prevailing opinion in Brussels and Washington was that technological developments were unstoppable, and society had to adapt. The DSA

differentiates between technology, business models, and content moderation rules, and questions whether surveillance capitalism really is unavoidable. "Too big to regulate" no longer holds up.

Holding platforms accountable for what they do - not for their users' opinions

The second paradigm shift is the systemic approach. Prior to the DSA, liability and freedom of expression were considered to be the main areas of action for platform regulation. But regulation focusing primarily on platforms' liability for user-generated content is far too restrictive and leads to a dilemma. Platforms are given a normative responsibility to decide on users' freedom of expression, thus gaining even more power in a realm of information which, due to its own profit-oriented mechanisms, is the reason why such masses of problematic content are generated in the first place. Legislators and judicial authorities would therefore relinquish even more power to commercial stakeholders, precisely the opposite of what regulation seeks to do. At the same time, large platforms cleverly used the notion of freedom of expression as a main focus in the public debate, thus singing from the same song sheet as the defenders of freedom of expression and human rights, who are quite rightly concerned about restrictions to freedom of expression online.

Especially in countries where the rule of law is not a given and state actions are more feared than those of private enterprises, this fear is more than justified. However, by restricting

the debate to the question of liability and freedom of expression, we turned a blind eye on what the platforms were actually doing. Freedom of expression is best guaranteed in an environment in which women and minorities are not systematically suppressed by hate speech and where extremist opinions are not disproportionately reinforced by untransparent algorithms. That is precisely what platforms promote and effect. It is true in democratic states, but even more so in autocracies, as demonstrated by the most recent research by Amnesty International[6] into Facebook's role in the genocide of the Rohingya in Myanmar. „Facebook's algorithms were intensifying a storm of hatred against the Rohingya which contributed to real-world violence," said Amnesty International Secretary General Agnès Callamard.[7]

The DSA opens our eyes to the bigger picture in this respect. Whilst honouring the hosting liability exemption privilege of the E-Commerce Directive, it places the focus much more on the platforms' conduct through the regime of due diligence obligations. Transparency provisions, clear notice-and-action processes, internal complaint mechanisms, and independent dispute settlement authorities ensure clarity in the moderation of individual content and finally give rights to users whose content is arbitrarily blocked or deleted.

Who knows what - Tackling information asymmetry

However, looking into the deeper workings of these very large platforms is even more important. Thanks to the contribu-

tions of Facebook whistle-blower Frances Haugen, the Council and Parliament built upon the Commission's hesitant initial proposal. The DSA now addresses some systemic issues. Not with finished solutions but rather with a toolbox which offers insight and concrete intervention options to the European Commission, national supervisory authorities, independent researchers and, unfortunately to a lesser extent, NGOs and thereby the public.

The systemic approach leads to the third paradigm shift of the DSA. It tackles and hopefully reduces the information asymmetry. So far, platforms knew everything about us due to the extensive collection and analysis of our most private data. We knew nothing. The little we could say with any kind of certainty came from whistle-blowers like Frances Haugen and others.

The DSA now offers methods to obtain knowledge about how platforms work. The very large platforms have to write risk assessments in which "systemic risks stemming from the design, including algorithmic systems, functioning and use made of their services in the Union" are identified, analysed and assessed. It is therefore no longer just a question of abuse of the systems by "malicious actors" but rather the intended workings ("design") of the social networks themselves. The list of explicitly stated risk areas is extensive. It applies to basic human rights in general and to human dignity and data protection, as well as to public opinion-forming, elections, violence against women, child protection, and public health. The factors which must be considered explicitly in the risk assess-

ments not only include rather obvious aspects, such as recommendation systems, algorithms, content moderation systems and terms and conditions, but also advertising and data practices.

All very large platforms are independently audited at least once a year. Moreover, the Commission, Digital Services Coordinators in the Member States, and vetted independent researchers will be granted access to large platforms' data. Civil society organisations are at least allowed to use publicly available data freely. That finally enables quantitative analyses and ensures that data access can no longer be used as a means to reward friendly researchers and hinder critical minds from digging deeper. These rules also afford valuable insight into the platforms' conduct. If supervisory authorities, researchers, and NGOs can pose questions and answer them in an evidence-based manner, it will be possible to use that knowledge to design platforms to promote democracy and freedom of expression, rather than hinder them.

The new Regulation also contains a new restriction on how platforms can use our data, from which they derive so much knowledge about our society. The DSA prohibits sensitive data categories as per the GDPR from being incorporated into advertising profiles. Furthermore, data from people known to be minors can no longer be used for advertising purposes. The cautious wording reflects a weary struggle with two opposing positions: keeping the status quo, i.e., using all personal data for which consent was granted via questionable cookie banners in extensive profiles, versus a complete reform of the on-

line advertising model, towards purely contextual advertising without the use of personal data. Prohibiting the use of sensitive data is especially relevant, given the leaked Facebook documents[8] which show that Facebook (now Meta) is not structurally able to distinguish certain data categories from others and thereby fulfil its related obligations not only under the GDPR but also the DSA/DMA.

It is precisely these extensive data profiles that make polarisation in social networks so dangerous. The algorithms prioritise content which triggers negative emotions such as fear and anger. Extensive user data profiles enable strong personalisation, meaning everyone sees exactly the information that personally aggravates them. Polarisation is strongly personalised and keeps people at their screens. Platforms thereby increase their profits, whilst democratic decision-making processes, which require facts and objective discussions, draw the short straw. The UN Secretary General warns: "Our data is being bought and sold to influence behaviour."[9] Data protection should not only be about protecting an individual right but rather about protecting whole societies from manipulation.

That is where the DSA comes in. It doesn't just scratch the surface; it takes a critical look at the actual causes of these major threats to our democracy: hate, incitement, misinformation, and surveillance. Behind its abstract wording are dynamic instruments to put an end to the surveillance practices of Google and Meta, in particular, which use data hoovers for advertising purposes and polarisation, and to expose the algorithms which push hate messages and false information to the

top of the list, and thus completely blur public debate. It lays the foundations for precise analyses which legislators and regulators need to enact evidence-based policies and precise provisions for an internet where everyone's voice is heard.

Enforcement and global impact

Will the DSA revolutionise the internet? One thing is clear: it all depends on whether it is properly enforced. The enforcement of the chapter dedicated to the very large platforms is currently the responsibility of the European Commission, which is establishing a corresponding competence centre. Part of the financing comes from the fees to be paid by the companies to be supervised. That is good because highly qualified experts can then be employed with that money. In the long term, however, the competence centre and the supervisory body should be further developed into an independent European authority to prevent political influence. That is even more urgent, given the current developments in Europe. With Italy and Sweden now joining Poland and Hungary, there are two further Member States with extreme right-wing governments in power who could send commissioners to Brussels in 2024, who might have greater interest in maintaining polarising algorithms and extensive data collection than protecting democracy. The supervisory authorities in the Member States also play an important role. The rule that researchers must be accredited in the "member state of establishment", i.e., in the very country in which the Big Tech companies can exercise the most influence, is dis-

appointing. There is a good reason why the European Commission has the bulk of enforcement tasks regarding Big Tech.

Despite justified criticism, the DSA has the potential to become a global standard. There has been huge interest from around the world, especially from the USA, but also from countries such as Brazil, Pakistan, and Japan. As the first democratic continent to present a well-thought-out law, we have the opportunity to set the course and save the internet from being monopolised by surveillance companies. A powerful and consistent enforcement at EU level and in the Member States will be crucial for its success.

References

1. Keach Hagey and Jeff Horwitz, "Facebook Tried to Make Its Platform a Healthier Place. It Got Angrier Instead." *Wall Street Journal* (New York City, 15 September 2021) <https://www.wsj.com/articles/facebook-algorithm-change-zuckerberg-11631654215> accessed 23 December 2022.
2. Wikipedia, "Natascha Strobl" (*Wikipedia* 2022) <https://de.wikipedia.org/w/index.php?title=Natascha_Strobl&oldid=229099655> accessed 23 December 2022.
3. Vanessa A. Boese and others, "Democracy Report 2022: Autocratization Changing Nature?" (*V-Dem Institute*, March 2022) <https://v-dem.net/media/publications/dr_2022.pdf> accessed 19 January 2023.
4. Ingvill Bryn Rambøl, "Launched Action Plan to Support Journalism and Fight Disinformation" (*Nobel Peace Center*, 2 September 2022) <https://www.nobelpeacecenter.org/en/news/nobel-laureates-launched-action-plan-to-support-journalism-and-fight-disinformation> accessed 23 December 2022.
5. Antonio Guterres, "Need for Regulatory Frameworks." (*Twitter*, 25 September 2022) <https://twitter.com/antonioguterres/status/1574111500201074688> accessed 23 December 2022.
6. Amnesty International, "Myanmar: Facebook's Systems Promoted Violence against Rohingya; Meta Owes Reparations" (*Amnesty International*, 29 September 2022) <https://www.amnesty.org/en/latest/news/2022/09/myanmar-facebooks-systems-promoted-violence-against-rohingya-meta-owes-reparations-new-report/> accessed 23 December 2022.
7. Ibid.
8. Franceschi-Bicchierai L, "Facebook Doesn't Know What It Does With Your Data, Or Where It Goes: Leaked Document" *VICE* (New York City, 26 April 2022) <https://www.vice.com/en/article/akvmke/facebook-doesnt-know-what-it-does-with-your-data-or-where-it-goes> accessed 23 December 2022.
9. Same as reference 5.

Ilaria Buri

A Regulator Caught Between Conflicting Policy Objectives

Reflections on the European Commission's Role as DSA Enforcer

The Digital Services Act (DSA) has landed on an increased centralisation of its enforcement powers in the hands of the European Commission (EC). The Regulation grants the Commission exclusive supervision and enforcement powers *vis-à-vis* the biggest platforms and online search engines for their most important due diligence obligations (such as the ones on the assessment of systemic risks, access to research data and crisis protocols). In addition, the Commission is also competent – together with the Member States – to supervise the same platforms for their compliance with rules which do not apply exclusively to very large online platforms (VLOPs) and very large online search engines (VLOSEs). However, the national regulators (the Digital Services Coordinators, DSCs) will only be competent to step in when the Commission has not taken any initiative against the same suspected infringement. The final text also introduces an annual supervisory fee, to be paid by the VLOPs and VLOSEs, to cover the costs incurred by the EC as a result of its supervisory tasks.

As observed in previous analysis,[1] the rationale behind EC centralised enforcement is understandable, particularly in light of the experience with the General Data Protection Regulation's (GDPR) enforcement. At the same time, this choice also raises new issues that are worth discussing.

This analysis focuses on the implications, from a fundamental rights and democratic values perspective, of opting for the EC as the body in charge of supervising and enforcing the DSA against the most powerful online platforms. Given the importance and broader implications of the DSA, the policy choice of

making the EC the most important enforcer in the DSA architecture needs to be scrutinised more, especially where the centralisation of enforcement powers around the EC may become recurrent in future pieces of legislation. In particular, aspects that deserve more attention relate to the difference between the EC and a separate independent EU supervisory authority and to the tensions inherent to the different policy objectives pursued by the EC, which might impact the way it performs its oversight tasks under the DSA.

The DSA regulators and their independence: The Digital Services Coordinators and the European Commission

Article 50 of the final DSA text states that DSCs must carry out their task in *"an impartial, transparent and timely manner"* and that they must exercise their tasks and powers *"with complete independence,* [...] *free from any external influence, whether direct or indirect, and* [without taking] *instructions from any other public authority or any private party"*. In this regard, this language is identical to that of Article 52 GDPR on the independence of supervisory authorities.

Under the GDPR, the independence and willingness of certain national supervisory authorities to enforce the law has been questioned. This is particularly the case for the Irish Data Protection Commission and its regulatory performance under the one-stop-shop mechanism, which also led to a formal complaint before the EU Ombudsman[2] about the EC's failure in ensuring that the GDPR is adequately applied across the EU. In

the context of the DSA debate, this situation contributed to the legislative choice of granting the EC – which is presumed to be more resilient to dynamics of regulatory capture than national regulators – key functions in the oversight and enforcement of the DSA. Indeed, as recently admitted by the EC's Vice-President Vestager, "there was distrust"[3] among member states that Ireland could act as an effective regulator against Big Tech. As the DSA's rules and their enforcement will have a clear and undeniable impact on fundamental rights and democratic values, the question arises of how the above-mentioned requirements of independence play out when it comes to the EC. Complex assessments involving fundamental rights such as the freedom of expression, right to privacy, and any restrictions thereto are normally entrusted to independent bodies[4] not vulnerable to direct political control.

The EC, however, is not an independent regulator, but the main executive body of the EU. It is, starting from its very composition and appointment, a deeply political body, which is entrusted with the power of legislative initiative and plays a crucial role in the legislative negotiations. Through its many legislative proposals and institutional tasks, the Commission pursues and combines a variety of policy objectives, with significant implications on fundamental rights.

The European Commission and its many (often conflicting) policy objectives

The main policy objectives of the DSA are the promotion of the digital single market, addressing online harms, in particu-

lar illegal content, and ensuring the protection of fundamental rights online. The coexistence between these policy objectives is complex: it is marked by inevitable tensions, which require policy choices and continuous balancing. *Vis-à-vis* these policy objectives, the position of the EC – both as the executive body holding the monopoly of legislative initiative and as a DSA enforcer – is also very complex. Different parts of the EC (Directorate Generals, DGs) relate differently to different policy objectives, which are often in tension with each other (more often than not, promoting the single market and favouring trade versus the protection of fundamental rights). As a consequence, it would seem unlikely that the assessments and initiatives carried out by the Commission as an enforcer under the DSA will not be influenced by the agenda pursued by the same institution in DSA-related domains and other policy areas.

Systemic risks in the DSA and the EC's policies in the area of data protection

One area where the EC's action and initiatives might be in conflict with its role as DSA enforcer is EU data protection law and its enforcement. Online platforms' services (particularly those of VLOPs) entail the processing of massive amounts of personal data, and some of the most relevant systemic societal risks are connected to the adverse impact of these practices on the fundamental right to the protection of personal data and privacy. It is in recognition of these issues, that the final DSA text mentions privacy and data protection among the

fundamental rights which might be impacted by systemic risks, and expressly refers to targeted advertising systems and data-related practices, in Articles 34 and 35 on systemic risks. In general, the entire debate about the risks of tracking-based ads shaped up as one of the most heated issues in the entire DSA process. It included the idea of restricting the use of minors' personal data and that of special categories of data for the purposes of online ads (Article 26 and 28 of the DSA final text). Overarchingly, these inclusions build upon the realisation of the impact that business models relying on the systematic collection of personal data have on fundamental rights and other important societal values. Given the wealth of data protection and privacy-related aspects in the DSA framework and their enforcement, the European Data Protection Board (EDPB) also called on the co-legislators[5] to ensure that the DSA foresees cooperation in enforcement with data protection authorities.

Against this background, the EC's role as the main enforcer for VLOPs and VLOSEs might be difficult to reconcile with (i. e., to keep uninfluenced by) the policy choices or legislative proposals that the same institution is undertaking in the area of data protection law or in other domains which are related to it. In other words, it could be argued that the way the EC perceives possible systemic risks connected to the fundamental right to data protection (and the adequacy of platforms' measures to mitigate those) is heavily influenced by the policy choices that the same institution has taken or is pursuing in that domain or connected ones.

In the area of international data transfers, for instance, the

EC typically deals with different (and often conflicting) policy objectives: international trade, on the one hand, and the protection of fundamental rights, on the other hand.[6] With regard to the EU-US international personal data transfers, the EC's assessment of how to balance these policy goals resulted in two adequacy decisions, the EU-US Safe Harbour and the EU-US Privacy Shield, both of which were invalidated by the CJEU, in 2015 and 2020, for failing to provide adequate protection to the rights of EU citizens. A new framework for transatlantic data flows,[7] with great implications for the VLOPs, is currently being negotiated by the EC and might be referred to the CJEU again.

This example shows, first, that in a hypothetical scenario where the EC is the central data protection regulator for big platforms, conflicts of interest would be inescapable, and, second, that some of these same tensions might easily characterise the EC's tasks in its DSA supervisory and enforcement functions.

The EC's proposal on child sexual abuse material

The controversial new proposal on combating child sexual abuse material (CSAM),[8] presented by the EC in May 2022, similarly shows the conflicting policy objectives it has to deal with. The draft regulation obliges providers to scan private communications to detect CSAM material. In reaction to the proposal, civil society organisations have warned against the staggering risks to privacy, security and integrity of private communications and other fundamental rights brought about by the draft

regulation. The German Federal Commissioner for Data Protection has called the proposal incompatible with EU values and data protection law, for deeply interfering with fundamental rights and democratic principles such as the confidentiality of private communications.

As explained by the EC, the CSAM Regulation builds upon the DSA's horizontal framework, thus acting as *lex specialis*. While the DSA provides a framework for addressing illegal content online in general, the CSAM Regulation introduces more specific rules as regards the fight against a particular form of illegal content. Providers would therefore be subject to a more general systemic risk assessment obligation under the DSA and a more specific one under the CSAM Regulation.

Thus, one could legitimately wonder whether and how risk assessments and mitigation measure choices – undertaken by platforms under the DSA and overseen by the Commission – would be influenced by the CSAM framework (and similar specific regulations adopted in the future). Could the assessment of DSA systemic risks on illegal content and fundamental rights, and the enforcement of such obligations, be impacted in practice by (and assimilated to) CSAM obligations and standards? The Explanatory Memorandum to the proposal[9] seems to confirm this:

> *"Those providers can build on the more general risk assessment in performing the more specific one, and in turn, specific risks identified for children on their*

> *services pursuant to the specific risk assessment under the [CSAM] proposal can inform more general mitigating measures that also serve to address obligations under the DSA." (page 5 of the Explanatory Memorandum)*

Therefore, technologies implemented in the context of CSAM compliance, which translate into extensive forms of surveillance,[10] could potentially also be used to comply with DSA-related obligations.

In particular, conflating the operationalisation of DSA and CSAM assessments and mitigation measures raises the question of whether the Commission might be tempted to adopt CSAM standards, and the underlying fundamental rights balancing (proposed by the same EC), when overseeing and enforcing VLOPs' risk assessment and mitigation under the DSA.

All these problematic aspects are also clearly related to the extensive surveillance risks inherent to the CSAM proposal. While providers' obligations under the DSA (and the e-Commerce Directive) build upon the principle of "no general monitoring or active fact finding", the CSAM proposal revolves around an overhaul of such prohibition of generalised monitoring. In other words, with the CSAM regulation the EC opts for a very different balancing of the (conflicting) rights which underlie that prohibition.

All these issues raise concerns on how the EC, as a DSA enforcer caught between its many other legislative proposals, will solve important and complex evaluations relating to a variety

of fundamental rights and any tensions between those. Given the interlinkages between the CSAM and the DSA proposals, knowing how the EC intends to operationalise the DSA enforcement in practice is more urgent than ever.

Freedom of expression and responses to the Ukraine war

Another important area where tensions might emerge, between the EC's enforcement role under the DSA and its other institutional initiatives, is in the protection of the right to freedom of expression. In this regard, it is worth stressing that content moderation is highly contested and politicised, and questions connected to the perceived legitimacy of the EC, across Europe, in overseeing the regulation of these matters might have been underestimated.

Further, the war in Ukraine has prompted a number of unanticipated developments in the domain of content moderation and platform regulation which are clearly of relevance for the DSA discussion. The EC had a crucial role in some of them: at the end of February, the EC announced a ban on the Russian media outlets Russia Today and Sputnik, which was immediately followed by Council measures prohibiting the broadcasting in the EU of media outlets which are considered essential tools of Russian propaganda. While the measures have been upheld by the General Court of the EU[11] (in the proceedings initiated by RT France), experts have raised doubts[12] on the proportionality of the ban and warned about its implications on freedom of expression and access to information in the EU.

During the third trilogue in March 2022, following the Russian invasion of Ukraine and related Russian disinformation campaigns, the EC proposed to introduce a crisis management mechanism[13] for exceptional circumstances (Article 36 of the final text), in order to supplement the anticipatory and voluntary crisis protocols already set out under Article 37 DSA proposal. Thirty-eight civil society organizations[14] active on digital rights warned that "decisions that affect freedom of expression and access to information, in particular in times of crisis, cannot be legitimately taken through executive power alone". Thus, they urged the DSA negotiators to ensure that this new crisis management system complies with human rights law and includes safeguards against abuses (in particular, time limits, ex-post scrutiny by the EP and a specific definition of crisis).

Concluding remarks

The final DSA text confirms the EC's central role in the DSA supervision and enforcement architecture *vis-à-vis* VLOPs and VLOSEs.

However, the implications of this legislative choice, from a fundamental rights and democratic principles perspective, have not yet been adequately discussed and explored.

The examples discussed in this analysis indicate that central issues of the separation of powers should take centre stage in the current conversation on platform regulation. Careful attention should be paid to the independent design of the DSA's

oversight and enforcement actors, with a view to ensure a fundamental rights-supportive regulatory structure. In this regard, it is essential to understand how the supervision of the VLOPs and VLOSEs will be concretely operationalized within the EC.

References

1. Ilaria Buri and Joris Van Hoboken, "The DSA supervision and enforcement architecture" (*DSA Observatory*, 24 June 2022) <https://dsa-observatory.eu/2022/06/24/the-dsa-supervision-and-enforcement-architecture/> accessed 14 October 2022.

2. Irish Council for Civil Liberties, "EU Ombudsman Is Not Satisfied with EU Commission Answers to ICCL's Complaint about Enforcement of Data Rights" (*Irish Council for Civil Liberties*, 19 July 2022) <https://www.iccl.ie/2022/eu-ombudsman-is-not-satisfied-with-eu-commission-answers-to-iccls-complaint-about-enforcement-of-data-rights/> accessed 14 October 2022.

3. Peter O'Dwyer, "Vestager: There Was a 'Distrust of Ireland as an Enforcer' on Big Tech" *Business Post* (Dublin, 1 October 2022) <https://www.businesspost.ie/news/vestager-there-was-a-distrust-of-ireland-as-an-enforcer-on-big-tech/> accessed 14 October 2022.

4. Ben Wagner and Heleen Janssen, "A first impression of regulatory powers in the Digital Services Act" (*Verfassungsblog*, 4 January 2021) Verfassungsblog <https://verfassungsblog.de/regulatory-powers-dsa/> accessed 14 October 2022.

5. European Data Protection Board, "Statement on the Digital Services Package and Data Strategy" (*European Data Protection Board*, 18 November 2021) <https://edpb.europa.eu/system/files/2021-11/edpb_statement_on_the_digital_services_package_and_data_strategy_en.pdf> accessed 14 October 2022.

6. Svetlana Yakovleva, "Privacy Protection(ism): The Latest Wave of Trade Constraints on Regulatory Autonomy" [2020] 74 University of Miami Law Review 416 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3463076> accessed 19 January 2023

7. Alfred Ng, Vincent Manancourt, Mark Scott and Clothilde Goujard, "Biden Signs Executive Order on EU-U.S. Data Privacy Agreement" *Politico* (Arlington, 7 October 2022) <https://www.politico.com/news/2022/10/07/biden-executive-order-eu-data-privacy-agreement-00060872> accessed 14th October 2022.

8. European Commission, "Fighting Child Sexual Abuse: Commission Proposes New Rules to Protect Children" (*European Commission* 11 May 2022)

<https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2976> accessed 14 October 2022.

9. Proposal for a Regulation of the European Parliament and of the Council Laying down Rules to Prevent and Combat Child Sexual Abuse [2022] COM/2022/209 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2022:209:FIN> accessed 14 October 2022.
10. EDRI, "Johansson's Address to MEPs Shows Why the CSA Law Will Fail the Children Meant to Benefit from It" (*EDRi*, 10 October 2022) <https://edri.org/our-work/johanssons-address-to-meps-shows-why-the-csa-law-will-fail-the-children-meant-to-benefit-from-it/> accessed 14th October 2022.
11. Ronan Ó Fathaigh and Dirk Voorhoof, "Case Law, EU: RT France v. Council: General Court Finds Ban on Russia Today Not a Violation of Right to Freedom of Expression" (*Inforrm's Blog* 19 August 2022) <https://inforrm.org/2022/08/19/case-law-eu-rt-france-v-council-general-court-finds-ban-on-russia-today-not-a-violation-of-right-to-freedom-of-expression-ronan-o-fathaigh-and-dirk-voorhoof/> accessed 14 October 2022.
12. Natali Helberger and Wolfgang Schulz, "Understandable, but Still Wrong: How Freedom of Communication Suffers in the Zeal for Sanctions" (*Media@LSE*, 10 June 2022)<https://blogs.lse.ac.uk/medialse/2022/06/10/understandable-but-still-wrong-how-freedom-of-communication-suffers-in-the-zeal-for-sanctions/> accessed 14th October 2022.
13. Luca Bertuzzi, "DSA: European Commission Pitches Crisis Management Mechanism, Supervisory Fees" (*Euractiv*, 23 March 2022) <https://www.euractiv.com/section/digital/news/dsa-european-commissions-pitches-crisis-management-mechanism-supervisory-fees/> accessed 14 October 2022.
14. EDRi, "A New Crisis Response Mechanism for the DSA" (*EDRi*, 12 April 2022) <https://edri.org/our-work/public-statement-on-new-crisis-response-mechanism-and-other-last-minute-additions-to-the-dsa/> accessed 14 October 2022.

Julian Jaursch

Platform Oversight

Here is what a Strong Digital Services Coordinator Should Look Like

The Digital Services Act requires EU member states to name a "Digital Services Coordinator" (DSC) to coordinate national regulators involved in platform oversight. But the DSCs are more than just "coordinators", as they have to fulfil specific oversight tasks themselves. That is why member states should resist the temptation to build a small-scale coordinator and instead build a strong DSC with skills in data analysis, community management and flexible case-based work.

"[L]andmark rules adopted for a safer, open online environment"[1], the European Parliament declared on its website in the summer of 2022. Parliament had just concluded its negotiations with member states and the European Commission on the Digital Services Act (DSA)[2]. The law provides for new, EU-wide rules for platforms and online marketplaces, including Amazon, Facebook, TikTok and YouTube. The DSA is indeed a big accomplishment. To be sure, there are still clear weaknesses in the law, for example, the limited progress on the problem of "deceptive platform design"[3], or aspects of the "crisis mechanism"[4] introduced shortly before the end of negotiations. Nonetheless, it is at least a recognition that self-regulation by the tech industry has often been insufficient to protect fundamental rights, ensure consumer protection and enable research.

But whether the DSA will actually create a "safer, open online environment" is still completely open. The DSA's success depends on how well it is enforced. The best rules on paper will not achieve much if regulators are not willing or able to enforce them. An unfortunate example of this is the EU's General

Data Protection Regulation (GDPR), which has been suffering from weak enforcement over the past[5] several[6] years[7]. For the DSA, the EU clearly wanted to learn from the GDPR, which is reflected in the DSA's enforcement regime.

How the DSA is supposed to be enforced

The DSA distinguishes between different types of platforms (for instance, hosting providers, search engines and online marketplaces) and between platforms of different sizes. Platforms with more than 45 million users per month in the EU are considered "very large online platforms" (VLOPs). For them, the DSA lists special due diligence requirements (Articles 33-43). Compliance with these due diligence requirements is monitored solely by the Commission (Articles 56, 65-78), with the aim of ensuring a consistent, EU-wide application, contrary to GDPR enforcement. Other rules for very large platforms are also mainly the responsibility of the Commission. For smaller intermediary service providers, national authorities in the respective member states are responsible. Unlike the GDPR, the DSA has clear timelines for cross-border cooperation between national regulators (Articles 57-59).

In each member state, multiple authorities may be tasked with enforcing the DSA (Article 49; Recital 113). This is likely to be the case in many member states because the DSA touches on issues as diverse as consumer protection, media regulation and data protection, for which countries often have separate authorities instead of one dedicated platform regulator. However, to coordinate these agencies and ensure exchange at the

EU level, there must be a single body in each member state acting as the DSC (Articles 49-51). In addition to this coordination role, the DSC must perform important oversight functions itself: It is the complaints body for all users (Article 53), it vets researchers seeking data access to platforms (Article 40) and it can certify out-of-court dispute resolution bodies (Article 21), among other things[8]. It is also part of the newly created European Board for Digital Services (Articles 61-63), bringing together all DSCs and the Commission. While this is mainly an advisory body, the Board can also initiate proceedings against platforms of all kinds (Articles 58, 60) and recommend actions in crisis situations (Article 36).

Who will the DSCs be and what do they have to do exactly?

Legislators in the member states now face the decision of how to set up their DSCs. Will it be an entirely new body? If so, does it take over as the country's single platform agency, merging other national regulators' platform-related tasks into its portfolio? Or is set up merely as a secretariat, forwarding most tasks to existing regulators? If no new body is created, what national regulator will additionally take on the role of the DSC? At least in the months after the conclusion of the DSA, it did not seem as if member states were keen on building the DSC as a centralized, all-in-one platform regulator. Rather, an existing regulator will take on the additional DSC role, allowing other authorities to potentially fulfil some DSA enforcement tasks as well. For instance, France is likely to pick its

newly merged audiovisual and digital communications agency Arcom[9] as the DSC and Ireland is building a new Media Commission[10], too, which will be tapped[11] as the DSC. If there is a DSA enforcement case involving questions on data protection, the French and Irish DSCs would have to coordinate with the respective national data protection agencies or forward the case to them. This could happen, for example, for questions surrounding online advertising transparency or deceptive platform design. In Germany, it is likely that a federal regulator[12] will be named DSC, which would then have to work with state-level media authorities for DSA proceedings pertaining to media regulation. These cases highlight the coordination role the DSC has to play at the national level, ensuring information exchange between regulators.

Yet, there other tasks that the DSC must fulfill and that go beyond national coordination. Consider these hypothetical sample cases and what oversight duties they each entail:

- A DSC requests data from a VLOP to check how the platform detects and mitigates potential risks for public health emanating from its services (Articles 34(1)(d), 40(1)), for example, the sale of supposed miracle cures for COVID-19.

- A person in Italy suspects that an online service operating in Italy but based in Ireland uses deceptive design practices. The user files a complaint with the Italian DSC, which does a first evaluation and forwards it to Ireland (Article 53).

- A research team at a university has found potential DSA violations at a VLOP and alerts the DSC in their country. The DSC writes up a reasoned request for the Commission to become active (Articles 65, 66). This leads to an investigation, in which the Commission involves the DSC (Articles 67(5), 68(2), 69(7)).

- The European Board for Digital Services, which is made up of all DSCs, gives a recommendation to the Commission regarding a current crisis situation, which allows the Commission to require short-term measures from VLOPs (Article 36).

- The internal complaint handling mechanism at a VLOP does not follow DSA standards. The Commission has yet to become active on this and the local DSC is either unwilling or unable to act. Three other DSCs request an investigation via the Board, ultimately leading to a joint cross-border investigation (Articles 56(4), 58(2), 60(1)(b)).

Recommendations for building a strong DSC

The fictitious cases show that the DSC requires skills and structures not only to coordinate various national agencies but also to conduct data analyses, build a community of researchers and other stakeholders, and take part in EU-level enforcement actions. The DSA emphasizes this important role for the DSCs, too (Recital 111), and stipulates certain requirements for the

DSC. It needs to be "completely independent" from political and business interests (Article 50(2), Recital 111), have certain investigatory and enforcement powers (Article 51) and have adequate resources (Article 50(1), Recital 111). Considering these formal requirements and the demands of the sample cases, what could a strong DSC look like?

Independence by law and design

The legal bases to create independent regulators will vary across member states, but beyond this, the way the DSC is built can provide for some independence as well. Leadership that is well-versed in economic and societal issues related to platforms and that is not picked (only) by the government can strengthen the DSC's standing. A transparency registry documenting meetings with lobbyists from all sides in real-time, cooling-off periods for job changes between the DSC and platforms, and strong whistleblower protections could help the DSC gain and maintain the public's trust. Moreover, the DSC should not receive instructions from the government, should have its own budget and regularly report to parliament as well as the public.

Platform experts and data science

The DSA is a data-generating piece of legislation. It contains[13] 20 reporting obligations for VLOPs, the Commission or DSCs, there are various transparency and evaluation reports and, crucially, DSCs and vetted researchers have the right to request data from VLOPs. Analyzing different types of data will require

data science capabilities at the DSC. Various governments and regulators have begun to establish data science units, one example being the French Pôle d'Expertise de la Régulation Numérique[14] (PEReN). The DSC should strongly build up this expertise as well, functioning as the primary national hub for platform research. With a dedicated research budget and data science unit, it could both finance external research and conduct its own studies, especially with a long-term view that civil society research often cannot afford. Data science skills should be paired with the specific expertise needed to understand the systemic platform risks the DSA tries to tackle. For example, the DSC needs to recruit and retain talent well-versed in content moderation, human rights impact assessments, fact-checking and risk management.

Community- and capacity-building via fellowships and an expert advisory council

In addition to developing internal expertise, the DSC should foster structures and a culture that actively engages and builds a community with platform experts. One way to do this could be via fellowships. Companies and not-for-profits employ various forms of fellowships that the DSC could draw inspiration from. Some regulators use this tool as well. For instance, the UK's Information Commissioner's Office seeks fellows[15] to help answer tech policy questions. Another way to tap into external expertise is creating a DSC advisory council or roundtable made up of experts from academia, civil society, business, media and maybe also platform users. These experts

could help in a lot of the cases mentioned above, for instance, regarding data access, complaints or cross-border investigations. There are lots of examples of advisory councils that offer good and bad practices for the DSC, as does the debate around "social[16] media[17] councils[18]". In general terms, for the advisory council not to be just a talking shop, it is necessary to clearly define its role and tasks, incorporate different perspectives and delineate its responsibilities from those of the DSC. Such a structural, continuous forum of exchange might further increase trust in the DSC's oversight work.

Flexible, cross-regime, case-based task forces

The DSC should be designed to work in case-based project groups or task forces. This seems like a suitable set-up for many EU countries, because the topics the DSA addresses are often spread across multiple regulatory fields (for example, consumer protection and media regulation). Thus, cross-regime regulatory cooperation[19] will be necessary, which could be done by a task force comprised of those national regulators with expertise on the specific case. If the case at hand can be clearly placed within the remit of a particular regulator, enforcement would remain with this regulator and the DSC would merely serve as a forum for information exchange. In cases of overlapping or missing responsibilities for some DSA rules, the DSC would step in to oversee compliance itself. For this to work, a collaborative mindset among regulators and a well-built communication system that can connect to or is based on the information exchange system that

the Commission is building (Article 85) are crucial. This type of case-based approach is nothing new at all. It is not only common in private companies, but also in regulators. Individual regulatory decisions – be it regarding monopolies, TV licenses or electricity grids – are, after all, "cases". Within the Commission's Directorate-General for Competition, "case handlers" work on files, e. g., regarding antitrust or state aid. Furthermore, the Commission's proposals on enforcing the DSA[20] and its restructuring of the Directorate-General for Communications Networks, Content and Technology (DG CNCT) hint at a case-based approach as well.

Member states' turn to build innovative platform regulators

When building the necessary structures for a strong DSC, member states might face legal and financial hurdles as well as political opposition. For instance, the inter-agency work envisioned for DSC task forces might not be feasible or, in fact, desired by existing agencies. Finding (and keeping) the right staff is hard anyways, but long recruitment processes in the administration and competition with big tech companies might make this more challenging. Budgetary debates might cause a stir, especially if existing agencies feel like a new "Coordinator" might take money or powers away from them. Ideally, member states would embrace these challenges and treat the development of the DSC as an opportunity to create a platform regulator that is fit to take on future tasks in this area as well, considering other EU legislation on artificial intelligence and the data economy are pending. While a dedicated,

specialized national platform regulator would be the most suitable solution[21], this scenario is unlikely in most member states in the short term. Rather, EU countries will each tap an existing agency as DSC. As a first step in this likely scenario, member states should bring together key national regulators with DSA oversight functions as well as academic and civil society experts to build a strong system for information exchange for the DSC. This could function as a trust-building exercise for agencies that will have to work together to enforce the DSA in the future anyways. Without this type of cooperation to ensure robust enforcement, it will be much harder to proclaim that the DSA has contributed to a "safer and open online environment".

References

1. Yasmina Yakimova, "Digital Services: Landmark Rules Adopted for a Safer, Open Online Environment" (*European Parliament*, 5 July 2022) <https://www.europarl.europa.eu/news/en/press-room/20220701IPR34364/digital-services-landmark-rules-adopted-for-a-safer-open-online-environment> accessed 5 July 2022.
2. Regulation (EU) 2022/2065 of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC [2022].
3. Nienke Palstra, "Brussels Takes on Big Tech: The Good, the Bad and the Ugly" (*Global Witness*, 5 July 2022) <https://www.globalwitness.org/en/blog/brussels-takes-big-tech-good-bad-and-ugly/> accessed 6 July 2022.
4. EDRi, "A New Crisis Response Mechanism for the DSA" (*EDRi*, 12 April 2022) <https://edri.org/wp-content/uploads/2022/04/EDRi-statement-on-CRM.pdf> accessed 13 April 2022.
5. Estelle Massé, "Four Years under the EU GDPR: How to Fix Its Enforcement" (*Access Now*, July 2022) <https://www.accessnow.org/cms/assets/uploads/2022/07/GDPR-4-year-report-2022.pdf>.
6. Johnny Ryan and Alan Toner, "Europe's Enforcement Paralysis: ICCL's 2021 Report on the Enforcement Capacity of Data Protection Authorities" (*Irish Council for Civil Liberties*, 2021) <https://www.iccl.ie/wp-content/uploads/2021/09/Europes-enforcement-paralysis-2021-ICCL-report-on-GDPR-enforcement.pdf> accessed 13 September 2021.
7. Matt Burgess, "How GDPR Is Failing" *Wired UK* (London, 23 May 2022) <https://www.wired.co.uk/article/gdpr-2022> accessed 23 May 2022.
8. Julian Jaursch, "New EU Rules for Digital Services: Why Germany Needs Strong Platform Oversight Structures" (*Stiftung Neue Verantwortung*, 2022) <https://www.stiftung-nv.de/sites/default/files/snv_why_germany_needs_strong_platform_oversight_structures.pdf>.
9. Arcom, "Gouvernance" (Arcom) <https://www.arcom.fr/larcom/gouvernance> accessed 5 August 2022.
10. Department of Tourism, Culture, Arts, Gaeltacht, Sport and Media, "Online Safety and Media Regulation Bill" (Government of Ireland, 18 February 2022) <https://www.gov.ie/en/publication/d8e4c-online-safety-and-media-regulation-bill/> accessed 8 August 2022.

11. Department of Enterprise, Trade and Employment, "Digital Service Act" <https://enterprise.gov.ie/en/what-we-do/the-business-environment/digital-single-market/eu-digital-single-market-aspects/digital-services-act/>.

12. Stefan Krempl, "Bundesnetzagentur will Deutschlands Plattform-Aufseher werden" *heise online* (Hannover, 30 September 2022) <https://www.heise.de/news/Regulierung-Bundesnetzagentur-will-Deutschlands-Plattform-Aufseher-werden-7280311.html> accessed 30 September 2022.

13. Julian Jaursch, "Overview of DSA Delegated Acts, Reports and Codes of Conduct" (*Stiftung Neue Verantwortung*, 15 August 2022) <https://www.stiftung-nv.de/en/publication/overview-dsa-delegated-acts-reports-and-codes-conduct> accessed 28 August 2022.

14. Pôle d'Expertise de la Régulation Numérique, "Who Are We?" (Pôle d'Expertise de la Régulation Numérique) <https://www.peren.gouv.fr/en/equipe/> accessed 5 July 2021.

15. Information Commissioner's Office, "Vacancy: Post Doctoral Research Fellowship in Artificial Intelligence (AI)" (*Information Commissioner's Office*, 19 May 2021) <https://web.archive.org/web/20221104072510/https://ico.org.uk/about-the-ico/jobs/vacancies/vacancy?Advert=xmenYOFfXOq0oZwyOrKD+A==> accessed 18 January 2023.

16. ARTICLE 19, "Social Media Councils" (*ARTICLE 19*) <https://www.article19.org/social-media-councils/> accessed 30 March 2021.

17. Megan Metzger and others, "Social Media Councils: From Concept to Reality - Conference Report" (*Global Digital Policy Incubator, ARTICLE 19 and United Nations Special Rapporteur on Freedom of Opinion and Expression*, 2019) <https://fsi-live.s3.us-west-1.amazonaws.com/s3fs-public/gdpiart_19_smc_conference_report_wip_2019-05-12_final_1.pdf> accessed 31 May 2019.

18. Matthias C Kettemann, "Platform://Democracy: Platform Councils as Tools to Democratize Hybrid Online Orders" (*Hans-Bredow-Institut*, 2022) <https://hans-bredow-institut.de/en/projects/platform-councils-as-tools-to-democratize-hybrid-online-orders> accessed 13 October 2022.

19. Giorgio Monti and Alexandre de Streel, "Improving EU Institutional Design to Better Supervise Digital Platforms" (*Centre on Regulation in Europe*, January 2022) <https://cerre.eu/publications/improving-eu-institutional-design/> accessed 17 January 2022.

20. European Commission, "Sneak peek: how the Commission will enforce the DSA & DMA" (*European Commission*, 5 July 2022) <https://ec.europa.eu/c

ommission/presscorner/detail/en/STATEMENT_22_4327> accessed 5 July 2022.

21. Jaursch, "New EU Rules for Digital Services: Why Germany Needs Strong Platform Oversight Structures" (n 8).

Alessandro Mantelero

Fundamental Rights Impact Assessment in the DSA

As our lives are becoming more and more intertwined with our online actions and behaviours,[1] the rights and freedoms we enjoy in the offline world must be reaffirmed in the online context and in its digital ramifications.

The long-standing substitute role of data protection in the defence of human dignity and individual rights in the digital environment cannot be extended any further. Rather than a catch-all notion of data protection, specific attention must be paid to human rights in their variety and specificity.

As has been the case with the right to privacy in the past, the peculiar nature of the online environment must be taken into account, considering new potential threats to human rights. This requires appropriate forms of assessment and mitigation of potential risks to these rights.

In line with this approach, the Digital Services Act (DSA) draws specific attention to the risks stemming from the design, functioning and use of digital services, considering their adverse effects on fundamental rights and, following the common approach to the protection of human rights, adopts an *ex ante* strategy centred on risk assessment.

The following sections will discuss, briefly and without the ambition of an in-depth analysis, this approach adopted by the EU legislator. Both the main elements of the risk-based framework as set out in the DSA and the approach to risk assessment will be considered.

The scope of the risk-based approach in the DSA

The EU legislator's intention to combine the protection of fundamental rights and market interests is evident in the DSA. As common in early generations of industrial risk regulation, the solutions adopted in the DSA circumscribe a risk-based approach to the most challenging areas, which are for our purposes here the "very large online platforms" or "VLOPs".

Compared to another challenging piece of risk-based EU regulation for the digital sector under discussion, namely the AI Act proposal, the DSA has adopted a size-based criterion rather than a proper risk-focused model (i.e., the high-risk threshold of the AI Act proposal). In this regard, while the size of the platform may impact the level of risk exposure, it has less influence on the other relevant variables in risk assessment, i.e., the probability of adverse consequences and their severity. However, the specificity of the applications considered – predominantly platforms – and their common features may justify a size-based approach in the DSA. This is because the size of a platform is a proxy for risk levels in a context centred on the network effect, which is not necessarily true in other fields – such as AI – where a variety of applications is possible.

Looking at the structure of the DSA, Articles 34, 35, and 37 are the relevant provisions dealing with risk management: Article 34 focuses on assessment, Article 35 on mitigation, and Article 37 on the complementary role of independent audits.

The DSA's risk-based approach covers different categories of risks, not only related to the adverse effects on fundamental

rights. The following five main categories can be identified: (i) illegal content; (ii) negative effects on fundamental rights; (iii) negative effects on civic discourse and the electoral process; (iv) public security; (v) negative effects in relation to gender-based violence, public health protection, the protection of minors, and serious negative consequences to the person's physical and mental well-being.

This variety of sources and types of potential risk may make it difficult to define appropriate and coordinated assessment tools. While specific tools have been developed to counter illegal content and there is some experience in assessing the impact on fundamental/human rights,[2] the evaluation is more complicated with regard to the negative effect on civic discourse and electoral process, as well as in relation to public security, which is a rather broad category in the case of global platforms.

The inclination of the EU legislator to accommodate a broad spectrum of different demands concerning the mitigation of potential risks is also evident in the fifth and last category, which brings together different situations relating to subjective status (minors), conduct (gender-based violence), collective (public health) and individual interests (physical and mental well-being).

The main result of this inclination is a fragmented generalisation of a case-based approach based on past experiences at the expense of a holistic view of potential risks. This mix of different risk categories does not provide a clear framework as needed in a future-proof regulation. The consequence of this

fragmentation is even more impactful for assessment tools, as it entails the development of a variety of specific instruments.

A binary model based on illicit content[3] and prejudice to fundamental rights – which may encompass many of the other risks listed – could thus have been a more straightforward solution, leaving room for case-by-case interpretation, as is usual in the civil law tradition in the field of tort law. On the contrary, this detailed list shows a kind of didactic intent but leads to a more rigid and complicated model, opening up potential conflicting interpretations.

In a similar way, Article 34(1)(b) provides a detailed list of potentially affected rights with explicit references to the Charter of Fundamental Rights of the European Union. Although the rights mentioned in this non-exhaustive list – namely human dignity, respect for private and family life, the protection of personal data, freedom of expression and information, including the freedom and pluralism of the media, the prohibition of discrimination, the rights of the child and consumer protection – are those most at risk in the context under consideration, this detailed approach seems superfluous where a general reference to fundamental rights would have been not only sufficient but even more comprehensive.

Finally, regarding the factual elements to be considered in the assessment, Article 34(2) provides a non-exhaustive list of key aspects to be considered. This provision could have been drafted in line with Recital 57, which states that "When assessing such systemic risks, providers of very large online platforms should focus on the systems *or other* elements that may

contribute to the risks" (emphasis added). This formulation is preferable since it includes contextual elements other than the features of the system. Indeed, the prejudice to fundamental rights is not limited to the design and functioning of platforms, but also concerns the context in which a given system is used (e.g., level of education of users, digital literacy, level of access to services among different groups and communities, etc.).

Assessment and complementary tools

With regard to the risk assessment methodologies, the provisions in the DSA offer limited input, as mentioned above. Following the pattern of industrial production regulation, a periodical (annual) assessment is preferred to the more common continuous assessment used in human rights. This is mitigated by the obligation to conduct such an assessment "in any event prior to deploying functionalities that are likely to have a critical impact on the risks identified" (Article 34(1)). However, the focus is on system functionalities, overlooking external changes that may impact on already implemented functions (e.g., new forms of disinformation campaigns and techniques).

When assessing the use of large platforms from a human rights perspective it should be kept in mind that their impact is not limited to the design of their recommender systems or other system features listed in Article 34.2. Impact assessments should include the overall effects of the "platformisation" of social interaction and their consequences on the enjoyment of

fundamental rights and freedoms:[4] this is a missing point in the framework outlined by the EU legislator in the DSA.

In this regard, the DSA is more in line with the security approach in risk mitigation, focused on the process and products, rather than close to environment or human rights impact assessments, where the emphasis also is on what is outside the system and how technology is likely to affect and change it. While design is necessarily an internal component of platforms, risk is the result of both internal and external factors. Focusing more on the former factor may prevent a holistic perspective.

This is even more true when, as in the DSA, the model adopted is based on self-assessment, which is usually characterised by an internal perspective on potential side effects. In addition, although soft-law instruments (guidelines, best practices, and recommendations) are provided for in the DSA, the competence required to carry out an impact assessment and the way it is to be conducted remain unclear. In Recital 59, there is a reference to "the involvement of representatives of the recipients of the service, representatives of groups potentially impacted by their services, independent experts and civil society organisations", which highlights the importance of integrating "such consultations into their methodologies for assessing the risks and designing mitigation measures, including, as appropriate, surveys, focus groups, round tables, and other consultation and design methods". As demonstrated in several cases in the digital environment, the role of the experts in performing self-assessment risk analysis is crucial, as

is the participation of rightsholders and stakeholders.[5] The DSA should therefore have paid more attention to defining these elements and their requirements. Other experts, in turn, are involved in the audit process, as set out in Article 37, and in this case, a specific condition of independence is required. But the auditors are not explicitly tasked with reviewing the fundamental rights impact assessment carried out by the platform. Although Article 37 is not clear on this point, referring to compliance with "the obligations and with the commitments", reviewing the impact assessment carried out by the platform seems possible. However, given the variety of impacts a platform may have on fundamental rights, the effort required to re-assess the risk may lead to a narrower interpretation,[6] excluding re-assessment. As a result of this second interpretation, the role of audits risks being more formal than substantive, all the more so in a model centred on self-assessment. Therefore, a clear interpretation of this provision is needed, hopefully in favour of re-assessment.

Finally, Article 35 deals with the obligations resulting from risk assessment, focusing on risk mitigation. The option in favour of mitigation (which it means that a residual risk persists) rather than risk prevention is in line with the recent approach of the EU legislator. As in the AI Act proposal, this focus on mitigation is based on the idea that some uses of technology in the digital society are characterised by an endemic risk that we cannot fully prevent. We, therefore, accept this risk given the potential benefits provided by technology. This is in line with the legal approach already used in the regulation of

the risk society,[7] although it departs from the stronger position adopted in the GDPR where no high-risk applications are permitted.

Since the DSA does not set any risk threshold and only refers to the reasonableness and proportionality of the measures adopted, we can conclude that – as in the AI Act proposal – high-risk uses are permissible, provided they are supplemented by mitigation measures, without requiring the risk to fall below the high-risk threshold. On the other hand, compared to the AI Act proposal, the absence of a list of high-risk uses leaves more room for compliance assessment by the competent authorities (see also Article 35(3) guidelines).

In this context, research organisations can play a role in detecting, identifying, and understanding systemic risks (Article 40(4)). This may be an important contribution from academia, although the requirement of independence from commercial interest needs some clarification in an academic environment characterised by increasing research funding programmes sponsored by large platforms, which may affect the actual independence of beneficiaries in their future research.

Concluding remarks

The attention to fundamental rights in the new wave of EU digital regulation, confirmed in the DSA, is a significant step towards a more articulated and appropriate framework for protecting people in a context characterised by pervasive technologies that are often developed without adequate consideration of their impact on society. However, the emphasis on the

risk-based approach and accountability in the DSA, as well as in the AI Act proposal, is not supported by adequate models for conducting impact assessment and the existing practices in human rights impact assessment show some limitations in being extended to the digital context. For this reason, referring to commonly used risk assessment parameters (severity, provability, likelihood, scale, and reversibility, see Recital 56) is not sufficient, and a specific methodology is needed to operationalise them in the context of digital societies.[8] Although, in dealing with these issues, the DSA suggests giving "due regard to relevant international standards for the protection of human rights", the important reference to the UN Guiding Principles on Business and Human Rights (Recital 47) does not solve practical issues concerning the development of risk assessment model. While the Guiding Principles may play a role in countries where the level of human rights protection is low – although their actual impact has been questioned[9] –, the influence of these principles is more limited in EU countries where human rights principles are already largely covered by EU and national provisions.

Like other pieces of the new wave of EU regulation of the digital society, the DSA thus represents an important contribution to the development of a more human-centred technology, where the protection of human dignity and fundamental rights play a crucial role, but a major implementation effort will be needed.

References

1. The Onlife Initiative, "The Onlife Manifest" in Luciano Floridi (ed) *The Onlife Manifesto: Being Human in a Hyperconnected Era* (Springer International Publishing 2015) <https://doi.org/10.1007/978-3-319-04093-6_2> accessed 2 February 2022.

2. See, e.g., The Danish Institute for Human Rights, "Human rights impact assessment guidance and toolbox" (*The Danish Institute for Human Rights*, 25 August 2020) <https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-toolbox> accessed 19 October 2022; The Danish Institute for Human Rights, "Guidance on HRIA of Digital Activities" (*The Danish Institute for Human Rights*, 2020) <https://www.humanrights.dk/publications/human-rights-impact-assessment-digital-activities> accessed 19 October 2022.

3. See also Ilaria Buri and Joris van Hoboken, "The Digital Services Act (DSA) Proposal: A Critical Overview" (*DSA Observatory and Institute for Information Law*, 2021) 34 <https://dsa-observatory.eu/wp-content/uploads/2021/11/Buri-Van-Hoboken-DSA-discussion-paper-Version-28_10_21.pdf> accessed 25 September 2022. Although most of the allegedly illegal content will simply be removed on the basis of notice and takedown procedures, without a more extensive legal assessment, this is of limited relevance from the point of view of risk assessment, the latter being a different ex ante evaluation based on potential risks. The critical issue is thus not the lack of a more extensive legal assessment but the difficulty in defining the illegal nature of some content and consequently the content monitoring systems to be adopted for risk mitigation, as several aspects are contextual (e.g., culture-dependent aspects related to defamation or context-dependent legitimate use of copyrighted materials).

4. See Ellen Goodman and Julia Powles, "Urbanism Under Google: Lessons from Sidewalk Toronto" (2019) 88 Fordham Law Review 457 <https://doi.org/10.2139/ssrn.3390610>; Mantelero, *Beyond Data: Human Rights, Ethical and Social Impact Assessment in AI* (T.M.C. Asser Press The Hague 2022) 76-82.

5. See Mantelero (n4) 104-109 and 127-130.

6. See Buri and van Hoboken (n 3) 37.

7. See, e.g., Guido Calabresi and Philip Bobbitt, *Tragic Choices* (W. W. Norton & Company 1978).

8. Mantelero (n4).
9. See Surya Deva, "Treating Human Rights Lightly: A Critique of the Consensus Rhetoric and the Language Employed by the Guiding Principles" in David Bilchitz and Surya Deva (eds), *Human Rights Obligations of Business: Beyond the Corporate Responsibility to Respect?* (Cambridge University Press 2013) <https://www.cambridge.org/core/books/human-rights-obligations-of-business/treating-human-rights-lightly-a-critique-of-the-consensus-rhetoric-and-the-language-employed-by-the-guiding-principles/20E6A9EC8600D94AE7D7900FB4FAAAF3> accessed 31 August 2022.

Asha Allen

An Intersectional Lens on Online Gender-Based Violence and the DSA

The European Union (EU)'s Digital Services Act (DSA) introduces novel mandatory due diligence obligations for online platforms, with additional obligations for very large online platforms (VLOPs) to address potential societal risks posed by the provision of their services, such as risks to fundamental rights, participation in civic discourse, or as this essay will focus upon, the risk of online gender-based violence (OGBV). This approach of mandatory due diligence obligations is a recognition by EU co-legislators of the complexity of the issues the DSA aims to address. Striking the balance between the protection of free expression, addressing illegal content and creating a safe online environment will be challenging. However, the DSA is ambitious in its aims; if effectively implemented, these provisions have the potential to set important standards for tackling some of the most pervasive harms of the digital ecosystem.

Efforts to address these systemic risks and the related mechanisms for access to redress will require the adoption of an intersectional methodology as presented by Kimberlé Crenshaw[1] which will be elaborated below. Without such a methodology, the development of risk assessments by online platforms, the subsequent mitigation measures, evaluation by the European Commission and the effectiveness of and access to remedy provisions will simply fail to provide the necessary mechanisms for those most acutely impacted by these rights violations.

Tackling online gender-based violence through due diligence measures

Balancing freedoms whilst addressing harms is a fine line which, if not approached correctly in the DSA's implementation, risks further infringing rights, especially for those already historically marginalised within society. The obligations for VLOPs to conduct comprehensive assessments of systemic risks to fundamental rights from their services (Article 34), to develop and implement mitigation measures (Article 35), and to be subjected to independent audits to assess their efforts (Article 37), if implemented appropriately, may set a global precedent for striking this balance. After extensive advocacy from civil society and numerous amendments to the text, EU co-legislators chose to explicitly name a few specific systemic risks including negative consequences in relation to OGBV.

The inclusion of OGBV as a systemic risk within the DSA aligns with the EU's aim to criminalise certain forms of OGBV within a draft Directive to Combat Violence against Women and Domestic Violence[2], published in March 2022. The Directive seeks to establish minimum criminal standards for the perpetration of cyberstalking, non-consensual sharing of intimate or manipulated material and cyber-incitement to violence or hatred. The prevalence of OGBV in Europe has only magnified over the years. As documented by the European Institute for Gender Equality[3], 51% of young women hesitate to engage in online debates after witnessing or directly experiencing online abuse. Women of colour and non-binary people are at in-

creased risk[4] of experiencing OGBV.

Content moderation efforts by some online platforms to address OGBV continue to fall short. Reporting mechanisms often force users to attribute their experiences to predetermined categories which fail to capture[5] the multifaceted nature of the abuse. Content moderators are not provided with relevant, gender-sensitive training and many who report instances of OGBV feel "left in the dark"[6] about the outcome of their reports or are informed that their experience did not violate community standards. A handful of large online platforms committed to making substantive improvements[7] at the UN Generation Equality Forum. However, progress is yet to be made.

OGBV exists on a spectrum and can take many forms, including actions that may not rise to the level of illegal conduct, which nevertheless has a chilling effect on women and non-binary people's speech[8]. Therefore, the provisions of the DSA will need to address the systemic risks that stem from non-illegal conduct that nevertheless results in abuses. This would seem challenging, however, researchers have reiterated that comprehensive coordination between legislators, online platforms and civil society[9] to holistically analyse and address such phenomena is the best method to tackle systemic risks such as OGBV. Mandatory due diligence obligations must be accompanied by effective accountability mechanisms to ensure online platforms cannot renege on their responsibilities. Consultation with civil society, who can develop policy and enforcement recommendations should be better informed by an ever-increasing library of analyses based on increased access

to data for researchers. This is why the DSA is a concrete opportunity; the cyclical nature of the due diligence obligations provides a solid foundation for all stakeholders to consistently improve upon their efforts to evaluate and mitigate these systemic risks.

Intersectionality

We do not experience our lives in silos; the experiences of, for example, a woman of colour who is a member of a religious minority, reflect the unique intersections of those different identities and go beyond a summation of the experiences of women, of people of colour, and of religious minority groups. This reality means that in order for the risk assessments of the online platforms to be informative and effective, and for the subsequent evaluations of the European Commission to identify any shortcomings, a comprehensive understanding of how these forms of discrimination may intersect will need to be developed; adopting an intersectional methodology is, therefore, the best approach. Therefore, the risk assessments should be envisaged as Human Rights Impact Assessments (HRIAs), which are extensive, cyclical processes[10] of identifying, understanding, assessing and addressing the adverse effects of the business project or activities on the human rights enjoyment of impacted rights-holders. This process will not only identify specific impacts but their severity and how they may *intersect* with other fundamental rights violations.

Intersectionality is an analytical framework for understanding how aspects of a person's social and political identities

combine to create different modes of discrimination and privilege. Concretely, the method looks at the interconnected nature of social categorisations such as race, class, and gender, which can create overlapping and interdependent systems of discrimination or disadvantage. The methodology can be applied in various iterations such as in research, data analysis and in *ex ante* or *ex post* analyses of the effectiveness of a given policy or legislation for specific groups. This facilitates a more critical policy analysis and deeper understanding for lawmakers of how policy operates in different contexts, thereby leading to more progressive and inclusive legislative frameworks.

The adoption of this methodological framework within the risk assessments and the associated provisions of the DSA is an indispensable approach in ensuring that these assessments do not become empty checkbox exercises. Thus, as a first step, the assessments of the systemic risk of online abuse will need to have specific indicators related to the experience of OGBV amongst different marginalised groups, before then assessing how this systemic risk intersects with others identified in the DSA, such as the risk to civic discourse. For example, online platforms conducting the assessments, and organisations who will later on conduct audits on these efforts, could ask questions such as: *Are there additional variables to consider when developing content moderation mechanisms to address online OGBV? Do we need to provide more opportunities for users to give context to their experiences? Or do our current community standards address or maintain structural inequalities?*

Gendered disinformation

Gendered disinformation, as an example, flows from the same patriarchal context in which people experience OGBV and is often targeted at journalists, advocates and political candidates. Gendered disinformation characterises women candidates[11] as not being qualified, lacking the requisite knowledge, intelligence, or experience for the role, or as persons who lie, are too emotional for the task, prone to aggression, or lacking sanity. Once again women of colour are more likely to be the subject of disinformation when compared to other women or to men of colour and this disinformation is likely to include or be accompanied by racial discrimination[12]. Gendered disinformation, therefore, is based on misogyny but can simultaneously intersect with discrimination based on racism, ableism, religious identity etcetera and poses a risk to free expression, human dignity and to women's participation in civic discourse, all of which are specifically identified within the risk assessment provision of the DSA.

Online platforms developing these assessments, and indeed the European Commission which will assess and enforce these evaluations must engage in a cross-sectional manner with consistent civil society engagement. Primarily, the assessments that will be conducted in relation to each of the systemic risks identified should be followed by subsequent analyses in which findings are cross-referenced. For example: *Do the demographics who have been identified as most vulnerable correlate/overlap?; Are the impacts of one systemic risk resulting in the*

direct experience of another? In brief, the Article 34 risk assessments should only be considered concluded when the analyses on each systemic risk are then cross-reviewed in conjunction with one another.

Residual impact

The incorporation of an intersectional approach within the risk assessments and mitigation measures would positively impact the broader provisions governing VLOPs in the DSA. For example, efforts to improve content moderation mechanisms can avoid previously documented errors,[13] which led to women of colour being at increased risk of over-enforcement, whilst the abuse they face remains largely unaddressed by the reporting mechanisms in place. Similarly, analyses on how systematic risks impact communities differently will aid moderators managing Internal Compliant Mechanisms (Article 20) and entities engaged as Out-of-Court Dispute Settlement Bodies (Article 21) in reducing the risk of reaching inappropriate resolutions, which fail to address the unique impacts of these experiences. Moreover, a more comprehensive understanding of how a person may have to contend with multiple sources of oppression can contribute to more equitable treatment for marginalised communities within these bodies, who continue to face discriminatory treatment[14] or secondary victimisation[15] such as victim blaming within institutional or judicial contexts.

Civil society can assist in ensuring an intersectional approach in all these areas is adopted; the final Regulation in

fact includes several specific references to the need for civil society consultation, particularly within the due diligence provisions. A concrete example is the provisions related to access to data (Article 40) which includes civil society organisations among the entities that can conduct research. Researchers may for example request cross-sectional data points as one way of developing comprehensive analyses on issues such as OGBV and its acute impact on marginalised communities. The research community has emphasised[16] that, without data, it is unclear whether mitigation efforts like blocking accounts actually make a difference in the behaviour of those posting abusive content. Access to such data and the subsequent research developed is vital as marginalised communities already face an uphill battle in access to justice.

Conclusion

A "one size fits all" approach to the DSA's due diligence obligations, most notably the risk assessments and subsequent content moderation adaptations, will result in the considerable efforts placed in defining these obligations being a wasted endeavour. In the case of those most gravely impacted by OGBV, such an approach would fail victims. The European Commission needs to deeply and urgently reflect upon how it will harmonise the vast regulatory framework it has established. In this case, the Directive on Violence Against Women and Domestic Violence will bring certain forms of OGBV into the purview of illegal content, and the mandatory due diligence

obligations of the DSA, to ensure these combined efforts do not prove empty.

In short, the assessment of systemic risks, subsequent mitigation measures and the mechanism put in place to ensure access to redress must all be developed using an intersectional methodology and stakeholder consultation must be consistent and meaningful. Concretely, a formal mechanism by which civil society can actively participate, evaluate and provide recommendations for improved enforcement and implementation should be established. The EU cannot purport to be the global regulatory leader in online content governance if it subsequently fails to enforce, and make useful, the very provisions of the DSA that make the Regulation revolutionary.

References

1. Kimberle Crenshaw, "Mapping the Margins: Intersectionality, Identity Politics, and Violence against Women of Color" (1991) 43(6) Stanford Law Review 1241. <https://www.jstor.org/stable/1229039> accessed 20 September 2022.
2. Proposal for a Direction of the European Parliament and of the Council on combating violence against women and domestic violence [2022] COM/2022/105 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0105> accessed 21 September 2022.
3. European Institute for Gender Equality, "Cyberbullying restricts young women's voices online" (*European Institute for Gender Equality*, 11 October 2018) <https://eige.europa.eu/news/cyberbullying-restricts-young-women s-voices-online> accessed 20 September 2022.
4. Dhanaraj Thakur and DeVan L. Hankerson, "Facts and their Discontents: A Research Agenda for Online Disinformation, Race, and Gender" (*Center for Democracy & Technology*, 2021) <https://cdt.org/wp-content/uploads/2021/02/2021-02-10-CDT-Research-Report-on-Disinfo-Race-and-Gender-FINAL.pdf> accessed 18 September 2022.
5. World Wide Web Foundation, "The impact of online gender-based violence on women in public life" (*World Wide Web Foundation*, 2020) <https://webfoundation.org/2020/11/the-impact-of-online-gender-based-violence-on-women-in-public-life/> accessed 22 September 2022.
6. ibid.
7. Blathnaid O'Dea, "Tech giants commit to tackling online abuse of women" (Silicon Republic, 6 July 2021) <https://www.siliconrepublic.com/business/online-abuse-commitments-facebook-google-twitter-tiktok> accessed 22 September 2022.
8. Dhanaraj Thakur and DeVan L. Hankerson (n4).
9. Glitch UK and End Violence Against Women Coalition, "The Ripple Effect: COVID-19 and the Epidemic of Online Abuse" (*Glitch UK and End Violence Against Women Coalition*, September 2020) <https://glitchcharity.co.uk/wp-content/uploads/2021/04/Glitch-The-Ripple-Effect-Report-COVID-19-online-abuse.pdf> accessed 20 September 2022.
10. The Danish Institute for Human Rights, "Introduction to human rights impact assessment" (*The Danish Institute for Human Rights*) <https://www.humanrights.dk/tools/human-rights-impact-assessment-guidance-t

oolbox/introduction-human-rights-impact-assessment> accessed 20 September 2022.

11. Dhanaraj Thakur and DeVan L. Hankerson (n4).
12. Ibid.
13. Ángel Díaz and Laura Hecht-Felella, "Double Standards in Social Media Content Moderation" (*Brennan Center for Justice*, 2021) <https://www.brennancenter.org/our-work/research-reports/double-standards-social-media-content-moderation> accessed 22 September 2022.
14. Chiara Liberati, "Study Shows EU Justice Systems Discriminate Against Ethnic Minorities" (*Civil Liberties Union for Europe*, 11 February 2019) <https://www.liberties.eu/en/stories/disparity-against-foreigners-in-criminal-justice-systems-across-the-european-union/16684> accessed 21 September 2022.
15. European Institute for Gender Equality, "Secondary Victimisation" (*European Institute for Gender Equality*, 2016) <https://eige.europa.eu/thesaurus/terms/1358> accessed 19 September 2022.
16. World Wide Web Foundation (n5).

Catalina Goanta

Now What

Exploring the DSA's Enforcement Futures in Relation to Social Media Platforms and Native Advertising

After lengthy political debates, the Digital Services Act (DSA) has finally been agreed upon. Now, all attention is shifting towards how the European Union's most meaningful reform in the sphere of platform governance in the past two decades will look like in practice. The question of enforcement has already been getting considerable attention, not only in academic exchanges such as the Verfassungsblog's earlier DSA/DMA Symposium[1], but also in mainstream media, with the main concern being that the resources put forth by the European Commission are too humble when compared to the DSA's far-reaching goals. Indeed, the DSA's nature, the nature of the markets it aims to govern, as well as the plethora of stakeholders involved in platform governance make enforcement expectations more utopic than realistic.

However, the responsible digitalisation of platform compliance can, at least to a certain extent, modernise and simplify market monitoring. In this short essay, I will reflect on some of the enforcement implications of the paradigm shift proposed by the DSA with respect to its framing of illegal content.

To this end, I will first discuss the definition of "illegal content" and its extension to sectoral regulation; second, I will re-visit the discussion of native advertising and highlight how it currently falls in a grey and overly complicated applicable framework in between the DSA and sectoral regulation; and lastly, I will briefly explore a potential alignment solution I developed together with Prof. Anda Iamnitchi[2] and Thales Bertaglia[3] and which was published and presented as a paper

at the 2022 ACM Conference on Fairness, Accountability, and Transparency (the full paper can be found here).[4]

The nature of the DSA: One for all and all for none

Unlike its predecessor, the E-Commerce Directive, the DSA actually defines "illegal content" in Article 3(h), using a broad definition:

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

As elaborated in Recital 12 DSA, this definition fulfils the DSA's goal of drawing an equal sign between online and offline illegality. In addition, the Recital clearly states that illegal content should "be defined broadly to cover information relating to illegal content, products, services and activities". Included in the illustrative examples are the more traditional categories of illegal content such as child sexual abuse, but also emerging forms of illegal content such as unlawful non-consensual sharing of private images, or online stalking. In addition, the list of illustrative examples also includes "the sale of products or the provision of services in infringement of consumer protection

law", and Recital 68 DSA further specifies that even advertisements themselves may be illegal content.

The definition and subsequent examples acknowledge a new paradigm of illegality: from criminal illegality to content regulation. In contrast, the E-Commerce Directive focused on a narrower understanding of illegality, but also of content. For instance, references to consumer protection dealt more with the transparency requirements relating to e-commerce transactions, than with the actual concept of content illegality. This is understandable, since in the 2000s, online platforms were much more specialised, which is no longer the case today, as platforms increasingly copy each other's affordances.

As a result of illegality, and in combination with the prohibition of a general obligation to monitor (Article 8 DSA), platforms may be exempted from their liability for hosting such illegal activities or content if they "act expeditiously to remove or to disable access to that content" (Recital 22). In addition, platforms have the obligation of setting up notification mechanisms available to any individual or entity to report illegal content (Article 16 DSA).

The action undertaken by the platform may be:

- voluntary (Article 7), by which platforms carry out their own investigations and measures for detecting, identifying, removing, or disabling access to illegal content; and
- mandatory (Article 9), when platforms receive an administrative or judicial order to act against illegal content.

This broader understanding of illegal content is a double-edged sword. On the one hand, it clarifies that every item of "information" on the Internet may be content, and that content may very well fall under a web of applicable rules from a content regulation perspective. I argue this to be a positive development, since the earlier private regulatory adaptations to the E-Commerce Directive have led to platforms creating visible priorities for voluntarily monitoring certain types of content (e.g., criminally illegal content), while completely ignoring other types (e.g., violations of consumer protection). For instance, in a study[5] I conducted with Pietro Ortolani[6], we looked at four social media platforms (Twitter, Facebook, TikTok and Twitch) to understand what type of content could be reported by users, and we found that the predominant categories were criminal activities and intellectual property infringements. At the time when the study was conducted, the users of these platforms could not complain about content that did not abide by consumer protection standards, such as information duties or unfair practices. For instance, traders are required to disclose information such as address, contact, price and withdrawal rights details, and while these information duties have been central for marketplace governance, social media platforms have generally not developed any specific visual verification or affordances to communicate these details to their users. However, in the light of the broad definition of illegal content, it can be argued that platforms will have to enable reporting mechanisms under Article 16 for more categories of content than they have been acknowledging so far.

The DSA is thus a bridge between different types of content regulation, as can also be seen in Recital 68, which acknowledges the complementing role of the DSA vis-à-vis media and consumer regulation:

> *"Finally, this Regulation complements the application of the [Audiovisual Media Services Directive] which imposes measures to enable users to declare audiovisual commercial communications in user-generated videos. It also complements the obligations for traders regarding the disclosure of commercial communications deriving from the [Unfair Commercial Practices Directive]." (emphasis added)*

On the other hand, the DSA does not really elaborate on how complementarity will look like in practice. From an interpretation perspective, it will be interesting to see how closely courts, including the Court of Justice of the European Union, will interpret the DSA in relation to its supposed complements. Perhaps even more importantly, the complementarity of the DSA in relation to other sectoral regulation will also stumble at the enforcement level. As an example, Article 40 DSA refers to an obligation of very large online platforms (VLOPs) and very large online search engines (VLOSEs) to provide "access to data that are necessary to monitor and assess compliance with this Regulation" to the European Commission or the European Board for Digital Services, the new EU-wide entity tasked with DSA oversight. However, in the case of consumer protection, national enforcement authorities also have quite wide

data access rights for investigation purposes, as can be seen in the Consumer Protection Cooperation Regulation (CPC Regulation)[7]. Article 3(a) CPC Regulation states that among the investigation powers of competent authorities is also:

> *"the power of access to any relevant documents, data or information related to an infringement covered by this Regulation, in any form or format and irrespective of their storage medium, or the place where, they are stored."*

Yet the picture of how these powers will be exercised in parallel or in cooperation is far from clear. References to such overlap are not many and are not compelling (e.g., Article 57 DSA mentioning that "where appropriate, the [national] Digital Services Coordinator receiving a request by another Digital Services Coordinator to provide specific information [...] may involve other competent authorities or other public authorities of the Member State in question".)

Blind spot under the microscope: Native advertising on social media

The main danger of the lack of clarity with respect to the complementarity of the DSA in relation to other sectoral regulation is that it will create grey areas that will lead to underenforcement. Take for instance the influencer economy as a great example of a menu of consumer protection issues from which platform users must be protected. Since an earlier contribution on native advertising[8], a lot has happened on social media:

- In July 2022, YouTube made a deal with the well-known Canadian dropshipping platform Shopify[9], allowing YouTube users to purchase goods and services in real time as they watch content on the platform;

- As of June 2022, Twitter has made its Twitter Shops module available[10] to all its merchants in the United States;

- In May 2022, TikTok launched an "industry-first ad solution" called Branded Missions[11] that internalised the until then off-platform influencer marketing supply chain, allowing brands to offer advertising tasks to creators, mediated by the social media platform. Twitch continues to use a similar setup, called the Bounty Board[12], which was launched in 2018 and which allows streamers to engage in sponsorship deals without any other third parties than Twitch.

These are only a few examples that shape how social media is no longer a space solely dedicated to social networking and/or content delivery, but due to the booming monetisation policies pursued by platforms, it is a transactional space full of advertising and offers for products. Unfortunately, the DSA does not show the foresight of accounting for these market changes – doing so will at least entail some creative interpretation.

According to Recital 1, the DSA acknowledges "online social networks *and* online platforms allowing consumers to conclude distance contracts with traders" as separate categories

(emphasis added, see also Recital 13). So how are we to qualify a platform like Instagram, which is both? Leaving aside the fact that Instagram has a Checkout function in the United States, making it a straightforward marketplace for the purpose of that jurisdiction, even the European version of the app features a "Shopping" explore section, full of content from both traditional traders (e.g., companies selling to consumers), as well as emerging traders such as influencers. The latter are considered traders firstly because of offers/invitations to treat for goods or services they provide directly to consumers (e.g., selling digital courses or selling merchandise), and secondly because they are providers of commercial services in the form of advertising, to which consumers are exposed. This has led to national consumer enforcement authorities such as the Belgian Ministry of Economy[13] to ask influencers to abide by the information duties which traders are normally subjected to (e.g., disclosing trader identity, physical address), as a result of the application of the Consumer Rights Directive (CRD)[14] and the Unfair Commercial Practices Directive (UCPD)[15].

On the basis of our earlier exploration of the definition of illegal content, I would argue that not fulfilling transparency duties, or violating the prohibition of undisclosed advertorials, are clear violations of the European consumer *acquis*, and thus are illegal content. However, two main problems arise in this analysis. First, such transparency obligations are likely not covered by the DSA itself: if social media platforms are not interpreted as "online platforms allowing consumers to conclude distance contracts with traders", they will not be subjected to

specific obligations such as the compliance-by-design obligation enshrined in Article 31 DSA on information duties similar to the CRD. Moreover, due to the limited definition of "advertisements" in Article 3(r) DSA, influencer marketing has been specifically kept out of the DSA's framework for advertising, applicable to *inter alia* social media platforms (e.g., Article 26 DSA).

According to Article 3(r), advertising has a remuneration element which involves the platforms, and this excluded as such any off-platform advertising (e.g. contracts between brands and influencers which are not mediated by the social media platform). However, looking at the examples of on-platform influencer marketing as monetisation products currently pursued by platforms, some influencer marketing practices will be covered by this definition. As a result, the DSA, as a regulation designed around platform liability, will not be able to directly tackle a substantive proportion of the apparent issues. Second, the aforementioned consumer *acquis* provisions have not been developed for platforms, but for the traders providing the advertising or the contractual options such as the influencers themselves, in which case the scalability of monitoring requires policy choices that may reflect agency resources (e.g. only monitoring the biggest influencers due to visibility). Therefore, under national law, platforms – although at the front, left and centre of social commerce – are not the focus of enforcement.

Legal compliance API: A middle way

As a means to standardise data access, APIs are already embraced by social media platforms, more or less in compliance with Article 40(7) DSA. Recently, YouTube opened its API to researchers[16], and TikTok is planning to do the same[17] later in the year. If you are not familiar with the API concept, imagine it as a way for two or more systems to communicate with one another. In the case of the legal compliance API proposed by my co-authors and I, one communicating system would be a social media platform, and the other a number of DSA enforcement authorities, as well as other relevant public authorities, that need to coordinate on the platform's compliance with the actions necessary to be taken with respect to illegal content. A legal compliance API would be different than a research API, as it would be focused on the translation of the legal compliance tasks into the parameters of checking for compliance with, for instance, the hosting of content that is illegal or non-compliant with European consumer protection rules.

Article 44 DSA on standards elaborates that APIs could also be developed as voluntary standards for the submission of notices by trusted flaggers, as well as for advertising repositories (Article 39 DSA), particularly supported by the European Commission and the European Digital Services Board. Although vague, the present references to APIs in the DSA raise a concern relating to the streamlining not only of data standards but investigation practices by enforcement authorities. As Member States race into digitalisation with data units, all existing

authorities enforcing European Union (and national) law will have a stake in digital investigations and enforcement including data protection authorities, media authorities, consumer authorities, etc. If the DSA enforcement does not take this into account, and in its administrative limitations, creates standards only relevant for the powers of DSA-related authorities, this will lead to potentially harmful inconsistencies in digital enforcement which will enable platforms, as Laux et al. mention[18], to leverage their data dominance against a crowd of uncoordinated regulators with vastly divergent capacities and practices around the implementation of European law.

It is of course highly important that any digital enforcement mechanisms that contribute to surveillance (such as market monitoring), are developed in an accountable way, taking into account the wide-reaching implications of automated decision-making, both from a systems perspective, as well as from a procedural perspective. In my opinion, there is no other alternative to digital monitoring. Platforms already have the upper hand in technology and scale, and public oversight can do little to catch up with that – but it needs to at least try and reign in some of the uncontrolled platform discretion under the scrutiny of the rule of law through well-coordinated and well-designed further digitalisation.

References

1. "To Break Up or Regulate Big Tech? Avenues to Constrain Private Power in the DSA/DMA Package", Max Planck Institute for Innovation and Competition Online Symposium (*Verfassungsblog*, September 2021) <https://verfassungsblog.de/category/debates/power-dsa-dma/>.
2. Adriana Iamnitchi <https://www.maastrichtuniversity.nl/p70074082>.
3. Thales Bertaglia <https://www.maastrichtuniversity.nl/p70068231>.
4. Catalina Goanta, Thales Bertaglia and Anda Iamnitchi, "The Case for a Legal Compliance API for the Enforcement of the EU's Digital Services Act on Social Media Platforms" (*ACM FAccT Conference*, 2022) <https://facctconference.org/static/pdfs_2022/facct22-107.pdf>.
5. Catalina Goanta & Pietro Ortolani, "Unpacking content moderation: The rise of social media platforms as online civil courts", in Xandra Kramer, Jos Hoevenaars, Betül Kas & Erlis Themeli (eds.), *Frontiers in Civil Justice* (Elgar 2022), pp. 192-216.
6. Pietro Ortolani <https://www.ru.nl/en/people/ortolani-p>.
7. Regulation (EU) 2017/2394 of the European Parliament and of the Council of 12 December 2017 on cooperation between national authorities responsible for the enforcement of consumer protection laws [2017] OJ L 345/1 (CPC Regulation).
8. Catalina Goanta, "Human Ads Beyond Targeted Advertising: Content monetization as the blind spot of the Digital Services Act" (*Verfassungsblog,* 5 September 2021) <https://verfassungsblog.de/power-dsa-dma-11/>.
9. David Katz, "Ready, Set, Shop on YouTube" (*YouTube Official Blog*, 19 July 2022) <https://blog.youtube/news-and-events/youtube-shopify-integration-merch-shopping/>.
10. Justin Hoang & David Lietjauw, "Twitter Shops: More space to shop" (*Twitter Blog*, 1 August 2022) <https://blog.twitter.com/en_us/topics/product/2022/twitter-shops-more-space-to-shop>.
11. "TikTok, Introducing TikTok Branded Mission: Inspiring Brand and Creator Collaborations" (*TikTok*, 18 May 2022) <https://newsroom.tiktok.com/en-us/introducing-tiktok-branded-mission-inspiring-brand-and-creator-collaborations>.
12. Theo Salaun, "Streamer accidentally leaks how much money Twitch Bounties can reward" (*Dexerto*, 18 November 2020) <https://www.dexerto.com/

entertainment/streamer-accidentally-leaks-how-much-money-twitch-bounties-can-reward-1457079/>.

13. Hanne De Belie, "Boete tot 80.000 euro voor influencers als ze adres niet delen: 'Wat als hier iemand voor mijn deur staat?'" (*Nieuwsblad*, 8 August 2022) <https://www.nieuwsblad.be/cnt/dmf20220807_95887641>.
14. Directive 2011/83/EU of the European Parliament and of the Council of 25 October 2011 on consumer rights [2011] OJ L-304/64 (CRD).
15. 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 [2005] OJ L-149/22 (UCPD).
16. YouTube Researcher Program <https://research.youtube>.
17. Emma Roth, "TikTok to provide researchers with more transparency as damaging reports mount" (*The Verge*, 27 July 2022) <https://www.theverge.com/2022/7/27/23280406/tiktok-researchers-api-transparency-damaging-reports-china>.
18. Johann Laux, Sandra Wachter & Brent Mittelstadt, "Taming the few: Platform regulation, independent audits, and the risks of capture created by the DMA and DSA" (2021) 43 Computer Law & Security Review 105613.

Pietro Ortolani

If You Build it, They Will Come

The DSA "Procedure Before Substance" Approach

Content moderation is not only an Internet governance problem; it is also, unavoidably, a form of *de facto* adjudication. Online platforms make determinations that affect individual rights, whenever they decide whether to remove content, suspend/terminate accounts, or impose other restrictions. This is true not only for the user posting the content but also for third parties (including vulnerable or marginalised groups) seeking remedies against online harm. As a result, platforms are routinely required to balance legal entitlements against each other. Such a balancing test, traditionally considered as part and parcel (although not a monopoly) of the judicial function[1], is now carried out by private actors, with a frequency that no judicial authority could (or should be required to) sustain. To be sure, the platforms' decisions do not limit the users' ability to seek redress in court: content moderation, after all, is not a form of arbitration. Nevertheless, since platforms control the infrastructure enabling the self-enforcement[2] of their own decisions, content moderation procedures end up being the main avenue through which a wide range of parties seek redress. The outcome of those procedures will often not be reviewed by any State court.

Over the years, some platforms have expressly acknowledged the para-judicial nature of content moderation decision-making: the most prominent example is the one of Meta, which set up the Oversight Board[3] precisely for the purpose of developing a body of precedent and guidance (not unlike a sovereign willingly subjecting itself to judicial scrutiny)[4]. So far, however, the choice whether to embrace the adjudicative

nature of content moderation has been largely left to the platforms themselves. As a result, even though content moderation has progressively mutated into a form of private adjudication, access to these *de facto* private adjudication fora has been scattershot at best, with platforms prioritising certain categories of complaints over others (e.g. disregarding certain unfair commercial practices), and providing insufficient transparency over their decision-making procedures and substantive standards[5].

Observing the DSA through the lens of access to justice

This state of affairs is partially about to change with the Digital Services Act (DSA). The DSA has been described as marking a "procedural turn"[6] in European lawmaking: rather than setting forth any bright-line substantive rule on the limits of online freedom of expression, the new Regulation creates a series of procedural obligations and redress avenues. The DSA's "procedure before substance" approach is reminiscent of international investment law, where dispute resolution procedures were devised at a time when no consensus existed as to the substantive standards of investor protection.[7] Hence, it makes sense to observe this new instrument through the lens of access to justice,[8] to evaluate whether the DSA effectively enhances the possibility for aggrieved parties to obtain redress within platforms, as well as outside of them. But the thorny issue of access to justice is not only interesting for those affected by harmful content. Already in 1986, Mirjan Damaška[9] urged

us to study systems of justice as a way to understand how a State conceives of its own authority and officialdom. Today, conducting a similar exercise on content moderation and the DSA can show us how the EU lawmakers conceive of the public/private divide in the European digital space: as usual with procedural law, the big question is "who gets to do what?". The remainder of this contribution will briefly reflect on whether the "procedure before substance" approach of the DSA can indeed contribute to enhancing access to justice in the field of content moderation. What role do the different dispute resolution avenues of the DSA play? How do they interact with each other, and with the pre-existing framework of European civil procedure? To what extent can the EU lawmakers solve some of the many content moderation problems, by setting forth procedures (rather than substantive rules)? These question would deserve a much longer discussion than a blog post allows. This contribution, thus, is a mere first attempt to "scratch the surface" of DSA procedures, shortly considering selected provisions of this new Regulation.

Access to justice within platforms

Article 16 of the DSA requires hosting service providers (including platforms) to put in place a notice-and-action mechanism enabling "any individual and entity" to point out the presence of allegedly illegal content. Practice,[10] however, shows that certain categories of harmful content may be not outright illegal, but nevertheless incompatible with a platform's terms

and conditions. For these types of harmful content, the availability of a notice mechanism depends on the platforms, which remain free to determine the purview of user affordances.

From an access to justice perspective, importantly, notices prevent platforms from claiming ignorance about the presence of illegal content (as long as the notice enables a diligent service provider to identify the illegality without a detailed legal examination). This, in turn, excludes the platform's immunity from liability, thus opening the door for possible liability claims by affected parties, if the illegal content is not removed expeditiously (Article 6).

Furthermore, Article 44 of the DSA promotes the standardisation of the electronic submission of Article 16 notices. Such a standardisation could have an important impact on the practical usefulness of notice-and-action mechanisms as a tool for access to justice. More specifically, standardisation of notice affordances may help avoid dark patterns, and ensure that affected parties have equal access to the mechanism, irrespective of the type of illegality they are reporting. This may help overcome the current status quo, in which platforms facilitate the reporting of certain categories of illegal content, while failing to do the same for others (e.g. "advertorials" and other unfair commercial practices).[11]

Under Article 17, if platforms take content moderation measures (including not only take-downs or account terminations, but also, for example, deprioritisations or demonetisations),[12] they are obliged to provide a statement of reasons to the affected users. Interestingly, the DSA does not require such a

statement in cases where a platform *refuses* to take moderation measures, following a notice. Despite the somewhat one-sided scope of application of the provision, Article 17 enhances transparency in some meaningful ways, obliging platforms to disclose for example the nature and scope of the measure (thus minimising the grey area of "shadow bans"), as well as the legal or contractual ground relied upon. From this last point of view, the DSA draws a sharp distinction between moderation of illegal content, and moderation on the basis of the platform's own contractual terms and conditions. Interestingly, this dichotomy is not entirely consistent with the approach taken by the Oversight Board, which frequently interprets Meta's community standards in light of international human rights law,[13] rather than simply on the basis of the applicable contract law. In sum, despite some important limitations, the statement of reasons under Article 17 should provide insights into what the decision amounts to, and why it was taken. This information, in turn, can inform the future dispute resolution strategy of the affected parties.

Article 20 of the DSA requires platforms to put in place an internal complaint-handling system, partially modeled after[14] the Platform-to-Business Regulation.[15] This system is accessible both in cases where the platform has taken a moderation measure, and in situations where it has declined to do so; thus, both users posting content and parties submitting a notice can access the complaint-handling system. Article 20 sets forth some basic (and rather vague) guarantees. The system must be available electronically and free of charge for at least six

months after the platform's decision. While the provision requires the system to be "easy to access" and "user-friendly", no real procedural standardization is required here: the platforms remain largely free to decide how to organize their complaint-handling system, and the requirements of Article 20 can potentially be met by a wide range of different mechanisms, spanning from "appropriately qualified" human moderators to a highly judicialised body such as the Oversight Board. In any event, the platforms are obliged to reverse their original decision when sufficient grounds exist, and they are prevented from handling complaints solely through automated means. In practice, the lack of detail in Article 20 may prove detrimental to the possibility for internal complaint-handling mechanisms to ensure effective access to justice: the experience of international arbitration, for instance, demonstrates that the success of an alternative dispute resolution mechanism hinges (among other factors) on the availability of a predictable procedure, which remains comparable across different service providers.[16]

Access to justice outside of platforms

As already noted, the unprecedented volume of content-related disputes cannot be effectively dealt with by state courts. In order to guarantee access to justice, thus, it is necessary to provide any affected party with cost-effective and reasonably fast alternatives, as the experience of high-volume online dispute resolution has been showing for over two decades now.[17] To this end, Article 21 of the DSA foresees the possibility to access out-of-court dispute settlement mechanisms,

where the content moderation decisions made by platforms can be reviewed. In a similar vein, the European lawmakers have already attempted to meet the dispute resolution needs of consumers, by encouraging alternative dispute resolution with the Alternative Dispute Resolution Directive[18] and the Online Dispute Resolution Regulation.[19] Article 21 of the DSA, in particular, enables the Digital Services Coordinators of each Member State to certify dispute settlement bodies established on their territory (according to a procedure which only partially resembles Article 20 of the ADR Directive). Once certified, these bodies can offer dispute settlement services to all parties seeking redress against a platform decision: not only users at the receiving end of a content moderation measure, but also parties that have filed an unsuccessful notice under Article 16, and users that were unable to obtain redress through a platform's internal complaint handling mechanisms. In other words, the DSA aims to enlarge the market for dispute resolution, with the complainant being able to choose among different (private, and sometimes public) certified dispute resolution bodies.

The experience of the European ODR Portal[20] demonstrates that alternative dispute resolution risks becoming a paper tiger,[21] if the traders (or, in the case of content moderation, the platforms) have no incentive to participate in the dispute resolution procedure and comply with its outcome. From this point of view, the original DSA proposal was bold: platforms would be bound by the decisions taken by the certified bodies.[22] The final text is, from this point of view, much less demanding: platforms must inform the users about the possibility to ap-

peal to a dispute settlement body and must generally engage in good faith in the procedure, but have no obligation to comply with the outcome (Article 21[23]). This, however, does not automatically make out-of-court dispute settlement ineffective. The cost structure of these procedures remains extremely attractive for users when compared with court litigation, and platforms have a transparency obligation (under Article 24) to disclose "the share of disputes where the provider of the online platform implemented the decision of the body". Furthermore, compliance with the outcome of these out-of-court procedures may become part of the risk mitigation measures of very large online platforms (VLOPs) under Article 35. In sum, even if out-of-court dispute settlement has been significantly watered down (compared to the original proposal of the Commission), the overall framework of the DSA does recognise a meaningful role for these procedures, and VLOPs will not be able to systematically ignore the existence and outcomes of out-of-court dispute settlement. In practice, the impact on the protection of marginalised groups will also depend on what type of bodies will obtain certification, and what the purview of their expertise will be. At the very least, the information obligations of Article 21[24] will provide some transparency in this respect.

Finally, in addition to the possibility to lodge a complaint with the competent Digital Services Coordinator (Article 53), court litigation is never precluded under the DSA: the dispute resolution options described so far never impair the possibility for affected parties to initiate court litigation, seeking e.g. the removal or reinstatement of online content. Furthermore,

the right of the service providers to compensation for infringements of the DSA is expressly enshrined in Article 54. Nevertheless, court litigation will often remain inaccessible in practice for many affected parties, and the costs and duration of proceedings will vary dramatically across the Area of Freedom, Security and Justice (AFSJ).[25] These factual obstacles often preclude effective access to justice, especially for marginalised groups and impecunious litigants. In addition, the current European framework for content moderation-related litigation is fraught with doubt, concerning *inter alia* jurisdiction. Despite the fact that litigation involving very large platforms will often be cross-border in nature, the DSA does not enshrine any special jurisdictional rule, so that claimants will need to resort to the Brussels I *bis* Regulation[26] to establish jurisdiction before an EU Member State court. This, in practice, may turn out to be challenging: some claimants, for instance, may fail to qualify as consumers,[27] and thus be unable to establish jurisdiction in their home court. Furthermore, the application of the traditional tortious grounds of jurisdiction to Internet-based harms leads to a potential splintering of jurisdiction all over the AFSJ,[28] thus hampering legal certainty.

A final layer of doubts concerns the possible role of collective redress: could class actions become a tool for the protection of marginalised or vulnerable groups, affected by harmful online content? From this point of view, the DSA introduces some important innovations. First of all, Article 90 amends Annex I to the Collective Redress Directive,[29] thus enhancing the possibility (already existing in some Member States)[30] of class actions

for content moderation disputes. Furthermore, Article 86 expressly enables recipients of intermediary services to mandate a representative body to exercise their rights on their behalf.

Conclusion

When observed in detail, the "procedure before substance" approach of the DSA leaves many questions unanswered. The final text of the Regulation contains compromises (e.g. concerning out-of-court dispute settlement), and blind spots (e.g. the absence of jurisdictional grounds for moderation-related litigation). However, the DSA also brings about important procedural improvements, concerning e.g. notice-and-action mechanisms and statements of reasons. Looking at the allocation of powers across these different dispute-management and dispute-resolution avenues, there seems to be a growing expectation that platforms (especially very large ones) will contribute to law enforcement in Europe, and will apply legal standards when engaging in decision-making (concerning e.g., whether content is illegal, or incompatible with the platform's own general terms and conditions). However, many questions remain open. As far as access to justice is concerned, one of the most urgent ones is how EU Member State courts can deal with the growing challenges of the European digital space, while relying on a jurisdictional framework that dates back, in its overall architecture, to the 1968 Brussels Convention.[31] Furthermore, to what extent can the procedural innovations of the DSA address the challenges of content moderation, in the

absence of any major harmonisation of the substantive law applicable in this very broad and porous area? In the 1989 drama *Field of Dreams*, a mysterious voice whispers to Kevin Costner, "If you build it, they will come". The DSA has built (or, at least, enhanced) a procedural framework for content moderation disputes. Will legal certainty and access to justice follow? Only time will tell.

References

1. Kai Möller, "Balancing and the structure of constitutional rights" (2007) 5(3) International Journal of Constitutional Law 754.
2. Pietro Ortolani, "The Three Challenges of Stateless Justice" (2016) 7(3) Journal of International Dispute Settlement 596.
3. Oversight Board < https://www.oversightboard.com/ > accessed 20 October 2022
4. Lorenzo Gradoni, "Chasing Global Legal Particles: Some Guesswork about the Nature of Meta's Oversight Board" (*EJIL: Talk!*, 30 December 2021) <https://www.ejiltalk.org/chasing-global-legal-particles-some-guesswork-about-the-nature-of-metas-oversight-board/> accessed 20 October 2022.
5. Catalina Goanta and Pietro Ortolani, "Unpacking Content Moderation: The Rise of Social Media Platforms as Online Civil Courts" in Xandra Kramer, Jos Hoevenaars, Betül Kas and Erlis Thermeli (eds), *Frontiers in Civil Justice: Privatisation, Monetisation and Digitisation* (Elgar 2022) 192.
6. Christoph Busch and Vanessa Mak, "Putting the Digital Services Act into Context: Bridging the Gap between EU Consumer Law and Platform Regulation" (2021) 10 Journal of European Consumer and Market Law 109.
7. Taylor St John, *The Rise of Investor-State Arbitration: Politics, Law, and Unintended Consequences* (Oxford University Press 2018).
8. Bryant Garth and Mauro Cappelletti, "Access to Justice: The Newest Wave in the Worldwide Movement to Make Rights Effective" (1978) 27 Buffalo Law Review 181.
9. Mirjan Damaška, *The Faces of Justice and State Authority: A Comparative Approach to the Legal Process* (Yale University Press 1986).
10. Oversight Board, "Case 2021-002-FB-UA (Depiction of Zwarte Piet)" (*Oversight Board* 2021) < https://www.oversightboard.com/decision/FB-S6NRTDAJ > accessed 20 October 2022.
11. Goanta and Ortolani (n 5) 193.
12. Sofia Ranchordas, Giovanni De Gregorio and Catalina Goanta, "Big Tech War Activism" (*Verfassungsblog*, 10 March 2022) < https://verfassungsblog.de/big-tech-war-activism/ > accessed 20 October 2022.
13. Lorenzo Gradoni, "Constitutional Review via Facebook's Oversight Board: How platform governance had its Marbury v Madison" (*Verfassungsblog*, 10

February 2021) < https://verfassungsblog.de/fob-marbury-v-madison/ > accessed 20 October 2022.

14. Christoph Busch, "The P2B Regulation (EU) 2019/1150: Towards a 'Procedural Turn' in EU Platform Regulation?" (2020) 9 Journal of European Consumer and Market Law 133.
15. Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.
16. Alec Stone Sweet and Florian Grisel, *The Evolution of International Arbitration: Judicialization, Governance, Legitimacy* (Oxford University Press 2017).
17. Thomas Schultz, "Online dispute resolution (ODR) : résolution des litiges et *Ius Numericum*" (2002) 48 Revue Interdisciplinaire d'Études Juridiques 153.
18. Directive 2013/11/EU of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes.
19. Regulation (EU) No 524/2013 of the European Parliament and of the Council of 21 May 2013 on online dispute resolution for consumer disputes.
20. European Commission, "Online Dispute Resolution: Reports and Statistics" <https://ec.europa.eu/consumers/odr/main/?event=main.statistics.show> accessed 20 October 2022.
21. Marte Knigge and Charlotte Pavillon, "The legality requirement of the ADR Directive: just another paper tiger?" (2016) 4 Journal of European Consumer and Market Law 155.
22. 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.
23. Pietro Ortolani, "The Three Challenges of Stateless Justice" (2016) 7(3) Journal of International Dispute Settlement 596.
24. Lorenzo Gradoni, "Chasing Global Legal Particles: Some Guesswork about the Nature of Meta's Oversight Board" (*EJIL: Talk!*, 30 December 2021) < https://www.ejiltalk.org/chasing-global-legal-particles-some-guesswork-about-the-nature-of-metas-oversight-board/ > accessed 20 October 2022.
25. European Commission, "EU Justice Scoreboard" < https://ec.europa.eu/info/policies/justice-and-fundamental-rights/upholding-rule-law/eu-justice-scoreboard_en > 20 October 2022.

26. Regulation (EU) No 1215/2012 of the European Parliament and of the Council of 12 December 2012 on jurisdiction and the recognition and enforcement of judgments in civil and commercial matters (recast).
27. Case C-498/16, *Schrems II*, 25 January 2018, ECLI:EU:C:2018:37.
28. Joined Cases C-509/09 and C-161/10, *eDate*, 25 October 2011, ECLI:EU:C:2011:685.
29. Directive (EU) 2020/1828 of the European Parliament and of the Council of 25 November 2020 on representative actions for the protection of the collective interests of consumers.
30. Amsterdam District Court, JBP 2022/40, ECLI:NL:RBAMS:2022:557.
31. 1968 Brussels Convention on jurisdiction and the enforcement of judgments in civil and commercial matters, OJ L 299, 31.12.1972, p. 32 – 42.

Aleksandra Kuczerawy

Remedying Overremoval

The Digital Services Act (DSA) is a bold attempt of the EU to create a safer digital space. It provides a whole set of notice and action mechanisms to address online harms. The codified mechanisms, together with detailed procedures, are foreseen for content that is illegal but also for content incompatible with platforms' terms and conditions. But the DSA has also another goal, to ensure that the new rules respect fundamental human rights. Mindful of the effects that the notice and action mechanisms could have on the right to freedom of expression and access to information, the DSA includes remedies for situations when action leads to overreaction. Such overreactions may affect anyone whose content is considered shocking, controversial or otherwise "undesirable", but not illegal. Often, content restrictions affect members of marginalized communities leaving them with no meaningful recourse (see here[1], here[2] and here[3]). Does the DSA include sufficient mechanisms to prevent that and to ensure access to justice?

The underlying rationale of the DSA is that everyone whose rights have been violated should have access to justice[4] to remedy the situation. The idea that any violation of rights requires correction is reflected in Article 17 of the DSA, which provides that any restriction on content by a hosting service provider should be followed by a statement of reasons to the affected recipients of the service. The statement of reasons should also include information about available redress mechanisms, such as internal complaint-handling mechanisms (Article 20), out-of-court dispute settlement (Article 21) and judicial redress. The DSA, therefore, offers three different redress routes that

can be used in sequence or separately. Judicial redress does not have its own provision in the DSA, as it remains subject to national legislation and procedures. The DSA recalls, however, on several occasions, that this redress route must be available.

The following paragraphs explain the core elements of access to justice: the right to a fair trial and to an effective remedy, as interpreted by the European Court of Human Rights (ECtHR) and the Court of Justice of the European Union (CJEU). The next part summarises the most relevant elements of the DSA provisions on internal complaint-handling systems and out-of-court dispute settlements and provides critical assessment of the provisions. The analysis indicates that while definitely a good step towards more effective protection of users' rights, the true effect of the provided remedies will depend on their practical implementation. It is further argued that some elements of the new regime may be a bold experiment the result of which is not fully predictable.

Access to justice and the DSA

Access to justice is not a right on its own. It is a notion that encompasses a number of core human rights[5], such as the right to a fair trial (Art. 6 European Convention on Human Rights, ECHR; and Art. 47 Charter of Fundamental Rights of the EU, CFREU), and the right to an effective remedy (Article 13 ECHR and Article 47 CFREU). These are primarily procedural rights requiring states to organise domestic procedures to ensure better protection of rights. In a way, they serve as tools that help

to give maximum effect to substantive rights, for example, the right to freedom of expression, the right to privacy and reputation, freedom of assembly or freedom of thought.

The right to fair trial is composed of multiple elements[6], including procedural fairness. Procedural fairness refers to the way in which the case is handled rather than its outcome.[7] Ensuring that the process of resolving conflicts is handled in a fair manner improves the perception of its legitimacy. The DSA attempts to achieve that by increasing transparency and foreseeability of the process in its detailed provisions on notice and action (e. g. Articles 16-23).

The right to effective remedy embodies the principle *ubi ius ibi remedium*, meaning that where there is a right conferred on individuals, there must be an accompanying remedy to ensure its enforcement. The purpose of the right, therefore, is to allow a victim of a violation appropriate relief.[8] Appropriate relief involves a measure that can stop the violation, or that allows the victim to obtain adequate redress, including compensation.[9] The available remedy should be effective in practice and in law.[10] The "effectiveness" of a "remedy" does not depend on the certainty of a favourable outcome for the applicant.[11] Effectiveness also does not mean that a single remedy should entirely satisfy the requirement. Rather, a system of effective remedies may result from the combination of different mechanisms that are available for those affected.

The DSA refers to the right to an effective remedy and to a fair trial in multiple instances. In particular, in Article 17, as well as in Recitals 39, 52, 55 and 59. The statement of rea-

sons, described in Article 17, should inform about the available redress mechanisms in a way that is clear, comprehensible, precise and specific to allow recipients their effective exercise. Recital 39 highlights that Member States, when applying the DSA, should respect the fundamental right to an effective remedy and to a fair trial, as provided in Article 47 of the CFREU. The DSA, furthermore, should not prevent the national judicial or administrative authorities from issuing orders reinstating content that was in compliance with terms and conditions but has been erroneously considered illegal and has been removed. Further, Recital 59 adds that the possibilities to contest decisions of online platforms should not affect the possibility to seek judicial redress.

The DSA requires the EU Member States to ensure that redress mechanisms are in place. But it also addresses the platforms falling within the scope of the DSA, by enumerating what is expected from them, i.e., creating the prescribed internal systems and participating in out-of-court dispute settlements. It should be highlighted that even though the DSA certainly took cues from the two human rights instruments (ECHR and CFREU) and the accompanying case law, their application is not strict. Full compliance with the provisions of the human rights instruments that are originally addressed to States – giving instructions on how to organize their judicial systems[12] – cannot be achieved in the private enforcement context.

Internal complaint-handling systems

According to Article 20, providers of online platforms should create an internal complaint-handling system and make it available for at least six months from the time a measure against a piece of content was taken. The system should allow the contesting of platforms' decisions that led to content removal, restriction on visibility, suspension or termination of a service or an account, as well as decisions restricting the ability to monetize content. Complaints can refer to an action taken as result of a submitted notice or as a result of the platforms' own initiative. Further, the complaint system should allow the contestation of decisions both based on the illegality of content or its incompatibility with the provider's terms and conditions. Article 20 highlights that the complaint system should be available for the affected users but also to third parties who are not users but may want to submit a notice (e. g. regarding the post of a user). It should, furthermore, equally apply to decisions honouring or rejecting the submitted notice (e. g., removing or blocking content, or leaving it online). The crucial element of Article 20 is that platforms should reverse their previous content moderation decisions (e. g., either honouring the notice or disregarding it) if the complaint contains sufficient grounds to justify such reversal.

Art. 20 DSA brings some balance to the notice and action mechanism, by specifically mandating platforms to reinstate content that, upon review, turns out not to be illegal nor incompatible with terms and conditions. But Art. 20 also allows

the appealing of decisions where the content was left intact, disregarding a notice.

In the context of online expression, the right to an effective remedy comes into play on two separate occasions. First, when a victim of infringing expression attempts to stop it, for example by requesting removal. Second, in case of successful removal, when the author tries to contest the removal and asks for the expression to be reinstated. It can be used, therefore, by both sides of a conflict to remedy possible infringements of their rights. Including both scenarios is an improvement, since the initial DSA proposal[13] did not foresee an appeal mechanism for disregarded notices. The complaint-handling system should be easy to access and user-friendly, and it should enable and facilitate the submission of complaints that are sufficiently precise and adequately substantiated (Article 20(3)).

Platforms should handle complaints in a timely, non-discriminatory, diligent and non-arbitrary manner (Article 20(4)). The same requirements appear earlier in Article 16 on the handling of complaint notices. There is no further indication of what non-discriminatory and non-arbitrary mean exactly in this context, although Recital 58 adds that the system should lead to fair outcomes. It will be interesting to see if the two requirements will bring an end to platforms' special rules[14] providing more leeway for high-profile[15] accounts. Such whitelisting practices have been revealed to give more protection to speech by those with large numbers of followers (politicians, journalists, celebrities and athletes).

Complaints should not be resolved solely on the basis of au-

tomated means and decisions should be taken under the supervision of appropriately qualified staff (Article 20(6)). After resolving the complaint, platforms should inform the parties about their reasoned decision, without undue delay. They should also include information about the possibility of out-of-court dispute settlement provided for in Art. 21 and other available possibilities for redress (Article 20(5)).

Operating a sophisticated internal complaint system per Article 20 will inevitably be costly. It might be challenging for smaller platforms, especially if users start to appeal *en masse*. While providing for an appeal mechanism is arguably positive from the perspective of the right to an effective remedy, handling a large number of appeals will not be easy. It will also most certainly lead to more content being reinstated, either because of successful appeals, decisions of the settlement bodies under Article 21 or court orders.

Does that mean that the DSA is effectively pushing for a right to forum, forcing platforms to host all content that is not illegal? This conclusion would be too far-reaching. This is also not the intention of the DSA. Platforms can still decide in their terms and conditions what content they do not welcome, subject to qualifications under Article 14 (due regard given to freedom of expression, freedom and pluralism of the media, and other fundamental rights and freedoms). They will most likely become more restrictive and more precise in listing all unwanted content, also as a result of the transparency requirement of Article 14. That would also help them stay in line with recent decisions, such as in Germany[16], where courts started

ordering reinstatement of content that was violating vaguely formulated terms and conditions but was not illegal. More clarity and transparency regarding the internal rules of platforms is certainly a good thing.

Out-of-court dispute settlement

Article 21 describes the functioning of out-of-court dispute settlement mechanisms to contest platforms' content moderation decisions. Platform users, but also those who have previously submitted a complaint (as in Article 20), should be able to select any certified out-of-court dispute settlement body. This route of redress can be used as a follow-up, a form of second instance to complaints that have not reached a satisfactory outcome through the internal complaint-handling system. It could also be a self-standing mechanism for complaints that have not been subject to review through the internal system. Article 21 clarifies that the possibility to refer the complaint to a settlement body does not impact the users' right to initiate proceedings before a court, at any stage (see also Recital 59). Both parties to the dispute should engage in good faith with the selected body in an attempt to find a solution. Service providers, however, may refuse to engage if a dispute has already been resolved on the basis of the same information and the same grounds of alleged illegality or incompatibility of content (Recital 59, Article 21(2)).

It is crucial to note that the dispute settlement bodies do not have the power to impose a binding settlement of the dispute

on the parties (Article 21(2)). This is another crucial twist as the initial EC proposal[17] mandated the decisions to be binding (in Article 18[18]). The change of positions reflects the arguments that binding decisions would create extra-judicial bodies,[19] would lead to must-carry orders and would prevent platforms[20] from obtaining redress. The approach is also in line with the Directive 2013/11[21] on alternative dispute resolution. It leads to the question, however, of what will happen if a platform engages but then simply ignores any unfavourable decisions. The user could of course still seek recourse in court, but will they? Would such an approach be considered a failure to comply with the obligations of the DSA, and trigger consequences foreseen in Articles 51 and 52? Users of the platforms (and organisations representing them) could also file a complaint to the Coordinators on the infringement on the DSA (Article 53). Strictly speaking, there is no obligation to comply with decisions that are not binding. Such a continuous and systemic disregard, however, would definitely attract interest of the Digital Service Coordinators as well as the Commission (especially in the case of VLOPs).

Article 21 provides further details in nine paragraphs. The provisions specify that the rules of the procedure should be clear, fair and easily accessible (Article 21(3)). They specify time limits to reach a decision (90 days with a possible extension of another 90 days for complex disputes) (Article 21(4)). They also describe the payment system, which differs depending on whose claim succeeds (Article 21(5)). For the users of the service the dispute settlement should be available free of

charge or at a nominal fee, putting the main financial burden on the platforms. But if the costs are almost exclusively borne by platforms, and it is the users who initiate and select a settlement body, will these bodies be inclined to rule more in favour of the users? Will it lead to high numbers of put-back decisions, especially for content that is "awful but lawful"? Again, platforms could become overly restrictive to avoid awful but also "undesirable" content to prevent such an effect.

Finally, certified bodies should report annually to the Digital Services Coordinator, specifying the number of disputes they received, information about the outcomes, the average time taken to resolve them, and any shortcomings or difficulties encountered (Article 21(4)). The Digital Services Coordinators should further compose reports on the functioning of the out-of-court dispute settlement bodies, identifying best practices and recommendations on how to improve their functioning. Both reports will surely be helpful to tweak the process along the way.

All things considered, it is uncertain what the impact of the out-of-court dispute settlement mechanism of Article 21 will be. A specific regulated system in this form is rather novel in the area of content moderation. Due to the difference in scale, it cannot really be compared to the functioning of other mechanisms, e. g., the Facebook Oversight Board. At the moment, Article 21 seems more of an experiment that leaves many open questions. The main one is whether the first stage of this experiment should not be limited to VLOPs only as they have the appropriate resources to handle the process in a non-disruptive

manner (see, e. g., Daphne Keller's intervention[22] in the EP during the legislative process). After the initial findings on the functioning on the dispute settlement systems, and potential corrections of the issues identified in first reports, the scope could be broadened to other platforms.

Conclusion

The DSA takes a multi-step approach, offering not one remedy but three different options that can be used in sequence or separately. The triple-layered system in the DSA is certainly a positive development in comparison to the E-Commerce Directive, which did not contain any remedies[23] to address unwarranted content restrictions. It is laudable that the involvement of courts is emphasized (e. g., in Recital 59) in a way that is rather unique for EU instruments. After all, independent courts of law remain the most apt institutions to adjudicate on conflicts between different (fundamental) rights.

Articles 20 and 21 of the DSA and multiple mentions of the need to inform users about the available redress mechanisms throughout the Regulation certainly contribute to strengthening the right to an effective remedy and to a fair trial for those affected by the platform's actions. They provide an additional safeguard to strengthen the respect for fundamental rights in the DSA, and for that, they should be considered a big step forward. The question remains, of course, how the provisions will play out in practice. They could (and hopefully will) lead to a more effective exercise of the right to freedom of expression

online. Or maybe, a more pragmatic approach will win. And after the initial storm of appeals, platforms will become more restrictive in their terms and conditions, to protect their prerogative to choose the speech they want to host.

This chapter benefited from funding from FWO grant nr. 1214321N and a stipend from the Cyber Policy Center at Stanford University.

References

1. Carolina Are, "How Instagram's algorithm is censoring women and vulnerable users but helping online abusers" (2020) 20(5) Feminist Media Studies 741.
2. Transthetics, "YouTube's moderation process is failing the LGBT community. Can we fix this?" (*Transthetics*, 27 October 2018) <https://transthetics.com/youtubes-moderation-process-is-failing-the-lgbt-community>.
3. Joslin Trinady, "Black creators protest TikTok's algorithm with #ImBlackMovement" (*DailyDot*, 21 May 2020) <https://www.dailydot.com/irl/tiktok-protest-imblackmovement/>.
4. European Union Agency for Fundamental Rights, "Access to Justice in Europe" (*European Union Agency for Fundamental Rights*, 10 August 2012) https://fra.europa.eu/sites/default/files/fra_uploads/1506-FRA-Factsheet_AccesstoJusticeEN.pdf.
5. European Union Agency for Fundamental Rights and Council of Europe, *Handbook on European law relating to access to justice* (Publications Office of the European Union 2016) < https://www.echr.coe.int/documents/handbook_access_justice_eng.pdf>.
6. European Court of Human Rights, "Guide on Article 6 of the European Convention on Human Rights" (Council of Europe/European Court of Human Rights 2022) <https://www.echr.coe.int/documents/guide_art_6_eng.pdf>.
7. Steel and Morris v. the United Kingdom (ECtHR, 15 February 2005) para. 95.
8. Vilho Eskelinen and Others v. Finland (ECtHR, 19 April 2007) para. 80.
9. Kaya v. Turkey (ECtHR, 19 February 1998) para. 106.
10. Kudla v. Poland (ECtHR, 26 October 2000) para. 157.
11. M.S.S. v. Belgium and Greece (ECtHR, 21 January 2011) para. 289; ECtHR, Gebremedhin [Gaberamadhien] v. France, 26 April 2007, para. 53.
12. Case C-583/11 P *Inuit Tapiriit Kanatami and Others v Parliament and Council* [2013] para 100. See also Case C-50/00 P *Unión de Pequeños Agricultores v Council* [2002] para 41 and Case C-263/02 P *Commission v Jégo-Quéré* para 31.
13. 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 [2020] COM(2020) 825 final <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52020PC0825>.

14. Jeff Horwitz, "Facebook Says Its Rules Apply to All. Company Documents Reveal a Secret Elite That's Exempt" *The Wall Street Journal* (New York City, 13 September 2021) <https://www.wsj.com/articles/facebook-files-xcheck-zuckerberg-elite-rules-11631541353>.
15. Ibid.
16. Matthias C. Kettemann and Torben Klausa, "Regulating Online Speech: Ze German Way" (*Lawfare*, 20 September 2021) <https://www.lawfareblog.com/regulating-online-speech-ze-german-way>.
17. Proposal for a regulation of the European Parliament and of the Council on a Single Market For Digital Services (Digital Services Act) (n13).
18. Carolina Are, "How Instagram's algorithm is censoring women and vulnerable users but helping online abusers" (2020) 20(5) Feminist Media Studies.
19. Asha Allen and Ophelie Stockhem, "A Series on the EU Digital Services Act: Tackling Illegal Content Online" (*Center for Democracy and Technology*, 2 August 2022) <https://cdt.org/insights/a-series-on-the-eu-digital-services-act-tackling-illegal-content-online/>.
20. Jörg Wimmers, "The Out-of-court dispute settlement mechanism in the Digital Services Act – A disservice to its own goals", (2021) 12 JIPITEC 421 para 1 <https://www.jipitec.eu/online-first-articles-1/5357>.
21. Directive 2013/11/EC of the European Parliament and of the Council of 21 May 2013 on alternative dispute resolution for consumer disputes and amending Regulation (EC) No 2006/2004 and Directive 2009/22/EC (Directive on consumer ADR), OJ L 165/63 <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:165:0063:0079:EN:PDF>.
22. Daphne Keller, "US Developments and the DSA" (*POLICY DEPARTMENT FOR ECONOMIC, SCIENTIFIC AND QUALITY OF LIFE POLICIES*) <https://www.europarl.europa.eu/cmsdata/234757/3.%20DSA%20DK%20-%20presentation%203%20final.pdf>.
23. Aleksandra Kuczerawy, "Intermediary Liability & Freedom of Expression: Recent Developments in the EU Notice & Action Initiative" (2015) 31(1) Computer Law and Security Review 46.

Tomiwa Ilori

Contextualisation over Replication

The Possible Impacts of the DSA on Content Regulation in African Countries

Today, at the centre of the debate on online content regulation are questions on how online platforms and governments wield disproportionate powers. It is therefore unsurprising that both online platforms and governments have attempted[1] to consolidate these powers. However, while their attempts have been questionable and sometimes useful, there seems to be a global consensus that online harms, which are legitimate bases[2] for content regulation, threaten human rights and democracies. This consensus is gradually gaining momentum and so are regulatory solutions towards combating these harms. An example of such a solution[3] is the European Union's (EU) Digital Services Act (DSA).

The EU is notorious[4] for using regulatory solutions like the DSA to dominate and pre-empt global digital standards. Often, the major conversations on the international impacts of EU laws have oscillated[5] between capture and actually providing normative leadership on thorny aspects of digital regulation. Even though evidence of such capture is yet to be seen with the DSA, the DSA has shown some regulatory clarity[6] towards regulating online harms, which should be treated with cautious optimism[7]. This contribution discusses this cautious optimism especially as it concerns the DSA's potential impacts in African contexts if African countries choose to take inspiration from it. This contribution concludes that African countries should develop their own content regulation rules by paying more attention to their contexts and consider aspects of the DSA only where they will improve such local rules.

The "Brussels Effect" in African countries: Like the GDPR, like the DSA?

Modernising the primary law on intermediary regulation in the EU, the E-Commerce-Directive 2000/31/EC[8], the DSA is currently the most elaborate and comprehensive body of regional rules on content regulation. The DSA aims to ensure "a safe, predictable and *trustworthy* online environment" (Article 1(1) DSA, emphasis added), and balance the regulation of illegal content with the protection of fundamental rights.

Like the General Data Protection Regulation (GDPR), even though the DSA directly applies to all 27 EU member states (Article 2(1) DSA), the "Brussels Effect"[9], which is the impact of EU laws in non-EU contexts, may cause some (un)intended effects such as de facto and de jure effects[10].

Using the GDPR as an example, the EU was able to set some data protection standards[11] globally. Companies operating in the EU had to conform to the GDPR. As a result, a company's compliance measure meant for the EU could consequently become a measure applied across the globe, i.e., separate compliance measures are not developed for Europeans, rather, the measures are applied globally. This is a *de facto* impact of the GDPR. On the other hand, *de jure* effects involve the adoption of some aspects of the GDPR as data protection standards in non-EU countries, including in African countries[12]. These effects are mainly motivated by economic and trade interests[13].

Given this background, a possible international impact of the DSA is its normative clarity on how to combat online harms

while protecting fundamental rights. For example, the DSA offers inspiration for African countries on protracted regulatory issues in the area of online content moderation, through provisions on intermediary liability (Article 1(2)(a) and Chapter II), due diligence obligations for different types of services (Article 1(2)(b) and Chapter III), and a framework for oversight and enforcement (Article 1(2)(c) and Chapter IV).

The DSA provides specific responsibilities for platforms with respect to ensuring more transparency and accountability. Articles 14 - 20, 24, 26, 27, 28, 39 DSA and many others provide for various aspects of transparency obligations of online platforms. Articles 41, 49, 50, 51, 61 and 63 DSA also relate to platform obligations, accountability and oversight, provision for Digital Services Coordinators (DSCs) and their powers, and the European Board (Board) for Digital Services and their powers respectively. Under the DSA, DSCs are national supervisors of intermediary service providers and they make up the Board to jointly administer the DSA. While doing business in the EU, platforms now have to pay attention[14] to the DSA's provisions. As seen with the GDPR, in the course of complying with these provisions, platforms might internationalise the DSA. Such compliance might encourage platforms to become accountable in non-EU contexts. A *de jure* impact that could reduce platforms' disregard for non-EU contexts may be that law- and policy-makers in non-EU contexts begin to pass these principles as laws. For example, data protection regulations[15] in Egypt, Nigeria and South Africa bear similarities with the GDPR.

It is unclear whether the DSA will have the same international effect[16] as the GDPR in African countries. In fact, if we think of the GDPR beyond handing down fines to platforms and include other core aspects a data protection law needs to excel at such as putting data subjects at the centre of data control, the GDPR still has a long way to go[17].

The DSA, cautious optimism and need for contextualization in African countries

While African countries may choose to take inspiration from EU laws, there is a need to pay careful attention to local needs before blindly applying foreign rules like the DSA. Rather than replicating the DSA in the African context, African stakeholders, including governments, are encouraged to look more closely at the problems of online harms before they contextualise solutions. Even with its novel and bold moves at content regulation, the DSA has its rough edges and if transplanted without caution into African contexts, it might roll back the gains of human rights protection online in African countries.

To move towards contextualisation of online harms regulation that does not replicate errors but builds on useful aspects of existing regulation, African stakeholders will need to pay attention to a number of issues, such as old and new criminal measures on online harms, the role of African governments including Uganda[18], Democratic Republic of Congo[19] and Eritrea[20] in spreading online harms and complicating content regulation, in addition to the inherent shortcomings in the DSA itself.

Extant laws that criminalise[21] legally permissible content abound in many African countries. These laws, which have been used to regulate online communications, do not provide clear meaning of online harm and as a result, this leads to disproportionate measures that violate online rights. Many users have been harassed and arrested based on these laws. In addition, new cyber-regulatory laws[22] also provide for the offences of insults, false information, criminal defamation and libel. These political offences are often conflated with online harms and are incompatible with international human rights standards. When online harms such as hate speech or harassment are actually provided for in laws, they tend to be overbroad and vague[23] as seen in Nigeria, Kenya, Uganda, Ethiopia and other African countries.

Additionally, African governments are one of the biggest purveyors[24] of online harms in the region. Governments' active complicity makes it difficult to meaningfully regulate them – it is more or less like having cattle make the rules on hay.

Concerning the DSA's shortcomings, if it were copied into the African context, the DSA may pose at least three challenges to content regulation in the region.

One, Article 16, which provides for notice and action mechanisms. Article 16(2) DSA requires a "sufficiently substantiated explanation" for why an individual or entity alleges an item of information to be illegal. This provision is problematic for two major reasons. One, it is not clear what must be considered for such an explanation to be sufficiently substantiated. Two, this

creates more problems for human rights protection, if such sufficiently substantiated explanation is based on one or more of the various problematic laws on content regulation in African countries. This provision also adds to the challenge[25] of over-removal of content by platforms.

Second, some of the DSA's provisions, including ones that create significant new powers for the European Commission, if transplanted to an African context would create a lack of judicial oversight. For example, Article 40 DSA provides for data access and scrutiny by the DSCs and the Commission. As a result, it gives both the DSC and the Commission excessive powers[26] with respect to demanding, accessing and using such data from platforms without concomitant judicial oversight. Adopting this provision in African countries will put data protection in grave danger, as there will be no means of ensuring that such access is legal, proportionate and necessary.

Third, currently, the initial financial cost of hiring outside staff for the EU at the regional level to enforce the DSA and the Digital Markets Act (DMA) is estimated[27] at $26 million. This excludes other manifold costs required for building institutional capacities of national regulators and ensuring active monitoring and evaluation of compliance with the Act. These financial costs might dissuade African countries, hoping to model their online harms regulations according to the DSA. However, Article 43 DSA allows the Commission to charge VLOPs and VLOSEs for supervisory fees in proportion to the monthly active users in the EU and it shall not exceed 0.05% of the annual turnover of a VLOP or VLOSEs. These supervisory

fees could also be calculated and charged by African countries, as done in the DSA.

Recommendations

The adoption of the DSA in the EU has started generating necessary debates on its possible impacts[28] in non-EU contexts. While the internationalisation of the DSA might be useful, considering how it has provided regulatory clarity in some aspects, its adoption in non-EU contexts must be treated with cautious optimism and properly contextualised. One way of working towards such contextualisation for online harms regulation in Africa would be developing a regional normative document, led by the African Commission on Human and Peoples' Rights (African Commission), that elaborately articulates a rights-based approach to online harms regulation in Africa and this is possible given existing efforts in the region.

Adopted by the African Commission in 2019, the revised[29] Declaration of Principles on Freedom of Expression and Access to Information offers a starting point for African governments looking towards such contextualisation. While the Declaration can be referred to as the closest and the most elaborate regional constitution on digital rights, it provides for specific aspects of content regulation that can be further developed by African governments.

For example, Principle 22 of the Declaration provides for review of criminal measures such as offences of sedition, insults,

false information, criminal defamation and libel in line with international human rights standards. The repeal of these criminal measures addresses the problematic provisions of old extant laws highlighted above and it will go a long way in setting the tone for a foundational and ground-up development of a regional law on content regulation like the DSA in African countries.

Principle 39(4) of the Declaration also provides that governments shall not require removal of online content without considering five major safeguards. One of these safeguards as provided for under principle 39(4)(b) include ensuring that such a request must be imposed by an independent and impartial judicial authority. The only exception to such a request is that law enforcement agencies may make a request for removal to forestall imminent dangers to lives and properties which must also be subject to retroactive judicial review. This principle provides a useful backdrop for African governments to develop rules on notice and action which is one of the major shortcomings of the DSA.

In its implementation, and as a direct response to the challenge of limited ex ante judicial oversight under the DSA, the Declaration requires African governments to adopt judicial measures that give effect to its provisions. Therefore, the prior and retroactive judicial review of executive and legislative powers on regulation of online harms in African countries will be further strengthened.

Conclusion

Developing regulatory norms that seek to balance human rights protection and prevention of online harms in African countries like the DSA is difficult but not impossible. However, the major motivation for such development must involve the appreciation of the impacts of online harms on human rights and democracies, drive meaningful multi-stakeholderism to combat these harms, ensure victim-centred approaches towards regulatory policies and commit to dynamic enforcement and implementation strategies of these policies.

References

1. Robert Gorwa, "What is Platform Governance" (2019) 22 Information, Communication & Technology 4, 6 <https://gorwa.co.uk/files/platformgovernance.pdf> accessed 7 September 2022.
2. Amélie P Heldt, "EU Digital Services Act: The White Hope of Intermediary Regulation" in Terry Flew and Fiona R Martin (eds), *Digital Platform Regulation* (Springer 2022).
3. The Office of the High Commissioner for Human Rights (OHCHR), "Moderating online content: fighting harm or silencing dissent" (*OHCHR*, 23 July 2021) <https://www.ohchr.org/en/stories/2021/07/moderating-online-content-fighting-harm-or-silencing-dissent> accessed 6 September 2022.
4. Marta Granados Hernandez, "Global Gateway and the EU's Digital Ambitions" (*Centre for Strategic and International Studies*, 19 May 2022) <https://www.csis.org/blogs/development-dispatches/global-gateway-and-eus-digital-ambitions> accessed 12 September 2022.
5. Anu Bradford, "The Brussels Effect" (2012) 107 Northwestern University Law Review 35, 39 <https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1081&context=nulr> accessed 12 September 2022.
6. Chris Riley, "The EU's Digital Services Act will make big changes, although the details remain unclear" (*RSTREET*, 2 May 2022) <https://www.rstreet.org/2022/05/02/the-eus-digital-services-act-will-make-big-changes-although-the-details-remain-unclear/> accessed 8 September 2022.
7. Cory Doctorow, "Europe's Digital Service Act: On a Collision Course with Human Rights" (*Electronic Frontier Foundation*, 27 October 2021) <https://www.eff.org/deeplinks/2021/10/europes-digital-services-act-collision-course-human-rights-0> accessed 6 September 2022.
8. Directive 2000/31/EC on the certain legal aspects of the information society services [2000] OJ L178.
9. Covington, "The Brussels Effect – The EU's Digital Strategy Goes Global" (*Covington*, 27 February 2020) <https://www.cov.com/en/news-and-insights/insights/2020/02/the-brussels-effect-the-eus-digital-strategy-goes-global> accessed 9 September 2022.
10. Anu Bradford, "The European Union in a Globalised World: the Brussels Effect" (*Groupe d'études géopolitiques*, March 2021) <https://geopolitique.eu/en/articles/the-european-union-in-a-globalised-world-the-brussels-effect/> accessed 19 September 2022.

11. Mark Scott and Laurens Cerulus, "Europe's New Data Protection Rules Export Privacy Standards Worldwide" *Politico* (Arlington, 31 January 2018) <https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/> accessed 20 September 2022.
12. Dan Simmons, "17 Countries with GDPR-like Data Laws" (*Comforte AG*, 13 January 2022) <https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws> accessed 15 September 2022.
13. "Who Does the GDPR Apply To?" (*Data Privacy Manager*, 10 February 2021) <https://dataprivacymanager.net/who-does-the-eu-gdpr-apply-to/> accessed 23 November 2022.
14. Paolo Cesarini, "EU Digital Services Act: How to Approach Compliance" (*Teneo*, 11 July 2022) <https://www.teneo.com/eu-digital-services-act-how-to-approach-compliance/> accessed 15 September 2022.
15. Dan Simmons, "17 Countries with GDPR-like Data Laws" (*Comforte AG*, 13 January 2022) <https://insights.comforte.com/countries-with-gdpr-like-data-privacy-laws> accessed 15 September 2022.
16. Ibid.
17. Ilse Heine, "3 Years Later: An Analysis of GDPR Enforcement" (*Centre for Strategic and International Studies*, 13 September 2021) <https://www.csis.org/blogs/strategic-technologies-blog/3-years-later-analysis-gdpr-enforcement> accessed 16 September 2022.
18. Digital Forensic Research Lab, "Facebook Removes Inauthentic Assets Linked to Ugandan Government" (*Medium*, 10 February 2021) <https://medium.com/dfrlab/facebook-removes-inauthentic-assets-linked-to-ugandan-government-c3949be9f810> accessed 5 October 2022.
19. Digital Forensic Research Lab, "Inauthentic Facebook Pages Rebranded to Promote DRC Politician" (*Medium*, 6 August 2020) <https://medium.com/dfrlab/inauthentic-facebook-pages-rebranded-to-promote-drc-politician-cdc4785a3114> accessed 5 October 2022.
20. Digital Forensic Research Lab, "Eritrean Report Uses Fact-checking Tropes to Dismiss Evidence as 'Disinformation'" (*Medium*, 23 June 2021) <https://medium.com/dfrlab/eritrean-report-uses-fact-checking-tropes-to-dismiss-evidence-as-disinformation-385718327481> accessed 5 October 2022.
21. Tomiwa Ilori, "Stemming Digital Colonialism Through the Reform of Cybercrime Laws in Africa" (*Yale ISP*, 19 June 2020) <https://law.yale.edu/isp/initiatives/wikimedia-initiative-intermediaries-and-information/wiii-blo

g/stemming-digital-colonialism-through-reform-cybercrime-laws-africa> accessed 15 September 2022.

22. Tomiwa Ilori, "How Social Media Companies Help African Governments Abuse 'Disinformation Laws' to Target Critics" (*RestofWorld*, 4 November 2021) <https://restofworld.org/2021/social-media-africa-democracy/> accessed 6 September 2022.

23. Media Defence, "Module 7 on Cybercrimes" (*Media Defence Summary Modules on Litigating Digital Rights and Freedom of Expression Online*, December 2022) <https://www.mediadefence.org/ereader/wp-content/uploads/sites/2/2020/12/Module-7-Cybercrimes.pdf> accessed 19 October 2022.

24. Africa Centre for Strategic Studies, "Domestic Disinformation on the Rise in Africa" (*Africa Centre for Strategic Studies*, 6 October 2021) <https://africacenter.org/spotlight/domestic-disinformation-on-the-rise-in-africa/> accessed 12 September 2022.

25. Joan Barata, "The Digital Services Act and Its Impact on the Right to Freedom of Expression: Special Focus on Risk Mitigation Obligations" (*DSA Observatory*, 27 July 2021) <https://dsa-observatory.eu/2021/07/27/the-digital-services-act-and-its-impact-on-the-right-to-freedom-of-expression-special-focus-on-risk-mitigation-obligations/> accessed 16 September 2022.

26. Konstantinos Komaitis, Katitza Rodriguez and Christoph Schmon, "Enforcement Overreach Could Turn Out To Be A Real Problem in the EU's Digital Services Act" (*Electronic Frontier Foundation*, 18 February 2022) <https://www.eff.org/deeplinks/2022/02/enforcement-overreach-could-turn-out-be-real-problem-eus-digital-services-act> accessed 14 September 2022.

27. Jillian Deutsch, "Europe Passed New Tech Rules. That Was the Easy Part" *Bloomberg* (New York City, 2 August 2022) <https://www.bloomberg.com/news/newsletters/2022-08-02/europe-will-face-challenges-enforcing-new-tech-bills-dma-and-dsa> accessed 14 September 2022.

28. Papaevangelou C, "Digital Services Act, Brussels Effect and the Future of the Internet" (*JOLT*, 8 December 2020) <http://joltetn.eu/digital-services-act-brussels-effect-and-the-future-of-the-internet/> accessed 23 November 2022.

29. African Commission on Human and Peoples' Rights, "Declaration of Principles on Freedom of Expression and Access to Information in

Africa" (*African Commission on Human and Peoples' Rights*, 2019) <https://www.achpr.org/public/Document/file/English/Declaration%20of%20Principles%20on%20Freedom%20of%20Expression_ENG_2019.pdf> accessed 2 September 2022.

Nayanatara Ranganathan

Regulating Influence, Timidly

"We are proposing a new set of EU Digital Principles to shape our European society [...] and your views matter" declares an advertisement paid for by the official page of the European Commission on Facebook. This message, soliciting participation for a public consultation, was produced by the European Commission and circulated over Facebook advertising platforms, to over a million people.

Like many other institutions, the Commission uses the medium of advertising on digital platforms to reach people, garner support and generally maintain public relations. Facebook advertising platforms enable an influential body such as the Commission to stay relevant by having an active public-facing digital presence. Even as the institution spends millions of euros advertising on these platforms every year, the Commission passed a different regulation, the Digital Services Act, that attends to the question of regulating online advertising, or *influence*.

The DSA considers advertising and recommender systems as deserving of regulatory attention, and not immutable facets of an online world. But even as the regulation furthers current standards in disclosures around online advertising, it insulates advertising business models and consolidates platform efforts to sidestep the operative question that characterises online advertising: how and why advertisements reach who they reach, in less abstract terms.

Transparency and Other Obligations

Advertising business models have been at the heart of many of the persistent issues with technology practices and products. The circulation of advertisements over digital platforms is determined, secretly, by private mega-corporations incentivised by profit and growth. The inclusion of and focus on regulating online advertising and recommender systems within coherent frameworks is long overdue, and the DSA addresses these systems from a fundamental rights and collective "societal harms" perspective.

Practically, the DSA imposes transparency obligations upon "online platforms" like Facebook to declare when an advertisement is being displayed, on whose behalf the advertisement was paid for, and "meaningful information" to determine why the advertisement reaches a particular person (Article 26). Beyond this, the regulation requires "very large online platforms" (VLOPs) to make advertising transparency data available through Application Programming Interfaces (Article 39), a form that allows systematic analysis of data on a large scale.

Two large deceptions perpetrated by platforms' self-regulatory initiatives seem to have been addressed in the regulation. First, companies such as Meta and its group of advertising platforms presently offer transparency information about a small class of advertisements deemed to be "political". These advertisements make up less than 1%[1] of its total advertising revenue, by the company's own admission. This distinction of "political ads" is sustained on a forced binary

between commerce and advocacy, where only the latter is deemed political. Second, transparency information is often made available in forms such as graphical interfaces, that give the impression of informing but preclude assessment of information at scale.

Beyond transparency requirements, the DSA imposes due diligence obligations upon VLOPs to identify, analyse, assess and mitigate some categories of systemic risks: (i) illegal content, (ii) actual or forseeable negative effects on the exercise of fundamental rights as protected by the Charter, (iii) actual or foreseeable negative effects on civic discourse and electoral processes, and public security, and (iv) actual or foreseeable negative effect in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being (Articles 34 and 35). Beyond acknowledging the breadth of risks from VLOPs, these provisions buy into platforms' promise of continued refinement, effectively insulating them from any definitive consequence for proven or potential harm. Broad exemptions to disclosure of systemic risks publicly (Article 42(5)) leaves the provisions with no teeth.

The Commission will facilitate and encourage the development and application of voluntary codes of conduct for online advertising (Article 46) by online platforms and other entities. Codes of conduct carry the danger of being accessories, for platforms and regulators alike, to signal the operation of the rule of law in the online realm, but without much substance. Besides this, independent audits for compliance (Article 37) and

access to and scrutiny of data by vetted researchers (Article 40) are mandated for VLOPs. In a procedural realm, the DSA introduces mechanisms to charge VLOPs an annual supervisory fee to fund the resources required to carry out its supervisory functions (Article 43).

It is clear that the DSA is both ambitious about squaring the digital advertising ecosystem with fundamental rights, as well as cognizant of the varieties of risks posed by advertising and recommender systems. Nevertheless, its regulatory approaches follow the Big Tech transparency playbook, and go little further than where technology businesses themselves have ventured. The interventions in the regulation are constrained in their imagination by the forms and substance of platforms' self-regulatory efforts.

Predatory inclusion and discriminatory exclusion

Advertisements on online platforms are typically delivered based on a determination of "relevance" for users (among other factors). While "relevance" is an abstraction, viewership of advertisements is determined through predatory inclusion and discriminatory exclusion. At a collective level, these circulatory logics have translated to polarized publics, election-related information asymmetries, etcetera. So while companies like Facebook are considered online platforms because they perform a function of "dissemination to the public" (Article 3(k)), practically, they craft calculated *audiences*, the opposite of making information available "to a potentially unlimited number of third parties".

In the form and substance of transparency requirements, the DSA entrenches existing orientations of technology development. The two areas in which the DSA requires transparency disclosures are content moderation, and advertising/recommender systems. But the insights sought are able to address any harms only after the fact. Insofar as the DSA seeks to complement transparency measures with other obligations, such as risk assessment and mitigation methods, it is far-fetched to expect companies to be either perceptive or forthcoming about the systemic risks of their own products.

It is worth recounting that online advertisement transparency emerged as a self-regulatory response to a crisis of accountability in the operation of online platforms. The power of platforms to influence elections became a flashpoint for broader concerns about online advertising and algorithmic systems of information curation. The voluntary commitments that emerged in the aftermath were inspired by regulation for a previous media era, where only a particular class of advertisements ("political ads") were understood as worthy of scrutiny. Within this class, the substance of transparency information is focused away from platform workings.

Transparency for a different media era

As advertisement space was used for political campaigns in print, TV, radio and such older forms of media, political advertisements became a subject of regulation. The substance of political advertisement transparency in previous media eras correlated with dangers arising therein. Business models of media

companies, characteristics of different media, and more contributed to how regulations were created. For example, political parties investing in print ads in newspapers were required to disclose advertising expenditure. As advertisement revenue was the business model for many newspapers, a transparency mandate was designed to minimize risks of partisan reporting in newspapers, for continued relations with political parties. Regulations and guidelines about online advertising have tried to extend the transparency response from the past era to digital advertising without accounting for the divergences in business models, and the different kinds of publics they create and address. In the present information society, the forms in which political messages are received, the diverse motives for advertising, the computational methods of delivery, etcetera create vastly different conditions than their mass media predecessors.

Transparency of abstractions

In the past, advertisers had to specify the exact nature of the audiences they desired to reach (through interests, behavior and demographic information). Today, advertising systems on social media platforms function with no more than a clear definition of the desired results (e.g.,100 app installs, 5000 page views, 1 million impressions, etc.). Based on the outcomes sought, platforms are able to balance the demand for attention (advertisements) and the supply (users' impressions) in the most "optimal" or profitable distribution, without requiring advertisers to spell out any predatory forms of targeting.

Advertisers are able to derive audiences that are niche and hyper-local, or global and transnational, and everything in between.

Meanwhile, in their transparency initiatives, platforms have managed to abstract away the kind of determinations used in finding matches between advertisements and their viewership. Information is offered in the form of broad demographic breakdowns of audiences for every ad, avoiding the determinations made by the platform in assigning matches between ads and people entirely.

By leaving "meaningful information" (Article 26) open for interpretation and allowing platforms the power to determine the degree of abstraction by which they make their advertising operations legible to the public (breakdown by age brackets, gender, etc.), the DSA will allow companies to disclose only as much non-threatening information as their business models permit.

Contrast this with the fact that more than 2 million data points[2] are used by Facebook in the determination of why a particular ad was chosen for a particular user's attention, and the indeterminate number and type of factors which are used by machine learning algorithms that curate audiences for ads. While broad demographic information about targeted groups is still meaningful to an extent, the DSA effectively treats people like market segments from a different media era. Given the liberties of abstraction available in the DSA, the state of play will not shift towards preempting hidden infractions of rights that these technologies might embed.

Influencing regulation

In a sense, the Cambridge Analytica scandal galvanized technology businesses to make a demonstrable effort in being accountable for their services. Transparency initiatives took the form of nominal accountability for the *activities on the platform*, rather than accountability for the *workings* of the platform. As these voluntary commitments arrived on the heels of a massive shift in public opinion towards the platforms, they are equally crafted to be public relations campaigns. What has followed in the form of transparency initiatives has become the ceiling of platform accountability standards. The form and substance of transparency has skirted around any possible threats to the business models of these companies. Following the breadcrumbs laid by self-regulatory initiatives makes regulation run the risk of being a legal spectacle, where compliance becomes mere performance.

References

1. Josh Constine, "Zuckerberg defends politician ads that will be 0.5% of 2020 revenue" (*Tech Crunch,* 31 October 2019) <https://techcrunch.com/2019/10/30/zuckerberg-political-ads/> accessed 4 November 2022
2. Ian Bogost and Alexis C Madrigal, "How Facebook works for Trump" (*The Atlantic,* 17 April 2020) <https://www.theatlantic.com/technology/archive/2020/04/how-facebooks-ad-technology-helps-trump-win/606403/> accessed 4 November 2022

Nicolo Zingales

The DSA as a Paradigm Shift for Online Intermediaries' Due Diligence

Hail To Meta-Regulation

In October 2022, the final version of the Digital Services Act (DSA) was published[1] in the Official Journal. The importance of this legislation in shaping the governance of online content in the years to come cannot be overstated. While several provisions are worth highlighting, in this blog post, I focus on one specific aspect: the adoption of a meta-regulatory approach. Specifically, after providing a definition of this concept, I discuss its virtues and limits and illustrate how this approach is operationalised in the DSA with regard to a subset of online intermediaries: providers of Very Large Online Platforms (VLOPs) and Very Large Online Search Engines (VLOSEs). The bottom line is that, while the shift to a meta-regulatory model should be welcomed for enabling reflexive and adaptive regulation, we must also be weary of its risk of collapsing in the absence of well-resourced and independent institutions. Indeed, this risk affects the extent to which the exportation of the DSA outside Europe would be in the public interest.

The concept of meta-regulation

The DSA marks a fundamental shift towards the definition of due diligence obligations for online intermediaries: first, it departs from a system of liability limitations that left a wide range of issues up to self-regulation, in the absence of specific provisions of national law. Second, it produces a comprehensive set of obligations which are imposed directly by EU law but necessitate specific implementation by providers

through a framework that involves self-assessment accompanied by close monitoring by the regulator. This approach, which on the one hand leaves businesses with a significant amount of discretion in the implementation of regulatory principles, and on the other involves a process of continuous evaluation and monitoring of the results, has been called "meta-regulation"[2] or "enforced self-regulation"[3]: "meta" because one (macro) regulator oversees another (micro) regulator in their management of risk; "enforced" because, in case of inadequacy of the self-regulatory practices, the (macro) regulator has the power to take enforcement measures. To determine whether such measures are warranted, meta-regulation establishes norms of organisation and procedure through which self-regulatory practices can be assessed. By doing so, it assumes a fundamentally "reflexive" character[4]: it focuses on enhancing the self-referential capacities of social systems and institutions outside the legal system to achieve broad social goals, rather than on prescribing particular actions.

Furthermore, as noted by Morgan and Yeung[5], at the core of meta-regulation are participatory procedures for securing regulatory objectives and mechanisms that facilitate and encourage deliberation and mutual learning between organisations. Considering these characteristics, the meta-regulation model is particularly apt to deal with complexity and uncertainty, where some experimentation and dialogue between different stakeholders may be necessary. According to Ayres and Braithwaite[6], there are other inherent advantages, including the fact that the rules can be tailored to the specifics of each

regulated entity and adapt more quickly to an evolving environment, in addition to generating typically a higher level of commitment due to the company´s own elaboration of those rules, and imposing a high share of costs of regulation on the regulated entities (as opposed to the regulator).

On the other hand, weaknesses of the model include the regulator´s costs of regularly monitoring and approving a vastly increased number of rules, the possibility that regulated entities write rules in a way that assists them to evade the spirit of the law (as occurred, for instance, with the implementation of the NetzDG law in Germany[7]) and the lack of effective independence of those who certify the adequacy of the measures undertaken. We return to these points below, explaining how they might apply in the context of the DSA.

Meta-regulation in the DSA

Chapter III in the DSA deals with due diligence obligations for intermediary service providers. To provide a harmonised framework for due diligence obligations and promote a safe, predictable and trustworthy online environment where respect for fundamental rights is ensured, the Regulation distinguishes different types of intermediaries, based on the type, size and nature of their services. The more demanding types of obligations concern very large online platforms (VLOPs) and very large online search engines (VLOSEs), which are the focus of this contribution.

This is because it is with regard to these categories of intermediaries that the meta-regulatory character of the DSA is

most evident: once designated, these entities are effectively required to act as risk regulators, subject to the oversight and enforcement by the European Commission, the national Digital Services Coordinators and the European Board for Digital Services in their capacity as meta-regulators. Specifically, VLOPs and VLOSEs are required under Article 34 to conduct regular assessments of any systemic risks stemming from the design or functioning of their service and its related systems (including algorithmic systems), or from the use made of their services, and provide information to the Commission and the Digital Services Coordinator upon request. They also must put in place, pursuant to Article 35, reasonable, proportionate and effective measures for the mitigation of such risks. Further, a similar obligation was introduced relatively late in the process of DSA negotiations (in 2022, after Russia's invasion of Ukraine) to deal with the event of a "crisis", i. e., extraordinary circumstances leading to a serious threat to public security or public health in the EU or a significant part of it. According to Article 36, in such a situation the Commission can request VLOPs and VLOSEs to assess and mitigate the risks of their contribution to the serious threats that have been identified, and report over them at regular intervals.

As a mechanism to document the compliance with the above-mentioned measures, under Article 37, VLOPs and VLOSEs shall be subject, at their own expense and at least once a year, to independent audits to assess compliance. They must also transmit to the competent Digital Services Coordinator, the Commission and the Board (and make public within

3 months) audit reports, as well as audit implementation reports (showing how the audit´s recommendations have been addressed). These audit obligations constitute a critical element for the functioning of the meta-regulatory framework, providing a necessary check on the implementation of the measures that have been undertaken as part of the providers´ due diligence. The same auditing applies to the implementation of commitments contained in voluntary codes of conduct that can be drawn up to contribute to the proper application of the DSA under Article 45, and the effectiveness of which must be regularly monitored and evaluated by the Commission and the Board[8]. The codes of conduct facilitate this by establishing clear objectives and key performance indicators, drawing from the lessons learned[9] by the Commission with the Code of Practice on Disinformation about the ineffectiveness of general commitments without concrete measurement criteria. Furthermore, Article 41 of the DSA requires VLOPs and VLOSEs to set up a compliance function, independent from their operational function, which serves as a channel of cooperation with the Commission and the Digital Service Coordinators. Among other duties, the management body of the compliance function must devote sufficient time to the consideration of risk management measures, ensure that adequate resources are allocated to risk management, and approve and review at least once per year the risk management, monitoring and minimisation policies of that VLOP or VLOSE.

All these obligations are prodromic to a process of dialogue with the regulator, in particular on the adequacy of the mea-

sures adopted, possibly leading to the adoption of enforcement measures. For instance, in the case of systematic failure to comply with the codes of conduct, the Commission and the Board may invite the signatories to the codes to take the necessary action. Similarly, in the context of the crisis response mechanisms, the Commission may, on its own initiative or at the request of the provider, engage in a dialogue to determine whether the implemented measures are effective and proportionate. If it considers that they are not, the Commission may (after consulting the Board) request the provider to review them. Ultimately, Digital Services Coordinators may accept and make binding the compliance commitments offered by those providers, impose fines and periodic penalty payments, and exercise a range of enforcement measures as per Articles 51 and 52. These backstops are essential incentive mechanisms for the due diligence that meta-regulation seeks to promote.

The meta-regulatory framework is also supplemented by flanking obligations, such as a data access framework for vetted researchers, transparency reporting to the broader public about the risk assessment and identification (in addition to the audit and audit implementation reports), as well as the human resources dedicated to content moderation by each VLOP and VLOSE provider. These create an opportunity for further monitoring of the adequacy of the measures adopted, thus potentially improving the regulator's detection of non-compliance. In fact, the Board will draw from these sources when publishing yearly reports, in cooperation with the Commission,

to identify the most prominent and recurrent systemic risks, along with best practices for VLOPs and VLOSEs providers.

Open issues and criticism

Having explained the dynamics at play in the DSA, let us return to some of the criticism that has been raised against the use of meta-regulation. The first one we mentioned, having to do with the costs of monitoring and approving a vastly increased number of rules, has been directly addressed by the latest version of the DSA: its Article 43 now provides that the Commission shall charge an annual supervisory fee to providers of VLOPs and VLOSEs upon their designation as such. While the criteria used to determine the amount are to be developed in implementing acts of the Commission according to pre-established criteria, one could question the rationale for the establishment of a cap of 0,05% of the worldwide annual net income in the preceding financial year. Indeed, considering that the fee is intended to cover the estimated costs that the Commission incurs in relation to its supervisory tasks under the DSA, and that there is concern[10] about its insufficient enforcement resources, one may wonder whether the Commission might not have underestimated the costs that can be raised by a non-cooperating firm.

The second concern relates to the possibility for regulated entities to pursue a strategy of stylised compliance, crafting rules in a way that enables them to evade the spirit of the law. In principle, regular reporting and monitoring should permit

the detection of this kind of behaviour and trigger remediation, with a request to modify the risk identification and management measures. However, there is a risk that the depth of inquiry into each relevant document will depend on the resources available for the relevant regulator - a matter that, as seen above, is not uncontroversial. To prevent regulatory failure, a further instrument in the toolbox is the possibility that the European Commission or the national Digital Services Coordinator receive this information from a researcher who has obtained access pursuant to Article 40, or to anyone who has examined the auditing and self-assessment documents made public by the relevant VLOP or VLOSE under Article 42. This could give rise to a complaint by a user of those services or by a body mandated to exercise the rights of the DSA pursuant to Article 53, or even a private action for compensation of any consequent damages (a measure introduced under Article 54 by the latest version of the DSA).

Notably, providers are only required to make risk assessments, mitigation measures and auditing reports public three months after the receipt of each audit, which creates a delay for the possible detection. In the absence of this documentation, the data access framework might be insufficient to detect misconduct in real-time. Furthermore, those qualified researchers that are granted access to data may not have access to complete datasets, due to the need to take into account the interests of VLOPs and VLOSEs (including the protection of trade secrets) and those of their users (including privacy and data protection). Compared to Digital Services Coordinators, they may

also lack the overarching structure necessary to conduct a comprehensive and systematic review of the compliance with each provider's practices. A different type of safeguard used in the DSA to ensure that VLOP and VLOSE providers undertake appropriate commitments is to include the participation of other stakeholders from the start of the meta-regulatory conversation. For instance, Recital 90 requires their risk assessment and mitigation to be based on the best available information and scientific insights, and that their assumptions in this exercise are tested with the groups most impacted by the risks and the measures they take. This may entail involving representatives of groups potentially impacted by their services. Additionally, Article 45(2) grants the Commission the power, where significant systemic risk emerges and concerns several VLOPs and VLOSEs, to invite relevant stakeholders to participate in the drawing up of codes of conduct, including by setting out commitments to take specific risk mitigation measures, as well as a regular reporting framework on any measures taken and their outcomes. However, the practical effect of these provisions remains to be seen: the latter is a highly circumscribed possibility, while the former is only contained in Recitals and not in the operative text of the DSA.

The third and perhaps most contentious point concerns the lack of effective independence of those who certify the measures undertaken. In the original formulation by Ayres and Braithwaite, this criticism was directed at the insufficient independence of the compliance directors, who are required to report to regulators on pain of criminal liability any manage-

ment overruling of compliance directives. In the context of the DSA, such criminal liability is not envisaged, and no specific requirements are detailed for the independence of the compliance function. As a result, the effectiveness of this safeguard may be questioned. On the other hand, more elaborate criteria are established for the independence of the auditors: Article 37 requires that they do not provide audits for contingency fees; that they have not provided non-audit services on matters audited to the provider for the past 12 months and do not provide them for 12 months after the completion of the audits; and that they have not provided auditing services to the provider or any legal person connected to it for more than 10 consecutive years. Nevertheless, it is easy to foresee that the mere expectation to provide auditing services to the same provider in the future might influence the auditor's objectivity. As convincingly argued on this blog[11], this situation could only be tackled through a public auditing framework - although for this to work effectively, a robust system of safeguards against regulatory capture[12] must be defined.

Effects beyond the EU?

There is one additional reason why we should not simply brush aside healthy scepticism on the institutional capacity to ensure the proper application of the DSA: the rest of the world is watching. Since the Regulation seeks to deal with content moderation challenges that are faced in a similar manner by regulators, intermediaries and users across the globe, it won't

be long before we see legislation in other jurisdictions inspired by the DSA.

By way of example, the Brazilian Congress has already been debating a bill that would replicate some of the dynamics of the DSA, including the meta-regulatory approach. The latest version[13] of the bill attributes a crucial role to self-regulation for social networks, search engines and messaging services, overseen by a self-regulatory institution of their own creation which would have the power to adopt and disseminate codes of conduct for the implementation of the law. Differently from the DSA, these codes would not be validated by a public authority: instead, it would be the Brazilian Internet Steering Committee (a multistakeholder body composed of 9 government representatives, 4 business representatives, 4 civil society representatives, 3 science and technology representatives, and a representative with notorious knowledge of Internet matters) which would become the entity to issue guidelines for the implementation of those codes, and certify compliance by the self-regulatory institution with the principles set out in the bill. More worryingly, the burden of monitoring and enforcement would be placed on the market, in particular through its self-regulatory institution. Institutional arrangements of this kind may be the norm rather than the exception in countries where public institutions suffer from insufficient resources and a low level of trust, with foreseeable consequences for the protections that the legislation seeks to provide to platform users and society.

One should also not underestimate a second type of Brus-

sels effect[14], which has to do with the possibility that regulated entities themselves export outside the EU the compliance framework that they establish under the DSA. While this could substantially improve the dialogue between platforms and regulatory institutions abroad, in the absence of adequate institutional backing it raises the twofold risk of selective importation and insufficient consideration of the local context. To prevent this, we need to ensure that the complexities of meta-regulation are properly communicated and understood. This starts from the realisation that the due diligence obligations imposed on providers are not to be taken in isolation: they are part and parcel of a broader ecosystem geared to enable appropriate experimentation, monitoring, and regulatory dialogue with possible escalation to enforcement. And crucially, robust mechanisms of oversight and accountability must be built into this framework if it is to deliver on its promises.

References

1. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) [2022] OJ L277/1.

2. Cary Coglianese and Evan Mendelson, "Meta-Regulation and Self-Regulation" in Martin Cave, Robert Baldwin, Martin Lodge (eds), *The Oxford Handbook on Regulation* (2010) <https://ssrn.com/abstract=2002755> accessed 5 November 2022.

3. Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992), <http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf> accessed 5 November 2022.

4. Neil Gunningham, "Regulatory Reform and Reflexive Regulation: Beyond Command and Control" in Eric Brousseau, Tom Dedeurwaerdere, and Bernd Siebenhüner (eds), *Reflexive Governance for Global Public Goods* (Cambridge, MA, 2012; online edn, MIT Press Scholarship Online, 22 August 2013), <https://doi.org/10.7551/mitpress/9780262017244.003.0103 accessed 5 November 2022.

5. Bronwen Morgan and Karen Yeung, *An Introduction to Law and Regulation: Text and Materials* (Law in Context, Cambridge University Press 2007), doi:10.1017/CBO9780511801112 accessed 5 November 2022.

6. Ian Ayres and John Braithwaite, *Responsive Regulation: Transcending the Deregulation Debate* (Oxford University Press 1992), <http://johnbraithwaite.com/wp-content/uploads/2016/06/Responsive-Regulation-Transce.pdf> accessed 5 November 2022.

7. Amélie Heldt, "Reading between the lines and the numbers: an analysis of the first NetzDG reports" (2019) 8(2) Internet Policy Review <https://policyreview.info/articles/analysis/reading-between-lines-and-numbers-analysis-first-netzdg-reports> accessed 5 November 2022.

8. It is also worth noting that these codes of conduct are not only available for VLOPs and VLOSEs, thus offering an opportunity for other intermediaries to be brought under this particular meta-regulatory procedure.

9. Commission (EC) "European Commission Guidance on Strengthening the Code of Practice on

Disinformation" COM (2021) 262 final <https://digital-strategy.ec.europa.eu/en/library/guidance-strengthening-code-practice-disinformation> accessed 5 November 2022.

10. Letter from Monique Goyens and Ursula Pachl (The European Consumer Organisation) to Ms Margrethe Vestager (Executive Vice-President European Commission), "The European Commission Must Allocate Sufficient Resources to DMA and DSA Enforcement" (May 10, 2022) <https://www.beuc.eu/sites/default/files/publications/beuc-x-2022-045_letter_to_evp_vestager_ec_must_allocate_sufficient_resources_to_dma_and_dsa_enforcement.pdf> accessed 5 November 2022
11. Ben Wagner, Martin Husovec, Ľuboš Kukliš and Eliška Pírková, "The next step towards auditing intermediaries" (*Verfassungsblog*, 23 February 2022) <https://verfassungsblog.de/dsa-auditing/> accessed 5 November 2022.
12. Ernesto Dal Bó, "Regulatory Capture: A Review" (2006) 22(2) Oxford Review of Economic Policy <https://doi.org/10.1093/oxrep/grj013> accessed 5 November 2022.
13. Substitutivo ao Projeto de Lei No 2.630, de 2020 (Senado Federal, Alessandro Vieira – Autor, Orlando Silva - Relator) (BR) <https://www.camara.leg.br/midias/file/2022/03/fake.pdf> accessed 5 November 2022.
14. Anu Bradford, *The Brussels Effect: How the European Union Rules the World* (Oxford University Press 2020).

Daphne Keller

The European Union's New DSA and the Rest of the World

The European Union's Digital Services Act (DSA) is a major milestone in the history of platform regulation. Other governments are now asking themselves what the DSA's passage means for them. This post will briefly discuss that question, with a focus on platforms like Facebook or YouTube and their smaller would-be rivals.

Direct global impact

The Good: Transparency, fair processes, improved platform practices

The DSA will have major spillover effects for the rest of the world. In some cases, this will lead to real benefits for users, mostly in the form of platform features or internal systems built for the DSA, but deployed globally. For example, platforms' more clearly articulated speech policies under Article 14 and better explanations of algorithms under Articles 27 and 38 will improve understanding both inside and outside the EU. The largest platforms will likely also globally deploy some specific user protection measures, such as improved tools for communicating with the "accusers" and the "accused" in notice and action systems. Positive changes made as part of very large online platforms' (VLOPs') risk mitigation efforts under Article 35 seem likely to be global, as will more indirect benefits resulting from things like improved researcher access to data under Article 40.

The Bad: Fundamental rights risks and competition burdens

Not all of the DSA's spillover effects will be beneficial, however. The harms will be harder to identify, but I believe they will be real. One set of risks involves Internet users' rights. Civil society groups have raised the alarm,[1] for example, about future back-room negotiations between regulators and platforms as part of Article 36 "crisis response mechanisms" or Article 35 "risk mitigation" measures. If history is any indication, platforms like YouTube, Facebook, Microsoft, and Twitter – the companies that negotiated the Hate Speech Code of Conduct and created a controversial[2] upload filtering[3] system for terrorist content -- will readily make concessions to European regulators in order to protect their own businesses. The resulting standards have been publicly criticized[4] by civil society groups for bypassing democratic processes and forfeiting users' fundamental rights. Whatever we think of the *current* set of regulators and platform representatives who will negotiate comparable new agreements under the DSA, we should be wary of granting too much discretion and power over fundamental rights to their successors.

The other predictable global harm will be to competition. The DSA burdens even very small platforms with obligations that today's incumbents never shouldered, or else took on only much later in their development. Facebook, for example, first[5] released a transparency report in 2013, when it was worth $139 billion.[6] It first allowed users to appeal removals of photos, videos, and posts (but not comments) in 2018,[7] when the com-

pany was worth $374 billion[8] and had some 35,000[9] employees. Newer market entrants will take on similar obligations at a much earlier stage: once they reach just €10 million and *fifty* employees. (These are the platforms above the DSA's "small or micro" category. A chart listing which DSA obligations will affect companies of different sizes is here.[10])

The DSA also requires transparency and user notice-and-appeal operations on a scale that even the largest incumbents have never attempted. YouTube, for example, currently allows appeals for the roughly 9 million videos it removes every three months. But it does not yet do what the DSA will require: offering appeals for the additional *billion* comments[11] it removes in the same time period. That's more than a hundred-fold expansion. YouTube will presumably spend the money to extend appeals and other DSA requirements to comments – a category of online speech that can be important in attracting and retaining users, but that is often high in quantity and low in quality. Academic researchers attempting to assess sentiment or political valence of YouTube comments, for example, have complained that they are frequently "irrelevant", "trivial",[12] and "tedious" to review. For smaller companies, simply eliminating comments may be the more affordable choice. A second, and perhaps even more important change in the scale of operations under the DSA may likely come from its extension of transparency and notice-and-appeal operations to content that is demoted or rendered less visible, rather than removed.

Other DSA obligations, like Article 21's out-of-court dispute resolution requirement for disagreements about content mod-

eration, are much more untested. The threat of outside review may incentivize[13] better moderation by platforms in the first place. And settlement bodies will surely remedy incorrect moderation decisions in many cases. But there are also a lot of ways that they may go awry, including by providing conflicting outcomes that encourage forum-shopping by users and create pervasive fragmentation and inconsistency in interpretation of platforms' community standards. Platforms above the "small or micro" DSA category will all, under the DSA, have to participate in this experimental system. They also have to fund it – paying their own costs and those of users who prevail in disputes.

As I discussed in a previous post,[14] it is not clear that requiring platforms with just a few hundred employees to build out detailed and cumbersome new content moderation, "due process", and transparency capabilities will have upsides sufficient to justify the barriers to market entry these burdens will create. If we want smaller platforms to one day rival today's giants, perhaps we should not treat them like Meta or Google so early in their growth. In this respect, too, the DSA will have worldwide effect. Companies like Facebook and Twitter grew by being globally available, and expanding gradually in regions where significant user bases developed. Their successors will not have this flexibility. Investors and entrepreneurs around the world will factor in the now-substantial compliance costs that come with attracting EU users before they even consider launching new platform businesses.

The Future: Uncertain

Those are my predictions. The DSA's future is uniquely difficult to game out, though. The DSA superficially resembles another major regulation, the GDPR, particularly in its standardized compliance practices and reliance on regulatory action. But while the GDPR built on long-established legal structures, platform practices, and regulatory relationships, the DSA's mechanisms and systems have been, until now, theoretical or tested only at much smaller scale.

That makes the DSA, like any other cutting-edge tool or system, something of an experiment. Some of its innovations will probably be great successes. Others will not. If Article 17 truly requires platforms to notify users *every* time their content is demoted or otherwise restricted in visibility, for example, users may rapidly tire of the resulting flood of notices. Or platforms may refrain from deploying beneficial measures to, for example, demote "borderline"[15] content in order to avoid costs and hassle. That would leave users in the EU more exposed to potential disinformation, racial slurs, and other harmful content. The DSA's unprecedented and extensive appeal mechanisms, similarly, will have some predictable benefits. But it could also turn out that users who avail themselves of measures like Article 21's out-of-court dispute mechanisms are disproportionately far-right trolls, crackpots, and contrarians. At a minimum, research suggests they may be mostly men.[16] That would leave us in need of different tools to protect the rights of online speakers who are marginalized or simply less assertive, as well

as readers and viewers whose rights to *access* information have been harmed by improper takedowns. As a final example, the Commission may build its planned, unprecedented database under Article 24, hosting billions of notices about platforms' content moderation decisions, only to discover both high costs and important limitations. This may occur in particular if the platforms' removal of any personally identifiable information means that researchers using the database often have no idea what content was actually removed, or which users were actually affected.

Impact on national laws around the world

Lawmakers around the world are champing at the bit to enact their own new platform regulations. My suggestion to them would be to wait a few years before enacting laws that look like the DSA. There is plenty of other regulatory work to be done in the meantime. The U.S., for example, is in dire need of a real federal privacy law. We could also use basic legal reforms to enable "adversarial interoperability"[17] or "competitive compatibility"[18] – allowing new technologies to interoperate, build on, and draw users away from today's incumbents. There is room for productive legal debate and reform relating to more ambitious "middleware"[19] or "protocols, not platforms"[20] approaches to content moderation, as well. Any "DSA 2.0" in other countries will be better if it builds on the demonstrated successes and inevitable failures of particular DSA provisions, after that law has actually been launched and operationalized.

There are a few more specific lessons from the DSA that bear notice in other countries.

Internal company "due process" changes

To DSA drafters' credit, many of its rules in areas like content moderation and transparency reflect longstanding asks from global civil society. The DSA also avoided problematic "turnaround time" requirements of the sort enacted in Germany[21] or required under the EU Terrorist Content Regulation and proposed in other countries including Nigeria,[22] which would require takedown on 24 hours' notice. Lawmakers in other countries should take heed of the DSA's approach, but also be aware of the potential harms from unnecessary international fragmentation in laws' details. Platforms of any size, but particularly small ones, would struggle with similar-but-not-identical requirements across borders – with resulting waste of operational resources, damage to competition, and risk of further Internet balkanization. One tool to address this concern might be the modular[23] model proposed by former U.S. FCC Commissioner Susan Ness and Chris Riley. Following that approach, lawmakers might select some standardized legal language or requirements for consistency across borders, while adopting their own rules where there are grounds for national divergence.

Regulatory relationships

Left-leaning thinkers in the U.S. have long been attracted[24] to the idea of creating new regulatory bodies, or empowering ex-

isting ones, to assume roles similar to those held by the Commission and DSCs under the DSA. Absent significant change in the U.S. Congressional balance of power, that does not seem likely to happen. Any U.S. "DSA 2.0" would likely lack that very important component of the EU's new system. The same may be true – and perhaps *should* be true – in many other parts of the world. Some activists in some Latin America countries, for example, have long cautioned against empowering regulators in this manner. Indian experts[25] have similarly been critical of the role assumed, and rules proposed, by that country's Ministry of Electronic and Information Technology.

Platform removal obligations for "lawful but harmful" speech

A major concern in platform regulation, both inside and outside of the EU, is about the impact of speech that is legal but causes harm. This category of "lawful but awful" speech exists, in some form, within any human rights-compliant legal system. The DSA chose not to regulate such speech directly by prescribing new content prohibitions to be enforced by platforms, but instead to regulate the systems and processes by which platforms enforce their own Community Guidelines or other speech rules. That avoids major human rights questions that would arise from laws restricting previously lawful speech. I think it is also wise for reasons of administrability and fair process, as I have discussed elsewhere.[26] But some countries may be tempted to instead follow the UK, where lawmakers have now spent several years in an on-again / off-again flirtation with regulating "harmful" speech.

"Must-carry" obligations

Courts in countries from Germany[27] to Brazil have ordered platforms to reinstate content that the companies themselves deemed unlawful or violative of their Terms of Service. Lawmakers in Poland,[28] Mexico[29] and elsewhere around the world have considered legislation to create carriage obligations. Legislators have also enacted (Australia)[30] or considered (U.S.,[31] UK)[32] *de jure* or *de facto* carriage requirements for specific content, usually relating to news or elections. Few U.S. experts would have considered such obligations feasible until very recently, when very strange and crudely crafted "must-carry" laws were enacted in two states: Texas[33] and Florida.[34] The resulting litigation[35] has sent an epoch-defining First Amendment question hurtling toward America's newly reckless, conservative-dominated Supreme Court. Other countries' incremental creep toward carriage mandates for major platforms may abruptly be bypassed by tremendous changes in the U.S.

Conclusion

The DSA is a far better law than most that have been proposed in other parts of the world. I have encouraged[36] U.S. lawmakers to emulate it in many respects. But lawmakers around the world should view it as a starting point, rather than an end point, in considering potential regulations in their own countries. That means looking at the law's substantial strengths, but also asking how to do better.

References

1. EDRi, "On New Crisis Response Mechanism and Other Last Minute Additions to the DSA" (EDRi, 2022) <https://edri.org/wp-content/uploads/2022/04/EDRi-statement-on-CRM.pdf> accessed 21 November 2022.
2. Open Letter from Access Now and others to Members of the European Parliament (*Center for Demoracy & Technology*, 4 February 2019) <https://cdt.org/wp-content/uploads/2019/02/Civil-Society-Letter-to-European-Parliament-on-Terrorism-Database.pdf> accessed 21 November 2022.
3. Human Rights Watch, "'Video Unavailable' – Social Media Platforms Remove Evidence of War Crimes" (Human Rights Watch, 2022) <https://www.hrw.org/report/2020/09/10/video-unavailable/social-media-platforms-remove-evidence-war-crimes> accessed 21 November 2022.
4. EDRi, "Guide to the Code of Conduct Hate Speech" (*EDRi*, 3 June 2016) <https://edri.org/our-work/guide-code-conduct-hate-speech/> accessed 21 November 2022.
5. Hayley Tsukayama, "Facebook releases first report on world governments' data requests" *The Washington Post* (Washington, D.C., 27 August 2013) <https://www.washingtonpost.com/business/technology/facebook-releases-first-report-on-world-governments-data-requests/2013/08/27/40e2d396-0f24-11e3-8cdd-bcdc09410972_story.html> accessed 21 November 2022.
6. Companies Market Cap, "Market capitalization of Meta Platforms" (*Companies Market Cap*) <https://companiesmarketcap.com/meta-platforms/marketcap/> accessed 21 November 2022.
7. "Facebook unveils appeal process for when it removes posts" (*Yahoo! News*, 24 April 2018) <https://sg.news.yahoo.com/facebook-unveils-appeal-process-removes-posts-092814445.html> accessed 21 November 2022.
8. Companies Market Cap, "Market capitalization of Meta Platforms" (*Companies Market Cap*) <https://companiesmarketcap.com/meta-platforms/marketcap/> accessed 21 November 2022.
9. Macrotrends, "Meta Platforms: Number of Employees 2010-2022" (*macrotrends*) <https://www.macrotrends.net/stocks/charts/META/meta-platforms/number-of-employees accessed 21 November 2022.
10. "DSA Rules by Entity and Size (without VLOSE)" <https://docs.google.com/spreadsheets/d/1rlFtpZmqiW4Vt1IQ54EaJUsk1XGFPzkDdCnLjF-xq3Y/> accessed 21 November 22.

11. Appellees' Brief 13 (US) <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=3657&context=historical> accessed 21 November 2022.

12. Rhitabrat Pkharel and Dixit Bhatta, "Classifying YouTube Comments Based on Sentiment and Type of Sentence" [2021] 2111.01908v1 arXiv <https://arxiv.org/pdf/2111.01908.pdf> accessed 21 November 2022.

13. Lenka Fiala and Martin Husovec, "Using Experimental Evidence to Improve Delegated Enforcement (forthcoming)" (2018) Intl Rev of L and Economics <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3218286> accessed 21 November 2022.

14. Daphne Keller, "The DSA's Industrial Model for Content Moderation" (*Verfassungsblog*, 24 February 2022) <https://verfassungsblog.de/dsa-industrial-model/> accessed 21 November 2022.

15. Meta, *Types of Content We Demote* (Corporate Policy, 2022) <https://transparency.fb.com/features/approach-to-ranking/types-of-content-we-demote> accessed 21 November 2022.

16. Jon Penney, "Privacy and Legal Automation: The DMCA as a Case Study" [2019] 22 Stanford Tech L Rev 412 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3504247> accessed 21 November 2022.

17. Cory Doctorow, "Adversarial Interoperability" (*Electronic Frontier Foundation*, 2 October 2019) <https://www.eff.org/deeplinks/2019/10/adversarial-interoperability> accessed 21 November 2022.

18. Cory Doctorow, "Competitive Compatibility: Let's Fix the Internet, Not the Tech Giants" [2021] 64 Communications of the ACM 26 <https://cacm.acm.org/magazines/2021/10/255710-competitive-compatibility/abstract> accessed 21 November 2022.

19. Daphne Keller, "The Future of Platform Power: Making Middleware Work" [2021] 32(3) Journal of Democracy 168 <https://www.journalofdemocracy.org/articles/the-future-of-platform-power-making-middleware-work/> accessed 21 November 2022.

20. Mike Masnick, "Protocols, Not Platforms: A Technological Approach to Free Speech" (*Knight First Amendment Institute*, 21 August 2019) <https://knightcolumbia.org/content/protocols-not-platforms-a-technological-approach-to-free-speech.> accessed 21 November 2022.

21. Federal Ministry of Justice, *Act to Improve Enforcement of the Law in Social Networks - Basic Information* (2017) <https://www.bmj.de/DE/Themen/FokusThemen/NetzDG/NetzDG_EN_node.html> accessed 21 November 22.

22. Iyunola Adekanye and others, "NITDA Draft Code for Interactive Computer Service Platforms and Internet Intermediaries" (*JD Supra*, 27 June 2022) <https://www.jdsupra.com/legalnews/nitda-draft-code-for-interactive-2201828/>.

23. Chris Riley and Susan Ness, "Modularity for Internet Governance" (*Lawfare*, 19 July 2022) <https://www.lawfareblog.com/modularity-international-internet-governance> accessed 21 November 2022.

24. Shiva Stella, "Public Knowledge Applauds Bill Creating Digital Regulator To Rein In Big Tech" (*Public Knowledge*, 12 May 2022) <https://publicknowledge.org/public-knowledge-applauds-bill-creating-digital-regulator-to-rein-in-big-tech/> accessed 21 November 2022.

25. Udbhav Tiwari, "India's new intermediary liability and digital media regulations will harm the open internet" (*Mozilla*, 2 March 2021) <https://blog.mozilla.org/netpolicy/2021/03/02/indias-new-intermediary-liability-and-digital-media-regulations-will-harm-the-open-internet/> accessed 21 November 2022.

26. Daphne Keller, "Lawful but Awful? Control over Legal Speech by Platforms, Governments, and Internet Users" [2022] Univ of Chicago L Rev <https://lawreviewblog.uchicago.edu/2022/06/28/keller-control-over-speech/> accessed 21 November 2022.

27. Matthias Kettemann and Torben Klausa, "Regulating Online Speech: Ze German Way" (*Lawfare*, 20 September 2021) <https://www.lawfareblog.com/regulating-online-speech-ze-german-way> accessed 21 November 2022.

28. Adam Easton, "Poland proposes social media 'free speech' law" (*BBC*, 15 January 2021) <https://www.bbc.com/news/technology-55678502> accessed 21 November 2022.

29. Sandra Weiss, "Mexico: Social media bill meets with skepticism" (*Deutsche Welle*, 10 February 2021) <https://www.dw.com/en/mexico-social-media-regulation-bill-meets-with-skepticism/a-56527781> accessed 21 November 2022.

30. Australian Competition and Consumer Commission, *News media bargaining code* <https://www.accc.gov.au/focus-areas/digital-platforms/news-media-bargaining-code/news-media-bargaining-code> accessed 21 November 2022.

31. S 673, 117th Congress <https://www.congress.gov/bill/117th-congress/senate-bill/673/actions> accessed 21 November 2022.

32. United Kingdom Government, *Explanatory Notes to the Online Safety Bill* (2022) <https://www.gov.uk/government/publications/fact-sheet-on-enhanced-protections-for-journalism-within-the-online-safety-bill> accessed 21 November 2022.

33. Texas HB 20 <https://docs.google.com/document/d/1DP62t5HoUiD-k_ac4hwcibejFIWfOK-XU0uFG1SC-HI/> accessed 21 November 2022.

34. Florida SB 7072 <https://docs.google.com/document/d/1GfPBmjqkfLICCOLhcxmmoPL77b9MoyHZ5hMF5CtKESg> accessed 21 November 2022.

35. Daphne Keller, "NetChoice Legal Arguments and Options" (2022) <https://docs.google.com/document/d/1U8Ed-FfOz7JgS7y00KsHGo7gu3ky5ZYs/edit#heading=h.jxudlqmzppge> accessed 21 November 2022.

36. Daphne Keller, "For platform regulation Congress should use a European cheat sheet" (*The Hill*, 15 January 2021) <https://thehill.com/opinion/technology/534411-for-platform-regulation-congress-should-use-a-european-cheat-sheet/> accessed 21 November 2022.

Read more

Verfassungsblog

Verfassungsblog is a not-for-profit academic and journalistic open access forum of debate on topical events and developments in constitutional law and politics in Germany, the emerging European constitutional space and beyond. It sees itself as an interface between the academic expert discourse on the one hand and the political public sphere on the other.

Check out Verfassungsblog.de to discover all our articles, debates and other resources.

Our Books

We've got more open access books on other topics available for you at Verfassungsblog.de/Books.

Verfassungsbooks
ON MATTERS CONSTITUTIONAL

The Digital Services Act was finally published in the Official Journal of the European Union on 27 October 2022. This publication marks the end of a years-long drafting and negotiation process, and opens a new chapter: that of its enforcement, practicable access to justice, and potential to set global precedents. The Act has been portrayed as Europe's new "Digital Constitution", which affirms the primacy of democratic rulemaking over the private transnational ordering mechanisms of Big Tech. With it, the European Union aims once again to set a global standard in the regulation of the digital environment. But will the Digital Services Act be able to live up to its expectations, and under what conditions?