



View metadata, citation and similar papers at core.ac.uk

provided by archive of European integration

rought to you by

COBE

on

in Europe

A contribution to the Exploration
Shaping Digital Policy - Towards a Fair Digital Society?

Governance of Digitalization in Europe

A contribution to the Exploration Shaping Digital Policy - Towards a Fair Digital Society?

Dr. Ben Wagner and Dr. Carolina Ferro

Legal Notice

© May 2020

Bertelsmann Stiftung

Carl-Bertelsmann-Straße 256

33311 Gütersloh

www.bertelsmann-stiftung.de

Responsible for content

Falk Steiner, Bertelsmann Stiftung

Authors

Dr. Ben Wagner and Dr. Carolina Ferro

Editing

Barbara Serfozo

License

The text of this publication is protected by copyright and licensed under the Creative Commons Attribution 4.0 International (CC BY-SA 4.0) license (Attribution – ShareAlike). You may reproduce and redistribute the material as long as you include the appropriate copyright and licensing information. You must indicate whether any changes have been made. If you change the material, you must distribute your contributions under the same license as the original. The full license text can be found at:

<https://creativecommons.org/licenses/by-sa/4.0/legalcode.de>.



Excluded from this are all photos and logos. They are not licensed under the above-mentioned CC license.

Cover photo: © Getty Images/iStockphoto/Mehmet Şeşen

Portrait photos: © Ansichtssache_Britta Schröder

DOI 10.11586/2020018 <https://doi.org/10.11586/2020018>

Contents

1	Preface	5
2	Vorwort	7
3	Zusammenfassung	9
4	Executive summary	11
5	Introduction	13
6	The current state of Digital Governance: Four case studies	16
6.1	The German Network Enforcement Act (NetzDG)	16
6.2	The automobile (software) emissions scandal	20
6.3	The internet multistakeholder governance model	24
6.4	The pending European platform regulation proposal and the Digital Services Act.....	27
7	Why are many digital governance initiatives failing?	31
8	What might “better” governance of digitalization look like? A proposal for a digitalization governance model based on the EU Digital Services Act	33
9	Conclusion	39
10	References	40
11	Abbreviations	44
12	About the authors	45

1 Preface

Digital policy is a unique policy area. As a cross-cutting policy issue, it has an impact not only on individual areas of regulation but on almost all other policy areas as well. Aspects of digital policy such as data regimes, cybersecurity and standardization issues are relevant not only to the future of the internet or 5G mobile communications infrastructure, but to other areas of our lives to which they are closely linked, which range from automated driving to digital assistance systems in education and healthcare to the digitalization of sectors such as agriculture and construction. Nevertheless, regulation efforts have thus far been primarily sector-specific and national in their scope. With a few exceptions, such as the EU's controversial General Data Protection Regulation, there are few digital policy frameworks in place for Europe that defines and integrates basic principles for broad application. Instead, we face a situation in which a variety of approaches stand side by side, at times complementing each other but also – all too often – competing with each other in ways that foster inconsistencies. The development of Europe's 5G infrastructure is illustrative of this state of affairs. Despite the presence of what were originally uniform objectives across Europe, 28 nationally distinct tendering procedures with different requirements have since emerged. As a result, we must now find ways to manage the problems associated with having three or more networks per country, high costs, a difficult debate over security and the threat of dependency on non-EU providers.

The coexistence of two worlds of digitalization is also creating new tensions. On the one hand, there is the “original” world of digitalization – primarily the internet industry – that is increasingly regulated by digital policy. On the other hand, there is the world of those digitalizing areas in traditional industries – such as the automotive industry – where the existing regulatory framework is increasingly challenged by digitalization. We nonetheless observe a trend toward the creation of common European rules for digitalization that should help secure Europe's standing as a stable location of values and competitiveness. In order to deliver such results, European digital policy needs not only an EU able to take action internationally but one that has the institutional capacity to take action internally. In addition to common European rules, this requires improved coordination across the individual sectors, both to strengthen the digital single market and to effectively enforce the European legal framework vis à vis third parties in the market. These prerequisites must be in place if Europe is to ensure its position as a strong digital location. However, since a complete shift of these areas to the European level does not seem realistic in the near future, other approaches are required.

The expertise presented here by Dr. Carolina Ferro and Dr. Ben Wagner on behalf of the Bertelsmann Stiftung draws on a variety of examples to highlight the shortcomings of current practice and outlines possible ways forward toward a European, cross-sectoral and yet flexible approach to governance that can address the unforeseeable problems of the future. As a proposal for discussion, this publication considers both national concerns and issues associated with European coordination. It proposes establishing a variety of discussion forums as well as clearly defined decision-making mechanisms for the common interpretation of European law and central support capacities. These steps seem prudent given the fact that several digital policy issues arise in almost all areas, though not at the same time and not permanently or with the same intensity. A European pool of experts complementing the resources of European and national actors could prove a valuable source of support in this respect.

This expert opinion paper was produced within the framework of the Bertelsmann Stiftung's 12-month exploratory project *Shaping Digital Policy – Towards a Fair Digital Society?* Underway since the summer of 2019, the project has identified significant potential for shaping a participatory digital policy in Europe. As part of the same series, two further analyses of European digital strategies (Joschua Helmer 2020) and the changing values in digitalization (Dr. Annegret Bendiek and Dr. Jürgen Neyer 2020) are scheduled to be published soon.

In an effort to facilitate further discussion and debate on the findings of this study, we are publishing this paper under a Creative Commons license (CC BY-SA 4.0 DE). We would like to thank Ben Wagner and Carolina Ferro for a wholly fruitful collaboration. Together with the authors, we would like to express our appreciation to Daphne Keller, Kay Meseberg, Lubos Kuklis, Eliska Pirkova, Paul Jasper Dittrich, Viktoria Grzymek and Louisa Well, whose

comments and insights have enriched this publication. Finally, we would be delighted to receive feedback as well as any constructive criticism regarding the content featured here.



Falk Steiner
Senior Expert Digital Policy
Bertelsmann Stiftung



Ralph Müller-Eiselt
Director Program Megatrends
Bertelsmann Stiftung



2 Vorwort

Die Digitalpolitik ist ein besonderes Politikfeld: als Querschnittsthema betrifft sie nicht bloß einzelne Regulierungsbereiche, sondern wirkt sich auf nahezu alle anderen Politikfelder aus. So sind digitalpolitische Aspekte wie Datenregime, Cybersicherheit oder Normierungsfragen nicht nur für die 5G-Mobilfunk-Infrastruktur oder die Zukunft des Internets relevant, sondern mit vielen verschiedenen Lebensbereichen engmaschig verknüpft – vom automatisierten Fahren im Straßenverkehr über Assistenzsysteme in Bildung und Gesundheit bis hin zur Digitalisierung von Branchen wie der Land- oder Bauwirtschaft. Dennoch dominiert bislang sektorspezifische und nationale Regulierung. Bis auf wenige Ausnahmen wie die umstrittene Datenschutzgrundverordnung fehlt ein digitalpolitischer Rahmen, der übergreifende Grundprinzipien definiert und integriert. Stattdessen steht eine Vielfalt unterschiedlicher Ansätze nebeneinander, die sich teils ergänzen, oft genug aber auch miteinander konkurrieren und Inkonsistenz gedeihen lassen. Der Aufbau der 5G-Infrastruktur ist ein gutes Beispiel: Trotz ursprünglich europaweit einheitlicher Ziele sind unterdessen 28 nationale Vergabeverfahren mit unterschiedlichen Auflagen entstanden. Drei oder mehr Netze pro Land, hohe Kosten, eine schwierige Sicherheitsdebatte und drohende Abhängigkeit von Nicht-EU-Anbietern sind die problematischen Folgen.

Neue Spannungsfelder ergeben sich auch aus dem Nebeneinander zweier Digitalisierungswelten: zum einen die originär digitalen Bereiche vorwiegend der Internetwirtschaft, die durch Digitalpolitik zunehmend reguliert werden, zum anderen die sich digitalisierenden Bereiche klassischer Industrien, bei denen wie etwa in der Automobilbranche der bestehende regulatorische Rahmen zunehmend von der Digitalisierung herausgefordert wird. Ungeachtet dessen ist derzeit ein Trend zu gemeinsamen europäischen Regeln für die Digitalisierung zu beobachten, die Europa als stabilen Standort von Werten und Wettbewerbsfähigkeit erhalten helfen sollen. Doch dazu braucht europäische Digitalpolitik nicht nur eine souverän agierende Union nach außen, sondern auch die nötige institutionelle Handlungsfähigkeit nach innen. Wesentlich hierfür ist neben gemeinsamen europäischen Regeln eine verbesserte Koordinierung über die Einzelsektoren hinweg, um sowohl den Digitalen Binnenmarkt zu ertüchtigen als auch den europäischen Rechtsrahmens gegenüber dritten Akteuren am Markt wirksam durchzusetzen. Beides ist die EU-interne Voraussetzung für einen starken Digitalstandort Europa. Da eine vollständige Verlagerung dieser Bereiche auf die europäische Ebene auf absehbare Zeit nicht realistisch erscheint, sind andere Herangehensweisen geboten.

Die hier vorgelegte Expertise von Dr. Carolina Ferro und Dr. Ben Wagner im Auftrag der Bertelsmann Stiftung zeigt anhand von unterschiedlichen Beispielen die Defizite der bisherigen Praxis auf und skizziert Lösungsansätze für einen europäischen, sektorenübergreifenden und trotzdem flexiblen Governance-Ansatz, der auch für heute noch nicht absehbare Problemstellungen trägt. Dieser Diskussionsvorschlag denkt sowohl nationale Belange als auch europäische Koordination mit. Er beinhaltet nicht nur Gesprächsforen, sondern auch klar definierte Entscheidungsmechanismen zur gemeinsamen Auslegung europäischen Rechts und zentrale Unterstützungskapazitäten. Denn viele digitalpolitische Fragestellungen stellen sich zwar in fast allen Bereichen, aber nicht immer zur gleichen Zeit und nicht immer dauerhaft in gleicher Intensität. Hier könnte ein die Ressourcen europäischer und nationaler Akteure ergänzender europäischer Expertenpool eine wertvolle Hilfe sein.

Diese Expertise ist als Teil der einjährigen Exploration *Digitalpolitik Gestalten – Towards a Fair Digital Society?* entstanden, in der die Bertelsmann Stiftung seit Sommer 2019 wesentliche Gestaltungspotenziale für eine teilhabeförderliche Digitalpolitik in Europa identifiziert hat. In der gleichen Reihe erscheinen kurzfristig zwei weitere Analysen über Europäische Digitalstrategien (Joschua Helmer 2020) und den Wertewandel in der Digitalisierung (Dr. Annegret Bendiek und Dr. Jürgen Neyer 2020).

Um den Diskurs und die Debatte über die Ergebnisse dieser Studie zu erleichtern, veröffentlichen wir sie unter einer freien Lizenz (CC BY-SA 4.0 DE). Wir bedanken uns bei Ben Wagner und Carolina Ferro für die produktive Zusammenarbeit und mit den beiden Autoren zusammen bei Daphne Keller, Kay Meseberg, Lubos Kuklis, Eliska Pirkova, Paul Jasper Dittrich, Viktoria Grzymek und Louisa Well, von deren Anregungen und Impulsen die Publikation

sehr profitiert hat. Über Resonanz und natürlich auch weitere konstruktive Kritik an dieser Publikation würden wir uns sehr freuen.



Falk Steiner
Senior Expert Digitalpolitik
Bertelsmann Stiftung



Ralph Müller-Eiselt
Director Programm Megatrends
Bertelsmann Stiftung



3 Zusammenfassung

Dieser Bericht gibt einen Überblick über die Bemühungen zur Governance von Digitalisierungsprozessen in Europa. Er versucht zu erläutern, wie solche Governance-Mechanismen derzeit funktionieren, und gibt Anregungen, wie solche Bemühungen in Zukunft effektiver funktionieren könnten. Er behandelt dabei vier Fallstudien, die die Herausforderungen und Mängel der Governance-Bemühungen zur Gestaltung von Digitalisierungsprozessen veranschaulichen. Die diskutierten EU-Beispielen sind das deutsche Netzwerkdurchsetzungsgesetz (NetzDG), der Automobil-(Software-)Emissionsskandal, das globale Multistakeholder-Internet-Governance-Modell und der erwartete Vorschlag der EU-Kommission zur Plattformregulierung.

Die Analyse dieser Fälle zeigt, dass Governance-Bemühungen, die auf digitale Prozesse ausgerichtet sind, in Europa zu scheitern scheinen. Bestehende Governance-Modelle stehen vor erheblichen Herausforderungen im Hinblick auf Effektivität, Transparenz, Rechenschaftspflicht und damit der Good Governance. Akteuren des öffentlichen Sektors auf subnationaler, nationaler, internationaler und supranationaler Ebene fehlt es häufig an der Fähigkeit oder der Bereitschaft, bestehende Gesetze umzusetzen und somit sicherzustellen, dass die Regulierungen effektiv durchgeführt werden. Es besteht ein offensichtliches Defizit im Hinblick auf das Verständnis der Funktionsweise von Technologie, ein ständiges Unterschätzen des Umfangs und des Ausmaßes des Problems und das scheinbar routinemäßige Bemühen, wichtige Fragen der Governance zu umschiffen, anstatt sie zu lösen. Dabei scheinen die Hindernisse keineswegs unlösbar.

Wenn aus diesem Bericht eine Reihe wichtiger Lehren gezogen werden können, bleibt die wohl wichtigste, dass die Staaten diese Herausforderung dringend annehmen müssen, wenn sie eine sinnvolle Rolle bei der Governance der digitalen Technologien spielen wollen. Die EU muss die Aufsicht über den Digitalisierungsprozess in eigene Hände nehmen. Gegenwärtig wird die überwiegende Mehrheit der Governancemaßnahmen, die auf digitale Umgebungen ausgerichtet sind, vom privaten Sektor durchgeführt, mit wenig staatlicher Intervention oder Aufsicht. Gleichzeitig legt dieser Bericht nahe, dass Nationalstaaten diese Regulierungsdynamik selbst gestalten können – jedoch nur dann, wenn sie die notwendigen Schritte unternehmen, um eine dezentrale und effektive Implementierungsstruktur zu organisieren.

Zu den Empfehlungen, die von den Autoren des Berichts diskutiert werden, gehören

- 1) Die Schaffung **neuer, unabhängiger Behörden auf EU-Ebene**, die die Aufgabe haben, die Vielfalt der von der Digitalisierung stark betroffenen Bereiche zu überwachen, wie z.B. die Online-Redaktion oder die Durchführung freier und fairer Wahlen. Dies würde die Schaffung sektoraler Regulierungsbehörden für digitale Dienste nach sich ziehen. Um wirksam zu sein, müssten solche Regulierungsbehörden ausreichend öffentlich finanziert werden und völlig unabhängig handeln können. Solche Aufsichtsbehörden müssten in der Lage sein, eine rasche und wirksame unparteiische öffentliche Entscheidungsfindung innerhalb ihres jeweiligen Regulierungsrahmens zu gewährleisten. Ebenso müssten sie mit den personellen und finanziellen Ressourcen und der Technologie ausgestattet sein, die zur Erfüllung ihrer Aufgaben erforderlich sind. Nur dann hätten die Regulierungsbehörden die Durchsetzungskapazität, die erforderlich ist, um eine effektive Governance der Digitalisierung effektiv zu gewährleisten.
- 2) Die **Rechtsetzung auf EU-Ebene** analog zur Datenschutzgrundverordnung (DSGVO), **zusammen mit einer entsprechenden Struktur für Regulierung**, in einer umfassenden Reihe von Bereichen, die von der Digitalisierung tiefgreifend beeinflusst werden. In jedem Bereich gäbe es idealerweise nationale Regulierer für jeden Mitgliedsstaat, einen europäischen Regulierer und ein Gremium auf europäischer Ebene, das alle relevanten Akteure in diesem Bereich zusammenbringt. Dies würde die Entwicklung unabhängiger Netzwerke der Regulierungsbehörden nach sich ziehen.

Die **Implementierung eines vernetzten und dezentralisierten Digitalisierungs-Governance-Modells für die Regulierung digitaler Dienste** im Binnenmarkt und insbesondere von Online-Plattformen. Im Gegensatz zu mindestens einer Option, die im Entwurf des Digital Services Act (DSA) der EU-Kommission enthalten ist, der die Schaffung einer neuen zentralen Behörde und eines zentralisierten Governance-Modells vorschlägt, schlägt dieser Bericht alternativ die Schaffung einer Digital Services Act Regulator (DSAR) vor. Der DSAR wäre keine zentrale Regulierungsbehörde für digitale Plattformen und Online-Dienste, sondern würde stattdessen als zentrale Einberufungsstruktur fungieren, die für die Koordinierung einer Reihe unabhängiger Regulierungsbehörden verantwortlich wäre. Dieses Gremium würde sich nicht auf einen bestimmten sektoralen Bereich konzentrieren, sondern würde die Befugnis erhalten, je nach zu erörterndem Thema verschiedene sektorale Regulierungsbehörden zusammenzubringen. Somit würde es Diskussionen zwischen unabhängigen Regulierungsnetzwerken mit dem Ziel koordinieren, die Zusammenarbeit und gemeinsame Entscheidungsfindung zu verschiedenen Themen innerhalb des geltenden Rechtsrahmens zu fördern. In einigen Fällen könnte der DSAR auch Probleme feststellen, die ein Tätigwerden der Gesetzgeber erfordern könnten. Er würde Probleme wie Online-Hassreden in sozialen Netzwerken, Transparenz in der politischen Online-Werbung, Desinformationskampagnen, Fairness im elektronischen Handel, Moderation von Inhalten, Transparenz in der Werbung und die Besteuerung von digitalen Gütern und Dienstleistungen behandeln.

4 Executive summary

This report provides an overview of efforts to govern digitalization processes in Europe. It seeks to understand how such governance mechanisms currently operate and provides suggestions as to how such efforts might work more effectively in future. It focuses on a set of four case studies that illustrate the challenges and flaws of governance efforts intended to shape digitalization processes. The EU examples discussed include the German Network Enforcement Act (NetzDG), the automobile (software) emissions scandal, the global multistakeholder internet governance model, and the EU Commission's pending platform-regulation proposal.

The analysis of these cases shows that governance efforts directed toward digital processes seem to be failing in Europe. Existing governance models are experiencing significant challenges with regard to effectiveness, transparency, accountability and good governance. Public-sector actors at sub-national, national, international and supranational levels demonstrate a frequent lack of capability or willingness to implement existing laws and ensure that regulations are carried out effectively. There is an evident deficiency with regard to understanding how technology works, a continual underestimation of the problem's scope and scale, and what appears to be a routine effort to evade rather than solve key governance issues. Therefore, the hindrances appear primarily institutional. They are by no means impossible to solve.

While a variety of important lessons can be learned from this report, the most important one is that states urgently need to accept this challenge if they want to play any meaningful role in the governance of digital technologies. The EU must take oversight of the digitalization process into its own hands. Currently, the vast majority of governance activities directed toward digital environments are conducted by the private sector, with little state intervention or oversight. At the same time, this report suggests that nation-states can themselves shape these regulatory dynamics, but only if they take the necessary steps to organize a distributed and effective implementation structure.

Recommendations discussed by the authors in the report include:

- 1) The creation of **new, independent public authorities at the EU level** tasked with overseeing the variety of areas highly impacted by digitalization, such as online speech or the conduct of free and fair elections. This would entail the creation of sectoral digital-services regulators. To be effective, such regulators would have to be adequately publicly funded and be able to act with complete independence. Such supervisory authorities would have to be able to ensure swift and effective impartial public decision-making within their relevant regulatory frameworks. They would similarly have to be furnished with the human and financial resources and the technology necessary to perform their duties. Only then would the regulators have the enforcement capability required to govern digitalization effectively.
- 2) The implementation at the **EU level of legislation** analogous to the General Data Protection Regulation (GDPR), **along with a corresponding regulatory structure**, across a comprehensive set of fields that are profoundly impacted by digitalization. In each area, there would ideally be national regulators for each member state, a European regulator and a European-level board that brings together all relevant actors within that area. This would entail the development of independent regulatory networks.
- 3) The implementation of a **networked and decentralized digitalization governance model for the regulation of digital services** in the Single Market, and of online platforms in particular. In contrast to at least one option contained within the EU Commission's draft Digital Services Act (DSA) proposal, which suggests the creation of a new central authority and a centralized governance model, this report alternatively proposes the creation of a Digital Services Act Regulator (DSAR). The DSAR would not be a central regulator for digital platforms and online services, but would instead act as a central convening structure, responsible for coordinating a set of independent regulatory authorities. This body would not be focused on any specific sectoral area but would have the power to bring together different sectoral regulators depending on the topic to be discussed. Hence, it would coordinate discussions

between independent regulatory networks with the aim of promoting collaboration and joint decision-making on various topics, within the applicable legal framework. In some cases, it might also identify issues requiring action by legislators. It would address problems such as online hate speech in social networks, transparency in online political advertising, disinformation campaigns, fairness in e-commerce, content moderation, advertising transparency, and the taxation of digital goods and services.

Effective governance requires institutions with the ability to regulate. The kind of oversight, implementation and enforcement needed to govern digitalization will be possible only if the EU is willing to promote GDPR-style legislation and regulatory structures with strong institutions across a broad set of relevant digital fields. This involves accepting that the challenge of governing digitalization calls for effective oversight requiring a robust institutional response. States certainly have the ability and resources to give such an answer. It remains to be seen whether they will actually be committed to do so.

5 Introduction

States around the world are trying to develop effective governance mechanisms for the ongoing process of digitalization. As some have described it, “software is eating the world” (Andreessen 2011), making this question more important by the day; nevertheless, it is today almost impossible to reconcile public discourses about digital technologies with the actual reality of these technologies. A body convened by the United Nations Secretary-General has debated new forms of governance in the digital age for more than a decade (Ermert 2019), and efforts to govern digitalization processes have often proved to be difficult, messy and complicated.

Before we go deeper into this debate, it is necessary to conceptualize the notions of digitalization and governance more precisely. Digitalization can be defined as a progressive use of digital technologies and digitalized data that changes how things are done, transforms the way in which citizens, government, civil society and companies engage and interact with one another, and restructures many domains of social life.¹ In the case of governance, we draw on the concept of “internet governance” as formulated by the Working Group on Internet Governance; here, this concept is defined as “the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programs that shape the evolution and use of the internet” (WGIG 2005) and of digitalization processes in general. While this definition is explicitly related to the internet, it can easily be applied more generally to digital technologies in general. This conceptualization provides us with a broad comprehension of governance mechanisms directed at digitalization processes, in which the institutions, actors and processes of governance can vary greatly while nevertheless suggesting the collective, policy-motivated shaping of a socio-technical system (van Eeten and Mueller 2012).

The abundance of public declarations of digital rights – which with the single exception of Brazil’s *Marco Civil da Internet* lack binding legal status – coupled with the myriad of European digital strategies that have not been systematically implemented (Volland 2019), tends to indicate a considerable implementation problem with regard to carrying out a targeted approach to digitalization. To date, it appears that the governance mechanisms proposed have been unable to achieve their desired policy outcomes. In some cases, the forms of digitalization governance discussed may even have been counterproductive.

In the following sections, this report will offer an overview of several digital governance mechanisms within and outside Europe. Grounded in the existing academic literature on technology governance (Brown and Marsden 2013; Crawford and Lumby 2013; Fountain 2007; Wagner 2016) as well as in wider theories of governance (Ackerman 2004; Barnett and Duvall 2005), the report seeks to improve our understanding of how the governance of digitalization processes currently functions, and how it might function in future. To achieve this goal, we will focus on a set of four examples chosen to illustrate the challenges of implementation and compliance in the digital age:

- 1) The German Network Enforcement Act (NetzDG)
- 2) The automobile (software) emissions scandal
- 3) The multistakeholder governance model and the Internet Governance Forum (IGF)
- 4) The pending European platform-regulation proposal and the Digital Services Act (DSA)

¹ By contrast, “digitization” is the process of converting information from analogue to digital format. For more information related to the concept of digitalization and digitization, please see: <https://medium.com/@colleenchapco/digitalization-digitalization-and-digital-transformation-whats-the-difference-eff1d002fbdf>. Accessed on 4 November 2019.

These examples will be used to provide an overview of the manner in which EU governments have sought to govern digitalization. We will use them to develop an analytical framework based on the following nine dimensions or core items of inquiry:

- 1) What actors are involved in shaping these processes?
- 2) What actors are not involved in shaping these processes, but should be?
- 3) How do these actors shape the process of digitalization? What mechanisms do they employ to ensure their voice is heard?
- 4) What role do sub-national, national, international and supranational public-sector actors play in governing digitalization?
- 5) Which actors are best positioned to respond to these governance challenges?
- 6) Are processes of self-regulation, co-regulation or full (state) regulation in play, and if so, how effective are these processes?
- 7) What is the role of the law in these processes? When is a focus on purely legal means helpful, and when are other means necessary?
- 8) What are the challenges for democratic governance raised by these implementation problems?
- 9) What are the strongest indicators of success or failure? How can this be measured effectively?

As this report will discuss, existing models of governance have experienced significant challenges with regard to effectiveness, transparency, accountability and good governance. This in turn has meant that as more and more of the world transitions to using digital technologies, the overall quality of governance is decreasing.

The broader question asked by the proposed framework is: **What would “better” governance of digitalization look like?** While it might be seen as an ambitious goal, this report will shed light on how better governance mechanisms might function. To do so, we will draw on the example of the EU Commission’s pending Digital Services Act (DSA) proposal, which raises the possibility of creating a new authority for the regulation of all digital services in the Single Market, and of online platforms in particular. This point of departure was chosen for two main reasons. First, the DSA discussions are still underway; this allows us to conceptualize an effective outcome before it reaches the implementation stage, and maybe even influence the ongoing debate. Second, rather than being focused on a specific area of the digital world (e.g., hate speech), this debate concerns state regulation of digitalization processes generally. Based on the DSA example, we will propose a digitalization governance model intended not to fix all flaws associated with the governance of digitization processes, but rather to serve as a contribution with regard to enriching the discussion on digital governance within the EU, and as a starting point in the visualization of better governance mechanisms.

It is no longer enough to argue about what the appropriate metaphor for a given digital domain might be, or whether an email should be considered a postcard, a letter or a telegram for regulatory purposes. The debate instead needs to shift toward an effort to understand how digitalization can be effectively governed to the benefit of societies as a whole. Unless better, more effective forms of governance are found, even well-intentioned political initiatives will fail. The digital world needs an effective leviathan that is able to govern democratically, not a headless chicken.

This report begins, in **Section 1**, by discussing four European cases related to the governance of digitalization processes (or the lack of it). This section is intended to illustrate the challenges of implementation, while providing

a current overview of selected digitalization governance efforts in Europe. In **Section 2**, these examples are discussed in a more cross-cutting manner. We ponder why many EU digital governance initiatives are failing, try to identify what these cases have in common, and seek to draw lessons from their flaws and successes. In **Section 3**, building on the EU Commission's pending DSA, we propose our own digitalization governance model, seeking to understand what elements might improve the efficacy of existing models. By way of conclusion, the report's **Section 4** issues an urgent call for states to create strong institutions with the ability to enforce digital-sector regulations if they want to play any meaningful role in governing digital technologies. Finally, the report suggests that it is perfectly possible for states to shape regulatory dynamics effectively if they take this issue seriously, willing to organize a distributed implementation structure.

6 Governance of digitalization: Failing forward? Four case studies

The following chapter presents four case studies from Europe that address attempts by public-sector actors and institutions to govern digitalization processes. These examples allow us to take a close look at the key challenges faced by states in regulating digitalization processes in different areas and at different levels. These case studies reveal an implementation gap that is in turn related to an institutional gap, indicating that as long as there are no institutions able to regulate effectively, governments are unlikely to play a meaningful role in the digitalization governance process.

6.1 The German Network Enforcement Act (NetzDG)

The German Network Enforcement Act (Netzwerkdurchsetzungsgesetz, NetzDG) is one of the most far-reaching efforts by a Western democracy to hold social-media platforms responsible for combatting hate speech and the incitation of violence (Tworek and Leerssen 2019). Along with the new EU Audiovisual Media Services Directive (AVMSD), it attempts to set standards for the regulation of online platforms.

Germany passed the NetzDG law in June 2017, with the first parts of the law coming into force on 1 October 2017. Social networks were given until the end of that year to prepare themselves for compliance. Hence, the law came into full force in January 2018. The law does not provide for any substantive changes with regard to the type of content being regulated. That is, most of what the NetzDG law does is refer to existing German legal norms on illegal content, although it does notably exclude some forms of illegal content such as copyright violations from the scope of the law.

At a procedural level, the NetzDG is much more ambitious. Its main objective is to reduce illegal content online by ensuring that platforms implement more effective ways of reporting and deleting potentially unlawful content, while also increasing the transparency and accountability associated with removal of content from the platforms (Wagner et al. 2020). Under the law, online platforms have to provide a mechanism for users to submit complaints about illegal content. Once they receive a complaint, platforms must investigate whether the content is illegal. They have a 24-hour deadline for the removal of “manifestly unlawful” content after receiving the complaint (otherwise disallowed content must be removed within seven days of the notification)²; failing this, they face fines of up to €50 million for the systemic failure to delete illegal content. It is as yet unclear precisely what systemic failure looks like. However, the German Federal Office of Justice has brought several cases that will probably lead to clarification in the courts.

NetzDG applies to for-profit media service providers with at least two million registered users that operate online platforms with user-generated content. Platforms that provide journalistic or editorial content do not fall under the scope of NetzDG, nor do instant messaging services like WhatsApp, Wire or Telegram (Wagner et al. 2020).

In point of fact, NetzDG has become a very controversial law. On the one hand, supporters see the legislation as a necessary response to the threat of online hatred and extremism. It is important to remember the context in which it was originally discussed, during Germany's 2017 election season; at this time, the fear that the right-wing Alternative for Germany (AfD) political party would win national parliamentary seats for the first time pushed legislators to act to prevent the propagation of hate speech on social media (Echikson and Knodt 2018; Wagner 2018). On the other hand, German and international critics view the law as creating legal mechanisms that are likely to undermine the freedom of expression online (Echikson and Knodt 2018; Kaesling 2018; Rebecca Zipursky 2019; Schulz 2018; Tworek and Leerssen 2019), thus promoting censorship, and as lacking transparency provisions

² An English version of the law is available at: <https://germanlawarchive.iuscomp.org/?p=1245>. Accessed on 4 November 2019.

around content-reporting mechanisms (Tworek and Leerssen 2019; Wagner et al. 2020). The law has even recently been the subject of parliamentary hearings in which potential revisions were discussed (Kettemann 2019).

In the context of this heavy criticism and the wider push for platform regulation in Europe,³ it is particularly important to evaluate the law's effectiveness and regulatory impact.

Most recently, the NetzDG has also been suggested as a mechanism for the reduction of the online hate speech deemed to be a key enabler of terrorist right-wing attacks such as the attacks on a Jewish synagogue in Halle on 9 October 2019. In response to these attacks, the German Interior Ministry has suggested that mechanisms could be introduced into NetzDG to promote the takedown of hate-driven content.⁴

But how does the NetzDG attempt to provide governance in the area of hate speech? Germany's Federal Office of Justice (Bundesamt für Justiz, BfJ), which reports directly to the Minister of Justice, plays a crucial role in the enforcement of the NetzDG. People can report violations of the law to the BfJ, which has made an online form available for the purpose, and companies must submit transparency reports to the BfJ. Section 2 of the NetzDG specifies that platforms that receive more than 100 notifications about unlawful content per year must publish a public transparency report in German every six months. These reports provide insight into the relevant statistics and information. Therefore, the BfJ is the main regulator with regard to enforcing the NetzDG.

Despite these changes, the NetzDG does little to change the existing dynamics of content regulation by online platforms. Thus, the previously existing self-regulatory regime for social-media platforms has been continued (Wagner 2018). Higher minimum standards for self-regulation by social-media platforms would go a long way toward responding to the many challenging questions about content regulation. Even with regard to illegal content under the NetzDG regime, the internet platforms are assigned the role of deleting content and blocking users, leaving the task of arbitrating such questions to them. While the fines provided for by the NetzDG increase pressure on social-media platforms to be more accountable, they essentially force the unaccountable private platforms to decide what is (and is not) illegal content. The short time frame in which the law expects companies to remove "manifestly illegal" content could easily lead them to err on the side of automated censorship in an effort to avoid steep fines and be more economically efficient (Wagner 2018).

This thus presents a kind of regulatory paradox. As legislators focus on regulating internet platforms, they find themselves in a downward spiral in which law-enforcement duties are legally transferred to private-sector entities, effectively amounting to a new kind of deregulation. "Perhaps vexed by the unique characteristics of social-media companies, legislators are dumping decision-making power and responsibility on the companies in a manner that is neither helpful nor effective in resolving the problem" (Wagner 2018). As such, they are privatizing decisions that should be made by independent authorities (Kaesling 2018). "More broadly, the question remains how and whether outside stakeholders can and should be involved in platform content moderation processes or their regulation" (Tworek and Leerssen 2019).

As we can see, there are many governance challenges regarding the implementation of the NetzDG. But what specific actors are involved, and what might "better" governance of these digitalization processes look like?

The primary actor involved in shaping NetzDG-related regulation processes is Germany's Federal Office of Justice (BfJ), a state actor. A key factor in understanding this case is the fact that BfJ is not an independent regulator. Rather, it is a subordinate public authority (*nachrangige Behörde*) of the Ministry of Justice. In the following discussion, we will address the challenges and risks associated with this regulatory design. In part, this model means the

³ Two representative EU examples would be the UK Government's "Online Harms White Paper" (UK Department for Digital, Culture, Media & Sport 2019) and the French proposal on making social-media platforms more accountable (French Government 2019).

⁴ Details of the proposal can be found here: <https://netzpolitik.org/2019/nach-halle-innenminister-praesentieren-wunsch-katalog-fuer-neue-ueberwachungsmassnahmen/>. Accessed on 24 October 2019.

Ministry of Justice itself and its minister are important actors to be considered. Finally, the large private social-media platforms such as Facebook and Twitter, which the law is struggling to regulate, play a central role.

Some actors that are not helping to shape the NetzDG process (though they most likely should be) are nonetheless important enough to require acknowledgement. Among them are comparatively small platforms such as Joyclub or change.org, which fall under the NetzDG's regulatory purview, but whose role was barely considered during the public debates about NetzDG. Civil society participation as a whole is lacking in the regulation process. The NetzDG law itself was drawn up in 2017 with little to no input from civil society organizations (Tworek and Leerssen 2019). Consideration of the input provided by German and international scholars on this topic would also be of great assistance in improving the governance of the NetzDG implementation process. This is particularly vital given that the law is based on user notifications, and there is no independent assessment of whether these notifications correspond to actual breaches of the law. As this process is driven by user flagging, it seems quite likely that certain types of content and certain types of users will be disproportionately affected. Indeed, the actual implementation of content-flagging systems can have considerable discriminatory consequences, similar to those already evident in the area of crowdsourced rating systems (Kocher and Hensel 2016).

Passage and implementation of the German law has been driven by national German electoral politics and a widely perceived need to respond to online hate speech (Wagner 2018). However, a variety of definitional and statistical problems in the law make it unclear whether the NetzDG will in fact be able to stop problematic speech. Most importantly, the measure covers only illegal content, and not legal content. Facebook is an emblematic case in this regard, since the BfJ fined the company in July 2019 (€2 million) for systematically failing to comply with the NetzDG's transparency requirements, and for the use of so-called dark patterns, or design techniques used to manipulate users. Facebook has appealed the ruling (Orth 2019). To better understand this BfJ decision, it is necessary to explain that Facebook's approach to NetzDG is different from that of most other platforms.

For most companies, user complaints can be made with reference either to the given social-media platform's community standards or to the NetzDG. However, Facebook has developed a completely separate reporting procedure for complaints made under the NetzDG (Echikson and Knodt 2018). The processes for reporting complaints under the NetzDG are very difficult to find on Facebook (even to the point of being hidden, you could say). For example, the reporting procedure is not launched at the point where the user is viewing the objectionable content (as in the case of Community Standards reports), but is instead initiated far away from the content itself, in the Facebook Help Center. This makes the process difficult to find, requiring users to expend extra effort. Facebook also attempts to redirect users to report the content as a Community Standards violation instead of under the terms of the NetzDG⁵ (Wagner et al. 2020). This mechanism, entailing an interface design aimed to divert, obstruct and redirect, can be considered a "dark pattern" that enhances information asymmetries and thereby limits users' abilities to access their rights (Wagner et al. 2020).

Another problematic angle of this story is Facebook's two-step approach to the reported content (Echikson and Knodt 2018; Wagner et al. 2020). The content is first reviewed with reference to the company's Community Standards. If these are violated, then the piece of content is removed globally. If the content in question violates German law but not Facebook's Community Standards, then the content is blocked only in Germany. Thus, analysis of the content under the company's own Community Standards takes precedence over ensuring that it complies with German law. This approach "has allowed Facebook to avoid having its broader content review process subject to NetzDG transparency reports" (Wagner et al. 2020).

In this context, the BfJ found that Facebook has underreported the number of complaints it had received about illegal content on its platform. In addition, the Justice Minister remarked that it is "exceedingly difficult for a user to complain to Facebook about posts that violate NetzDG" (Deutsche Welle 2019). To be fair to Facebook, the law's transparency requirements lack clarity. For instance, the lack of reporting requirements for the moderation of

⁵ See: <https://www.facebook.com/help/contact/2062389003993934>. Accessed on October 21, 2019.

content deemed legal opens the door to precisely the kind of category shifting between NetzDG and Community Standards that Facebook has engaged in. “What we now have in Germany is a law that demands respect and disproportionate attention from Facebook without actually forcing the company to reform its practices in the public interest” (Wagner 2018).

The current case is of far-reaching importance because the principles of “good regulation” (OECD 2005, 2011) regarding global platforms are being tested. On the one hand, the BfJ and the Ministry of Justice have taken an antagonistic approach to the regulation of these platforms. State regulators provide little or no help with regard to implementing the NetzDG, and the overall goal pursued by them seems to be to promote the primacy of German law over platforms’ community standards. On the other hand, platforms such as Facebook seem to be implementing the law poorly, which at least in Facebook’s case has led the BfJ to levy a €2 million fine (Orth 2019). Transparency requirements are being systematically ignored or misinterpreted because no one is entirely clear what they mean, and because it is convenient for the platforms (Wagner et al. 2020).

For transparency mechanisms to be effective, BfJ regulators must work in a collaborative manner and assist with the implementation of such practices, for instance by creating guidelines and a standard for transparency reports that enables statistics to be compared across platforms (currently, social-network platforms have each come up with their own individual reporting formulas; however, comparability across platforms is critical in order to gauge the effectiveness of NetzDG implementation). Furthermore, regulators should direct the platforms in their operations in a consultative manner; incentivize design practices that improve transparency, even to the point of offering grants to smaller companies to develop well-designed and easy-to-use user interfaces; and create a quality standard for complaint mechanisms enabling tech companies to be certified for user-friendly reporting processes. Such initiatives and others like them would support broader accountability regimes and promote access to human rights online (Echikson and Knodt 2018; Wagner et al. 2020).

Public-sector governance seems to be failing in the NetzDG case. Rather than deputizing social-media platforms to act as a privatized police force (by engaging in self-regulating content moderation), the law could instead shift the decision-making burden to public actors. At first glance, basing public-sector governance in a public-sector agency like the BfJ seems like a good idea with regard to regulating online platforms. However, the agency needs to be independent in order to ensure swift, effective and impartial public decision-making. “This is one important design flaw in NetzDG, as enforcement was not given to an independent regulator” (Wagner et al. 2020). The agency is currently subject to partisan political forces that affect its ability to make impartial decisions.

There is some danger in creating a central platform regulator. A better solution would be to create a wider range of individual regulators focusing on specific issues. Historically, problems related to digitalization have been dumped on data-protection authorities (DPAs), where they don’t belong, often because of the lack of preexisting public institutional structures able and willing to enforce regulations. The NetzDG is thus subject to an “implementation gap,” which is in turn related to an “institutional gap” in which “accountable public actors who should be ensuring the implementation of law in the digital sphere are lacking” (Wagner 2019).

Moreover, there are other areas in which the public sector could play a meaningful role in mitigating hate speech on social media. For instance, the Netherlands created a special centralized unit tasked with processing all takedown orders and requests for data from online service providers in an effort to ensure that they are legally sound (Wagner 2018). Other initiatives such as appeals bodies for takedown decisions and rapid-response judicial mechanisms to adjudicate complaints (Tworek and Leerssen 2019) would be beneficial in the interest of better regulation. However, even in these comparatively advanced approaches, there are challenges of transparency and accountability (Kaye 2019).

The NetzDG provides an interesting case study of state regulation, since self-regulation by private-sector organizations is unlikely to be successful in the absence of meaningful incentives underpinning such procedures (Access Now 2018). The approach in the German case is primarily legal and regulatory. If designed well, it could be highly effective. However, the challenges for democratic governance remain serious. The law could set in motion a

process initiating an open public debate incorporating all relevant stakeholders. Civil society needs to play a greater role in this process of regulation. For example, the creation of social-media councils that regularly convened representatives from the platforms, governments and civil society organizations to share information and debate possible new approaches would be highly beneficial (Tworek and Leerssen 2019). One major goal would be to determine minimum standards of self-regulation that conform with human rights and international standards for online platforms.

The design of the reporting mechanisms currently employed by the NetzDG do not lend themselves adequately to measuring the success or failure of the law's implementation. At minimum, they would also need to include all information related to the moderation of content deemed legal (as opposed to illegal) in Germany; a requirement that platforms standardize their categorization of content, thus enabling comparison; ideally, a provision requiring more frequent reports (monthly basis); regular third-party audits of representative samples of both legal/illegal and moderated/unmoderated content to establish whether the platform's definitions of legal and illegal content were deemed accurate; systematic third-party audits of all NetzDG-related procedures, similar to those currently conducted by DPAs on issues of data protection; and an independent BfJ – or alternatively a transfer of the BfJ's NetzDG-related tasks to a more independent public authority – that would be able to conduct such audits, with sufficient staffing to be able to do so. Finally, it would be crucial to create a comparative and open database enabling systematic comparison between platforms.

6.2 The automobile (software) emissions scandal

One could ask: Why should the “Dieselgate” scandal be considered as a digital governance issue in the first place? The digital dimension of Dieselgate lies in the fact that regulators and enforcement authorities underestimated the power of software, and as we will point out in the following discussion, were unable to check this particular part of the system in question. These are challenges of digital governance just as much as platform politics, but are seldom discussed in the same context. The challenges of digital governance cut across all areas of regulation, and are not just limited to areas such as data protection or privacy.

In 2013, the International Council on Clean Transportation (ICCT) in the United States initiated an examination of pollution from diesel cars. They had no idea it would lead to one of the biggest global automotive scandals to date, the Dieselgate scandal, as it became known. The Volkswagen emissions scandal began in September 2015, when the United States Environmental Protection Agency (EPA) issued a notice of violation of the U.S. Clean Air Act to the German automaker (Gardiner 2019). Volkswagen admitted that emissions software in four-cylinder diesel vehicles from model years 2009 – 2015 contained a “defeat device,” effectively a deliberate effort to evade the rules in the form of hidden software that could recognize whether a vehicle was being operated in a test laboratory or on the road (Chappell 2015). The defeat device had been installed in 11 million diesel-fueled vehicles worldwide.⁶ The software made those vehicles emit higher nitrogen-oxide levels when they were being driven in actual road use (as high as 40 times the legal limit) than during laboratory testing. Michael Horn, then the CEO of Volkswagen's U.S. business, confessed that the software had the express purpose of beating emissions tests, although he said he was not aware of this fact until the scandal came to light. “It was installed for this purpose,” he said (Chappell 2015).

As it turned out, Volkswagen wasn't the only one evading these laws; indeed, Fiat, Renault, Mercedes, Opel and Ford, among others, had also pursued analogous policies. Less flagrantly, but to similar effect, the vast majority of diesel cars were making a mockery of emissions rules in the United States, Europe and worldwide. “In the U.S., where only around 2% of cars are diesel, the rule-breaking had an impact. But the health consequences have been far more severe in Europe, where drivers had been encouraged for years to buy diesel cars – when the scandal

⁶ See Volkswagen's statement of 22 September 2015 at: http://www.volkswagenag.com/en/news/2015/9/Ad_hoc_US.html. Accessed on 22 October 2019.

broke, they accounted for more than half of all sales” (Gardiner 2019). A study revealed that Dieselgate helped cause 6,800 premature deaths in the EU in 2015 (Anenberg et al. 2017).

The disturbing light cast by the scandal did more than simply expose corporate transgressions. It also made visible the stunning failure by governments across Europe to enforce the law effectively. The negligence of so many governments with regard to enforcing the law represents the missing piece of this puzzle. “Member States contravened their legal obligation to monitor and enforce the ban on defeat devices set out in Article 5(2) of Regulation (EC) No. 715/2007. None of them found the defeat devices installed in the Volkswagen vehicles, in particular those Member States whose authorities type-approved those vehicles” (Gieseke and Gerbrandy 2017).

It even seems that some actors knew about the problem all along, as an official at Germany’s federal environment agency noted: “We publish this data. [...] In principle, this is nothing new” (Gardiner 2019). Even the EU Commission was aware of it. “Some years before the Dieselgate scandal erupted, the European Commission’s Joint Research Centre (JRC) signaled in 2011 that there was a significant discrepancy between car NOx [nitrogen oxide] emissions under laboratory conditions and those observed on the road” (ECA 2019). It is evident that there was negligence on the part of public-sector actors. “It [a European Parliament inquiry into Dieselgate] exposes a culture of looking the other way: the European Commission and member states turned a blind eye to industry-wide abuse of the system for emission regulation, and, in fact, even invited the car industry to shape the regulatory agenda and its enforcement. [...] Companies’ commercial interests were prioritized over public interests” (Hubner 2017).

The lack of good governance is astonishing in this case. There was no EU oversight of vehicle type approval, and little oversight by the national governments responsible for implementing the law. Carmakers that heavily influence political decision-making through this industry’s potent lobbying pressure were the most powerful actors, persuading politicians to support their cause (Hubner 2017). What might better governance look like in this context?

To grasp how it was possible for a scandal of this magnitude to occur, it is necessary to take a few steps back and review how the EU system of regulating car gas emissions worked (and, in great part, still works), along with its major flaws.

The European Commission sets the rules on how much pollution a car is allowed to produce. Framework Directive 2007/46/EC on type approval sets out the safety and environmental requirements that motor vehicles have to comply with before being placed on the EU market (European Parliament 2007). “Before a new model of vehicle can be sold in the EU, the manufacturer must submit it to the ‘type approval’ process. This process certifies that a vehicle prototype meets all EU safety, environmental and production requirements” (ECA 2019). The job of enforcing those rules falls to national governments (specifically, to the so-called type-approval authorities). Within this enforcement structure, it is possible to identify the core factors that enabled the Volkswagen (and other automakers) emission scandal to happen in the first place.

Let us take a closer look at Germany’s Federal Motor Transport Authority (Kraftfahrt-Bundesamt, KBA), which sits under the Federal Ministry of Transport and Digital Infrastructure, to see how enforcement of the law works in practical terms. One general observation would be that competition between various member states’ type-approval authorities makes governance more difficult. Under the current system, an automaker preparing to release a new model can choose which country certifies it; every EU nation must then honor this approval once granted. “Although common rules on type approval and test specifications are laid down, many witnesses highlighted the existence of a variety of interpretations in their application across the member states” (Gieseke and Gerbrandy 2017). Thus, a savvy carmaker can select a location in which it provides many jobs (and where officials are likely to be more pliant), or choose an authority based on its flexibility in interpreting the rules (Gardiner 2019; Gieseke and Gerbrandy 2017). This means that KBA did not have a monopoly with regard to its regulatory task, and it was easy for car companies that wanted to put new cars on the road to go elsewhere. This rule creates a competition-based incentive that significantly impairs good governance.

Another pertinent observation is that within the EU, there seems to be a lack of willingness to create institutions that both have the power to govern and the enforcement capability needed to give strength to pollution rules. National enforcement agencies are generally understaffed, poorly funded and lacking in technical expertise (Gardiner 2019; Gieseke and Gerbrandy 2017). Therefore, the European air-quality regulators do not have the clout or the resources needed to enforce the law properly. For instance, a significant part of KBA's budget comes from licensing fees gained from awarding cars their new car certificates. This practice urgently needs to be changed, as it creates incentives to be "nice" to carmakers. "The fact that type-approval authorities and technical services are usually financed in part by fees paid directly to them by the car manufacturers can give rise to conflicts of interest due to the need to maintain commercial relations" (Gieseke and Gerbrandy 2017).

Further problematic issues are related to the identity of those doing the testing and those who pay for it. The majority of member states designate technical services to test and inspect new car models (therefore, outsourcing such services). KBA, for instance, had no testing facilities of its own.⁷ "These [type-approval] authorities give accreditation to technical services (TSs), which are the bodies that actually test vehicles. The technical services may carry out tests at their own facilities (if they have them) or on car manufacturers' premises" (ECA 2019). Usually, it is the car manufacturer that chooses the technical service to be used, and tests are often carried out in the car manufacturers' certified laboratories under the supervision of the designated technical service. This is called "self-testing," and allows car manufacturers to test components in their own laboratories, giving them control over the testing conditions. "Approval would depend simply on the manufacturer providing the paperwork to the national authority" (Hubner 2017).

Additionally, when a manufacturer is preparing the launch of a new model on the EU market, the technical services that perform the official type-approval testing are paid directly by car manufacturers (Gieseke and Gerbrandy 2017; Hubner 2017). These financial and technical links between technical services and manufacturers can lead to conflicts of interest and compromise the independence of testing. Moreover, some technical services also do consultancy work for manufacturers on emission tests. Beyond that, the specifics of the tests – information on tested speed, acceleration, and so on – are publicly available (Gardiner 2019). Thus, a manufacturer can build its cars to produce little pollution under those particular conditions, while allowing them to emit much more the rest of the time.

National enforcement agencies' inability to enforce legal requirements remains a serious issue. According to Regulation (EC) No 715/2007 of the European Parliament and the Council on type approval of motor vehicles with respect to emissions, manufacturers are supposed to provide independent operators with unrestricted and standardized access to vehicle repair and maintenance information, including the software calibration identification number applicable to each relevant vehicle type (European Parliament 2007). Sadly, Volkswagen and most large car companies have refused to let third parties, including the KBA, look inside their software, claiming this to be an issue of market competitiveness. An EU Parliament report points out that type-approval authorities do not have access to electronic control unit (ECU) source code under the current system, although the same report questions the effectiveness of such access: "Experts have noted the consensus view that the preemptive checking and possible detection of a fraudulent emissions-system defeat device through unrestricted access to the vehicle's proprietary software is not a viable method, due to the extreme complexity of such software" (Gieseke and Gerbrandy 2017).

Additionally, data on car type-approval testing in the EU, such as the results of emission tests, are fragmented (ECA 2019). Neither the EU Commission nor the member states have a comprehensive view of such information. In general, existing data are kept at the member-state level. "[T]he lack of data transparency and public availability make the situation harder for interested parties to follow the issue and to contribute to the monitoring of vehicle emissions" (ECA 2019).

⁷ Hearing featuring Kraftfahrt Bundesamt (KBA) President Ekhard Zinke in 2016: http://www.europarl.europa.eu/cmsdata/110300/CRE_EMIS_%2011%2010%202016_EN.pdf. Accessed on 22 October 2019.

Lastly, another important issue in understanding the failure to implement this legislation properly is the absence of external testing options enabling outside parties to analyze the software. Car owners were not able to look inside their cars and understand what the various components were doing; nor could they have an expert look inside these components. If they had the legal right to do so, this scandal would likely have been uncovered much earlier.

The main state actors engaged in this digitalization process, the national governments as represented by their type-approval authorities, were fundamentally unable to shape the process. They lacked the necessary human and financial resources, as well as access to the relevant technology necessary to perform in-house testing, instead having to rely on tests performed in the car manufacturers' certified laboratories under the supervision of technical services. In many cases related to self-driving vehicles, KBA still lacks access to all relevant software. In addition, the competitive structure at the EU level enabled an unpleasant form of "race to the bottom" governance, leaving EU and national regulators alike in a position in which they were unable to govern effectively. "The Dieselgate scandal has lifted the lid on a culture of industry self-regulation and light-touch rulemaking that is facilitated by European decision-makers, including member states" (Hubner 2017).

In January 2016, following the Dieselgate exposures, the Commission proposed a fundamental reform of the vehicle type-approval system, replacing Directive 2007/46/EC in an attempt to tackle the perceived shortcomings of the current EU system (EU Commission 2018). The new rules were approved by the European Parliament in April 2018 (Regulation (EU) 2018/858), and will become mandatory beginning in September 2020. From this point forward, European regulators will require cars to be tested on the road, and not just in the lab. But it seems clear that the flaws in European nations' enforcement extend beyond the particulars of any given testing method. The problem lies in the system itself; moreover, with regard to important aspects of this problem, the EU Commission's effort to improve the system has failed to make significant strides forward.

To be sure, progress has been made in some areas. In the future, technical services will be regularly and independently audited, manufacturers will be obliged to disclose data necessary for third-party testing, type-approval authorities and technical services will be granted access to vehicle software, member states will ensure that there is enough national funding available in each country to test a minimum number of vehicles (the so-called market surveillance checks), member states will be subject to greater scrutiny, and the EU will expand its oversight of the vehicle type-approval process (specifically, the EU Commission will be able to suspend and withdraw type approvals, and impose penalties on manufacturers) (ECA 2019; EU Commission 2018; ICCT 2018). According to the EU Commission press release:

They will have to review regularly the functioning of their market surveillance activities and make the results publicly available. National type-approval authorities will be subject to peer evaluations if they assess their own technical services instead of the national accreditation bodies, but they will always be subject to an independent assessment carried out directly by the Commission to ensure that the relevant rules are implemented and enforced rigorously across the EU (EU Commission 2018).

However, the official type-approval testing will still be paid for directly by car manufacturers, producing conflicts of interest and compromising the independence of the testing process. The Commission proposed a modification of the remuneration system, but this element was not approved (EU Commission 2018). "To avoid any potential conflict of interest and reinforce the independence of testing, a type-approval fee structure was considered to cover the costs of all type-approval tests and inspections carried out by the technical services. However, the European Parliament and the EU member states rejected this part of the EC's proposal" (ICCT 2018). Additionally, another aspect originally proposed by the EU Commission (and supported by NGOs and consumer associations) – the creation of an EU-wide type-approval authority – was not included in the final regulation (ICCT 2018).

It will still be necessary to reinforce the independence and quality of testing and strengthen the overall type-approval system through greater European oversight. "In addition, thorough implementation of any of the adopted measures in practice will also require that member states provide sufficient financial resources for their type-approval bodies" (ICCT 2018). Or, in other words, as the EU Parliament report recognizes, "The presence of adequate in-house

independent, qualified human resources and the availability of in-house state-of-the-art testing facilities are essential to ensuring effective monitoring of the emission standards" (Gieseke and Gerbrandy 2017).

Ultimately, proper governance would be possible only with an independent and properly publicly funded KBA whose decisions were not subject to influence by a government minister. Moreover, consumer protection groups need better access to all relevant information in order to be able to play a watchdog role, and to be able to lobby effectively in consumers' favor. Car owners should be able to look inside and understand their own cars, and should be able to secure the services of external testing providers. Success should not require the emergence of intermittent scandals around such an important issue. Rather, it should be a question of systematic and regular reporting in this area.

6.3 The internet multistakeholder governance model

As mentioned previously, we utilise the concept of "internet governance" as formulated by the Working Group on Internet Governance. As such, we understand it as "the development and application by governments, the private sector and civil society, in their respective roles, of shared principles, norms, rules, decision-making procedures and programs that shape the evolution and use of the internet" (WGIG 2005). To understand the multistakeholder model of global internet governance and the role of the Internet Governance Forum (IGF) within it, it is first necessary to take a few steps back and recall the history of the Internet Corporation for Assigned Names and Numbers (ICANN).

ICANN was created in 1998, "emerg[ing] from a struggle over control of the internet's domain name system (DNS)" (Mueller and Wagner 2014). At that time, according to the authors, the internet was becoming a public mass medium globally, and there was no clear, legitimate policymaking body with authority over the central coordinating functions of the internet's underlying routing and address system. In response, the United States initiated a process to address the institutional problem of DNS governance: "The idea was to use a private-sector non-profit dominated by the technical community to govern DNS by private contract rather than public regulation or treaties" (Mueller and Wagner 2014). In this case, a private-sector governance authority was deemed helpful in order to circumvent the fear that national governments would impose their own domestic laws and regulations on the global arena of the internet. However, from its beginning, ICANN struggled to achieve collective legitimacy over this new institutional framework. One of the problematic factors was justifying the contention that ICANN was global while it was in fact headquartered in California and functioned under the terms of a Memorandum of Understanding drafted by the U.S. Commerce Department. This factor kept ICANN under the shadow of U.S. hegemony, preventing other states or institutions from becoming overly influential (Wagner 2016b).

In an effort to win other countries' support for the ICANN model, the institution included stakeholders from different countries and various types of organizations in its operations, a concept that afterward became known as the multistakeholder governance model. The concept of multistakeholder internet governance suggests that civil society groups, the business community, governments, and technical and academic experts all make decisions together, rather than these decisions being made by states alone (Cammaerts and Padovani 2006; Chapelle 2008; Hintz 2007; Wagner 2016b). In the sense that it claims to involve all participants in the decision-making process by sharing decision-making power with non-state actors, the multistakeholder governance model can be considered an innovative governance concept, although it raises serious issues of legitimacy, representativeness and accountability (Bendiek and Wagner 2012; Mueller 2010; Mueller and Wagner 2014; Wagner 2016b).

Private-sector actors play a key role in this DNS governance structure, as they are responsible for the technical standards that create the global basis for communication on the internet. Although the early institutional design of ICANN intentionally excluded governments from decision-making positions, a Governmental Advisory Committee (GAC) was created at the group's Berlin meeting in 1999, with the intention of allowing states to influence the decision-making process (Mueller and Wagner 2014). However, "despite this claim of inclusion of a broad group of

stakeholders from many different countries, the early ICANN quite evidently reflected the preferences of both the U.S. government and their allies” (Wagner 2016b).

Over time, a number of different actors have been critical of this multistakeholder global internet technical governance model. At the forefront of the international organizations seeking a role in internet governance has been the International Telecommunications Union (ITU), the United Nations-affiliated body that has helped lead advocacy for an intergovernmental approach to internet policy (Mueller and Wagner 2014; Wagner 2016b). The ITU helped organize the World Summit on the Information Society (WSIS) process, a United Nations-sponsored set of discussions aimed initially at ensuring that the developing world was able to participate in the internet’s benefits. It was at the second major set of WSIS meetings in Tunisia in 2005 that the first major, open challenges to ICANN’s role by developing countries and Europe emerged (Mueller 2010), led by non-OECD countries concerned about U.S. control over the internet. This conflict had several immediate outcomes.

With regard to ICANN specifically, the Tunis Agenda, a consensus statement that emerged from the WSIS Tunisia summit, ended up empowering the group’s GAC. Though many issues regarding U.S. control of ICANN were left unsolved, this gave a significantly greater role to the governmental representatives within the ostensibly private-sector organization (Mueller and Wagner 2014; Wagner 2016b). Separately, the 2005 WSIS participants also agreed on the creation of an annual multistakeholder forum at which policy-related topics could be discussed on a non-binding basis. This ultimately became the Internet Governance Forum (IGF), that should be governed in a multistakeholder manner like the ICANN. At this point, the discussion of DNS governance expanded to the discussion of Internet governance as a whole, going beyond the technical aspects and entering the high policy level.

While an apparent step forward in bringing international voices into the decision-making mix, the IGF was never endowed with instrumental power of any kind, making it difficult for this body to initiate or push through improvements in global internet governance. “Its purpose is to anchor the existing multistakeholder model of internet governance, at an international level, rather than to distribute instrumental power” (Wagner 2016b). Nevertheless, it has acted over the years as the nexus for a transnational network of actors (Flyverbom 2011), serving as an effective community-building and socialization mechanism (Franklin 2013; Mueller 2010; Mueller and Wagner 2014). For its part, the ITU continued to support the annual WSIS forum as its chosen policy framework, effectively in competition with the IGF. However, like the IGF, the WSIS draws its legitimacy from the Tunis Agenda (Wagner 2016b).

From the internet governance perspective, the primary function of the IGF seems to be a symbolic one. “While neither accountable nor effective in changing governance practices, these [internet] institutions nonetheless serve to justify ongoing internet governance practices at an international level” (Wagner 2016b). Secondly, another important function has been “institutional lock-in” (Wagner 2016b), preventing other institutions from governing the internet or contesting existing governance practices. Finally, a third component is related to “the strong split between legitimizing public front-stage process and the backstage power-allocation process. While the front stage is steeped in public symbolism and ritual, the latter is where power over governance practices resides” (Wagner 2016b). There is scarcely a tangible link between the front stage debates and the actual internet governance practices of the individual actors. “The IGF with its rituals, forums and symbolic interaction often seems more theatrical than oriented on producing a specific policy outcome” (Mueller and Wagner 2014).

After 2005, there was a proliferation of national and regional internet governance forums at various levels and on multiple topics, such as the Freedom Online Coalition and the London Cyberspace process. To a certain degree, all of these efforts were contesting the authority of the IGF as the central global forum for internet governance. “Crucially, neither key developing nations nor many international organizations within the UN system were happy with the IGF occupying a central role in the development of international internet policy. Even if the IGF had no [real] power, they feared that it might erode their own relevance and legitimacy within the international system”

(Mueller and Wagner 2014). The result has been to push the IGF to the fringes of the core debates on internet policy.

The authority of the IGF to “govern” the internet was strongly contested by the ITU in 2012 during the World Conference on International Telecommunications (WCIT). The WCIT showed that the legitimacy of the current global model of internet governance was being questioned globally, and demonstrated that there was no international consensus on the appropriateness of this model. However, while the actual usage of the Internet has shifted, ICANN became increasingly irrelevant as an institution (Wagner, 2016b). Likewise, the lock-in function of the IGF and ICANN decreased considerably. “Multistakeholder institutions like the IGF and ICANN are increasingly becoming empty shells to justify a model with little international buy-in” (Wagner 2016b). As a result, the multistakeholder model of internet governance has devolved into a theatrical performance with little influence on actual practices of internet governance (van Eeten and Mueller 2012; Hintz 2007; Mueller 2010; Wagner 2016b) despite claims to the contrary (Cammaerts and Padovani 2006; Chapelle 2008; Flyverbom 2011). So how to get from these empty institutional shells to actual governance in practice?

There are at least two clearly opposed groups of actors shaping, or fighting to shape, the process of internet governance. The recurring attempts over several decades to develop legitimacy and principles for internet governance have revealed ongoing and as yet unresolved tensions; in large part, these stem from the fact that the internet’s technical governance remains largely dominated by Western multistakeholder institutions (ICANN, IGF, Internet Engineering Task Force (IETF), World Wide Web Consortium (W3C), etc.), even as nation-states (including a large number of developing countries, as well as important emerging economies such as China, Russia, Brazil and South Africa) and UN-oriented intergovernmental institutions have demanded a more significant role. This latter group has long been trying to strengthen the ITU’s role in internet governance.

The United States’ continuing ability to shape this process is a primary reason why the multistakeholder internet governance model has persisted. “At the most fundamental level, this model of internet governance continues to persist because of sufficient U.S. hegemony over internet infrastructure” (Wagner 2016b). Even though the United States’ capacity to wield unilateral control over the technical functioning of the internet has declined over the last two decades, it still represents the dominant force holding together the existing internet governance regime.

The existing multistakeholder internet governance model continues to produce a great deal of meetings. However, a number of scholars argue that there is little in the way of real governance being produced (van Eeten and Mueller 2012), and that the symbolic theatre of ICANN and IGF has little to do with actual governance practices (Wagner 2016b). These institutions are captured by powerful interests (Milan and Oever 2017), undermining the ostensible benefits of the multistakeholder internet governance model. Stakeholders who claim to have a stake within the model do not necessarily have actual power. Companies’ dominant role in these institutions needs to be reduced, and participation by civil society and academic institutions should be promoted (Voelsen 2019).

To summarize, the multistakeholder approach as manifested in these organizations is of limited efficacy. There has been a lack of effective institutionalization, in the sense that there has been no real agreement within the IGF, ICANN or WSIS on how to alter or institutionalize any governance practices or rules for the internet. These institutions have become, at worst, a distraction from actual governance and, at best, a weak instrument of governance.

For many years, debates on internet governance itself have focused on a very narrow range of international institutions such as ICANN, IGF and WSIS, which have been of questionable importance (due to their limited actual authority over internet operations). This has constrained the scope of the overall debate (van Eeten and Mueller 2012; Wagner 2016b). The field of internet governance is highly interdisciplinary, and a plausible explanation for this myopic focus or blind spot might be that “studying a centralized institution is a lot more convenient than having to identify and study a wealth of disjointed, messy and globally distributed processes that together produce governance” (van Eeten and Mueller 2012:729). Additionally, given the increasing importance of the internet to our societies, there is a growing need for accountability, and a concomitant desire to be able to hold centralized and

formalized institutions accountable. However, focusing exclusively on these institutions would lead to an overestimation of the presence and influence of states in internet governance (van Eeten and Mueller 2012).

“In most areas, governance of the internet takes place under very different conditions: low formalization, heterogeneous organizational forms and technological architectures, large numbers of actors, and massively distributed authority and decision-making power. Whatever governance emerges under these conditions, it will be a lot less amenable to state intervention” (van Eeten and Mueller 2012:730). Non-hierarchical forms of cooperation are the dominant form of governance, supplemented by the factually narrow authority claim of ICANN (Voelsen 2019). Currently, “the internet is governed by numerous informal power relations and agreements – predominantly between private actors. Insofar as public actors are involved, their ability to influence internet governance, at both a national and an international level, has been extraordinarily limited” (Wagner 2016b). However, the absence of formal hierarchies does not mean that there are no power relations. In particular, companies are trying to enforce their interests in bodies such as the IETF (Voelsen 2019).

The multistakeholder model embodied in the organizations cited above is basically a networked model, but one without implementing institutions or co-decision-making. Structurally the multistakeholder model is weak, and lacking regulatory enforcement power. Additionally, as implemented, the model carries issues of legitimacy. Who gets to represent which constituency, and based on what type of legitimation process? For example, business stakeholders are not democratically elected, unlike state actors. Yet those present are able to wield direct influence over the debate within the multistakeholder model. For this reason, to deal with the internet governance a better approach might be to start with a networked approach at the government level, and then integrate non-state actors through classical co-decision-making procedures that are easily institutionalized, such as request-for-comment processes, public consultations and public hearings. Essentially, the multistakeholder model is not able to produce the strong institutions needed for actual internet governance. Rather, a networked model of regulation, and specifically one in which public actors would take responsibility and lead a process of democratic governance, seems to be the best approach. In this regard, questions such as the appropriate limits of involvement for non-state actors — particularly powerful companies — still need to be addressed.

6.4 The pending European platform regulation proposal and the Digital Services Act

The EU Commission is currently considering the creation of a new authority for the regulation of online services. This option was one of several contained in an internal European Commission note on the issue that was leaked in July 2019. The proposed Digital Services Act (DSA) or Digital Service Code would affect “all digital services in the Single Market, in particular online platforms [...] such as social media, search engines or collaborative economy services, as well as [...] online advertising services” (EU Commission 2019). In the note, the Commission presented current problems posed by the regulation of digital services, and proposed a number of measures that would update the regulatory framework for digital services, including a revision of the existing E-Commerce Directive (ECD). The paper was written by officials in the Commission’s Directorate-General for Communications Networks, Content and Technology (DG Connect). It was part of a discussion process moving toward the development of a more detailed proposal to be brought forward by the new Commission, which took office in Brussels in December 2019.

The new Act is intended to create European rules addressing issues such as online hate speech within social networks, transparency in online political advertising, disinformation campaigns and e-commerce fairness. According to the note, these issues are complicated by multiple sets of divergent rules across the various EU member states, increasingly uncoordinated national or even regional regulation, and an absence of standards for information exchange between local and national authorities. The note’s authors argue that this fragmented regulatory environment makes it difficult for newcomers to compete and survive. “Even if consumer rules, data protection rules [...] and contract rules have converged across the EU, in today’s regulatory environment, only the big platform companies can grow and survive,” it states. This situation is considered to be a “major strategic

weakness for the EU in the digital economy,” and a competitive disadvantage in comparison to non-EU services. The authors cite the example of Estonian start-up Taxify (now known as Bolt), which has had difficulties in scaling up across the EU and in growing to compete effectively with U.S.-based rivals such as Uber.

This “regulatory gap” is recognized by the EU Commission within the note when stating “there is currently no dedicated “platform regulator” in the EU, which could exercise effective oversight and enforcement, e.g. in areas such as content moderation or advertising transparency.” In their analysis, the authors observe that there is currently no regulatory authority available to provide quick and reliable EU-wide guidance on emerging and unforeseen issues, although the note recognizes that sectoral digital services regulators already exist in the areas of data protection, audiovisual media, competition, electronic communication services and consumer protection.

The note also posits a need for the EU to address the current self-regulation model for online platforms. These platforms are making “public-interest decisions that should be taken by independent public authorities, [...] without adequate and necessary oversight, even in areas where fundamental rights are at stake,” the authors write.

The document outlines a complete overhaul of the rules governing the net. “The nature of such an instrument should support its overall aim to update, clarify and harmonize rules for digital services in the Single Market, which could potentially mean that the directive should evolve into a regulation.” The main structural components would build on the existing blocks of the ECD. A revised set of rules would “complement” recently adopted sector-specific rules such as the Audiovisual Media Services Directive (AVMSD), the New Deal for Consumers, and other regulations on the issues of copyright, terrorist content, explosives precursors and child sexual abuse.

This ambitious EU Commission initiative faces a number of challenges. The potential confusion created by housing multiple institutional roles within a single institutional platform regulator is only one of these. Although the leaked note is just an initial step in a longer process of debate, its text produces major concerns. For example, it lacks specificity with regard to how platforms would be compelled or convinced to comply with the new rules. The relationship between a possible new platform regulator and existing regulatory bodies (national tax offices, existing platform regulators like the German BfJ, etc.) would require considerable thought and institutional engineering. Ensuring proper coordination across instruments (AVMSD, copyright, terrorist content) will be another challenge.

The details of all these issues remain vague in the leaked note. However, the text does list different options for monitoring compliance with the rules. With regard to regulatory oversight in particular, it says that the new Digital Services Act (DSA) could create a new “central regulator,” but that there could also be a “decentralized system” or “an extension of powers of existing regulatory authorities.” The degree of independence that any such new regulatory agency would have, along with the possible roles and powers associated with the regulatory structure, still need to be clarified. Outstanding issues include reporting requirements, powers to require additional information, complaint handling policies, the power to impose fines or other corrective actions, and the approval of codes of conduct, just to name a few. Thus, the governance challenge ahead is enormous. What might better governance in this area look like?

As relevant actors in this regulation process, we have the institutions of the European Union (the European Commission, Council and Parliament) trying to prove they can govern large platforms. Civil society is playing a role insofar as it is pushing for stronger regulation, especially (but not only) regarding social media, its influence on elections, and its role in spreading hate speech and misinformation. Global platforms, in turn, are resisting collaboration to the extent that they have failed to develop automated content moderation systems with the desired degree of transparency and accountability, for example, or transparency with regard to algorithmic recommendation systems of public relevance, such as newsfeeds.

Individuals within the European Union – that is, those who are most deeply affected by the misbehavior of online platforms – are the key actors who are not directly involved in shaping this process, but should be. European citizens are confused and suffering from the lack of regulation and governance of online services, often to the extent of seeing their fundamental rights and freedoms abridged. Among those experiencing the most harm are ethnic, racial and religious minorities; people who face discrimination based on sexual orientation or disabilities;

marginalized communities (particularly those who do not speak European languages); underprivileged citizens; and women.

The EU regulatory impetus fits into the broader Von der Leyen agenda, marked by the new Commission president's aim to demonstrate the ability to govern Europe. As a result, efforts to regulate may overshoot what is possible or practicable. The EU is likely to employ all its force to prove it can regulate global platforms, seeking to become a model worldwide. On the other hand, large platforms will certainly use their power to try to influence the decision-making process to soften any proposed regulations (favoring a "soft-touch" approach) or to recast the proposals in their favor. At this stage, it remains unclear how civil society and individual citizens will seek to ensure their voice is heard, what mechanisms they will use, or indeed whether they will be heard at all.

Based on the information currently available, the Commission appears to be positioning the DSA as a case in which state regulation properly takes over from an earlier process of self-regulation. However, the self-regulation regime was not developed voluntarily, but under conditions in which there was a lack of satisfactory regulation at the EU level. In this sense, it is a classic case of the EU moving slowly while the individual member states have speed ahead. It appears that this proposed law is being positioned to supplant self-regulatory approaches, both in the sense of superseding national-level approaches, and by reducing online platforms' freedom to regulate themselves. However, Germany has already passed its NetzDG law governing some of these issues, and France is developing its own digital platform laws (French Government 2019). This creates a problematic situation in which EU will have to carefully manage the interrelation between these national laws and the new EU platform law. Moreover, a number of EU-driven self-regulatory efforts regarding hate speech, illegal content, online crime prevention and the prevention of material relating to child sexual abuse have all been implemented prior to this new EU regulatory push, creating another significant challenge with regard to ensuring proper coordination across instruments.

The leaked EU Commission note was criticized by various sources. European Digital Rights (EDRi), an association of civil and human rights organizations from across Europe, remarked that "from a fundamental rights perspective, the internal note contains a few good proposals, a number of bad ones, and one pretty ugly" (EDRi 2019).

As an example of a "good" proposal, the group notes that "the Commission maintains that no online platform should be forced to actively monitor all user-uploaded content." As the Commission states, this prohibition of general monitoring obligations is a "foundational cornerstone" of internet regulation. According to EDRi, this type of policy "has allowed the internet to become a place for everyone to enjoy the freedom of expression and communicate globally without having to go through online gatekeepers." But EDRi's analysis points out that the note is somewhat weak on the issue of automated filtering technologies (Wagner 2014), since the leaked text merely recommends that transparency and accountability should be "considered" when algorithmic filters are used. "It's no secret though that filtering algorithms make too many mistakes – they do not understand context, political activism or satire" (EDRi 2019). Creating more transparency around the algorithmic decisions made by large online platforms would undoubtedly be welcome. However, this is not enough to prevent fundamental rights violations and discrimination.

EDRi is more critical of the note's proposal that the Commission analyze policy options for both illegal and potentially "harmful" but legal content. EDRi indicates that harmful content lacks a legal definition, and "it is unclear which content should be considered 'harmful' and who makes that call." The Commission authors acknowledge that when platform companies are pushed to take measures against potentially illegal and harmful content, their effort to balance interests often pushes them to overblock legal speech and monitor people's communications in order to evade legal liability. However, the note also suggests that harmful content can be best dealt with through the use of voluntary codes of conduct, which shifts the regulatory burden to the platform companies and decreases legal certainty for users (EDRi 2019).

According to EDRi, the "ugly" proposal relates to modifying platform operators' traditional exemption from liability for user-uploaded content. Currently, under the EU E-Commerce Directive, platform operators are not liable for illegal content uploaded by users as long as they can claim to have been unaware of the content, and remove it as soon as they are requested to do so. In other words, under Article 14 of the ECD, providers are liable for illegal

content uploaded by users, such as copyright infringements, only if they were previously aware of this content and do not remove it after being requested to do so. “Services such as Facebook, Flickr or YouTube would probably be unthinkable otherwise” (Rudl and Fanta 2019). Yet this could change under the new DSA. The note proposes to distinguish between providers, and in some cases to prescribe “proactive measures” in order to avoid direct liability (that is, creating a duty to proactively monitor and search for certain types of content in order to prevent its upload). “Such measures could include upload filters, as required by the recently adopted EU copyright reform” (Rudl and Fanta 2019). For EDRI, the question that remains unanswered here is: “How can the Commission save the current liability exemption for the sake of internet users and their fundamental rights, all the while making it compatible with the hair-raising provisions of the Copyright Directive?” The Commission needs to engage in a transparent discussion of how the liability exemption can be salvaged, how the negative impacts of the sectoral laws can be dealt with, and how to avoid collateral damage. It must also be careful to preserve the liability exemption for the sake of freedom of speech online.

As noted above, the prospective governance challenges are substantial in this case, since there are numerous actors involved at different levels (national, international, supranational and sub-national) and in diverse sectoral areas, along with multiple sets of sectoral laws to be considered and coordinated. In the interest of achieving satisfactory governance, a decentralized system would seem to be more appropriate. An independent set of European-level regulators (dealing with a wide set of relevant areas such as political campaigning and elections, online speech, urban mobility, data protection, audiovisual media, electronic communication services, consumer protection, among others), acting in concert with a set of national regulators, would seem to be beneficial. Democratic governance will be achieved only if the EU manages to create a regulatory model in which both civil society and online platforms (both large and small) have space to be heard, and can have their concerns and input considered.

Measuring the success or failure of this potential new EU authority for the regulation of online services will be difficult. Relevant indicators may be similar to those being used for Germany’s NetzDG law in some areas, but may well be distinct in other areas. These decisions will depend on the final extent and scope of the platform regulation, which has yet to be defined.

7 Why are many digital governance initiatives failing?

The notions of steering and collaboration seem to be common to most definitions of governance, in general, and of technology governance in particular (Ackerman 2004; Barnett and Duvall 2005; van Eeten and Mueller 2012; WGIG 2005). However, the case studies examined in this report illustrate that these notions can be extremely hard to implement in practice. What can we learn from these cases? Why are many digital governance initiatives failing?

The German Network Enforcement law (NetzDG) and the automobile (software) emissions scandal are examples of a failure to implement digitalization governance properly through institutions. In both cases, regulatory institutions exist: Germany's Federal Office of Justice (Bundesamt für Justiz, BfJ) in the case of the NetzDG, and Germany's Federal Motor Transport Authority (Kraftfahrt-Bundesamt, KBA) in the case of the automobile scandal. However, neither entity is sufficiently independent nor receives funding sufficient to carry out its assigned tasks. Therefore, they lack both the power to govern and the needed enforcement capability.

The case of the multistakeholder global internet governance model deals with a proposal that at first seemed innovative and promising, but ultimately failed to produce actual governance. While a networked model of regulation seems the correct approach, the multistakeholder model was unsuccessful in achieving its goal; that is, it was not able to effectively include representative actors from different countries and sectors (civil society, the business community, governments, and technical and academic experts) and there is no shared decision-making power among participants. The major institutions that use this model (ICANN) and the annual multistakeholder forum (the IGF, which was never endowed with real policymaking power) are focused on “performing” governance. As such, they are preventing other institutions from emerging to contest existing governance practices and question these organizations’ monopoly within this area.

This model is doomed to fail, as a number of different actors and forums have questioned the authority of the IGF as the central global forum for internet governance. In short, the model raises serious issues of legitimacy, representativeness and accountability. Multistakeholderism is limited in its approach, and is a weak instrument for governance, as it has proved unable to produce the strong institutions or facilitate the co-decision-making practices needed for actual internet governance. For the implementation of a truly democratic governance model, the role of powerful companies must be reduced. Crucially, public-sector actors must take primary responsibility for safeguarding governance and human rights, and therefore lead the process.

Finally, in the case of the Digital Services Act (DSA), if the EU Commission opts to create a new central platform regulator tasked with multiple responsibilities rather than a “decentralized system,” it faces the serious risk of attempting to build a perfect institution for the regulation of digital platforms and online services, but failing in the process of implementation. There are many dangers in seeking to create a central platform regulator, starting with the potential for confusion when multiple institutional roles are combined within a single regulatory institution platform, and extending to the potential for conflicts of interest across the various areas of digitalization.

Digital governance seems to be failing in Europe. Public-sector actors at different levels (national, international, supranational and subnational) demonstrate a frequent lack of capability or willingness to implement laws and regulate effectively. This challenge also appears related to the general unwillingness to create new, truly independent regulators. It is much easier to shift responsibility for all digital issues to DPAs or other existing government agencies than to acknowledge the true scope and scale of the problem. There is an evident deficiency in understanding how technology works; policymakers consistently seem to underestimate the scope of the problem, seeking to impose temporary fixes rather than durable solutions. Therefore, it appears that the stumbling-blocks are primarily institutional.

The recent case of the Irish Data Protection Commission's (DPC) budget is an example of the general lack of willingness among public-sector actors to create independent and strong regulators. In the 2020 budgeting process, the DPC received less than a third of the additional funding it sought (Taylor 2019). Its requests reflected the

significant increase in the agency's workload due to implementation of the General Data Protection Regulation (GDPR). Under the reduced budget outlay, the DPC will have to reassess its planned expenditure for next year and cope with an overload of work while trying to maintain efficient operations.

It is urgent that the EU takes the digitalization process into its own hands. To this end, it is necessary to create new, genuinely independent public authorities. In the context of this report, independent means that the regulatory body is adequately funded with its own budget, is a part of the public sector, and is able to act with complete independence, which in turns implies a decision-making power independent of any direct or indirect external influence. In this regard, the supervisory authorities must be able to ensure swift and effective impartial public decision-making within their relevant regulatory framework. In other words, any such body must have institutional independence, rather than being subject to partisan political influence that affects its ability to make impartial decisions. It should have access to the human and financial resources needed to perform its assigned tasks, as well as to any relevant necessary technology. Only then will the regulators have the enforcement capability required to govern.

8 What might “better” governance of digitalization look like?

Efforts to govern digitalization processes are often difficult, messy and defined by globally distributed processes. This is a particularly complex task because it involves actors from many different sectors (public, private, civil society, academia, etc.), among other reasons. Frequently, these actors do not share the same level of knowledge regarding technology, and do not have equal access to technological resources. Public-sector actors are commonly at a disadvantage because governments generally invest more slowly in technology than do private companies, for various reasons. In addition, the political dynamics of states progress at a different pace than do business negotiations, defined as they are by the formation of alliances, the making of laws, budget approval debates, multistakeholder discussions, and routine considerations of a wide variety of interests. These and other factors can make discussions and approvals slow and complicated.

Against this backdrop, this section of the report focuses on how “better” governance of digitalization processes in Europe might function. In it, we will develop a proposal for a digitalization governance model that draws on the example of the EU Commission’s Digital Services Act (DSA), which – though it remains in the discussion stage, and has not yet been officially proposed – has raised the prospect of a new authority tasked with regulation of all digital services in the Single Market, and of online platforms in particular. The Commission’s current discussions offer a useful opportunity to reflect on how digitalization governance efforts could be rendered more effective. This occasion is particularly valuable both because the relevant policymaking process remains underway (potentially leaving room for further input), and because the debate encompasses state regulation of digitalization processes overall, rather than being focused on a specific area of the digital world, such as online speech.

Therefore, we consider here how the EU DSA might be conceptualized in light of the governance flaws analyzed in the case studies presented in this report. In other words, if we had the opportunity to develop a template for the DSA, what might it look like?

The governance challenges that will face any EU DSA are substantial, as its implementation will engage numerous actors at different levels (national, international, supranational and subnational) and in diverse sectoral areas, and will require the consideration and coordination of a large set of sectoral laws. One option would be the creation of a central digital regulator, similar to the approach proposed by the UK House of Lords. However, this option risks entangling many of the separate but overlapping policy issues associated with platform regulation, creating unnecessary institutional tensions; for instance, there will be numerous issues in which the interests of freedom of expression and privacy collide, or where platform governance and human rights do not align well with internal inner-agency debates (Wagner 2011). In other words, digital platforms and the field of digital services more generally are characterized by the intersection of a large number of different areas with conflicting interests. This would produce a significant number of conflicts of interests that a central regulator could not, and in some cases should not, resolve internally. Particularly given the importance of national and regional regulators in implementing regulation in a wide variety of areas, these regulators should be involved at as early a stage as possible

The European Union’s data-protection regulatory regime offers useful lessons in this regard. Here, there are independent national regulators, in some cases also subnational regulators, and the European-level regulator, the European Data Protection Supervisor (EDPS). The EDPS is an independent supervisory authority responsible for ensuring that EU institutions and bodies comply with data-protection law when processing personal data.⁸ All these regulators also work together in the context of a European-level body. Previously, this advisory body was called the Article 29 Working Party (A29WP). On 25 May 2018, under the provisions of the EU GDPR, this was replaced by the European Data Protection Board (EDPB).

⁸ For more see: https://edps.europa.eu/about-edps_en

The EDPB is an independent European body composed mainly of representatives of the national data-protection authorities and the EDPS, and is focused on promoting cooperation.⁹ The main function of the Board is to ensure the consistent application of the GDPR. To that end, the EDPB can perform tasks such as: issue guidance for controllers and processors on aspects of GDPR; determine disputes between national supervisory authorities; support businesses ability to comply; advise the Commission on any issue related to the protection of personal data in the European Union, among other tasks. The European Commission and – with regard to GDPR-related matters – the European Free Trade Association (EFTA) Surveillance Authority have the right to participate in the activities and meetings of the Board, but without voting rights.

What if we had structures similar to that of the data-protection regime, as described above, for other areas highly impacted by digitalization, such as online speech or the efforts to secure free and fair elections in the digital age? Under such a model, each relevant area would feature national regulators within each member state, a European-level regulator and a European board that brought together all relevant actors in that area. Additionally, we propose the creation of a Digital Services Act Regulator (DSAR) that would not be focused on any specific area, but would be able to bring together different sets of sectoral regulators depending on the topic to be discussed.

And what would be the role of this DSAR? This new authority would be responsible for the meta-regulation of online services in general, coordinating the numerous regulators within the specific digital sectors, without itself engaging in traditional rule-making or enforcement activities. It would do this by bringing together the various independent authorities and boards (from the national, regional, subnational and European level) within the various sectoral areas, facilitating collaboration and joint decisions on various topics within the given legal framework.

For example, if the topic under discussion was online disinformation, then the relevant authorities in areas such as digital campaigns and elections, audiovisual media, online speech, and data protection and privacy, among others, would meet under the *coordination* of the DSAR. These entities would engage in joint actions and make joint decisions designed to counter disinformation online, within the legal framework given. The DSAR would also have the role of involving civil society and private-sector actors relevant to the topic under discussion; however, these actors would not be given decision-making power, participating instead in a more collaborative and advisory manner. As a regulatory authority body, the DSAR would not serve a legislative function, but would have the authority to raise issues to legislators if deemed necessary. It should also be involved in the regulatory process, possibly as a board advising the institutions of the European Union (e.g., the European Commission, Council and Parliament).

In other words, the DSAR would be primarily responsible for coordinating a set of independent, sector-specific regulatory authorities. The overall aim would be to update, clarify, harmonize and create rules for digital services in the Single Market, particularly for online platforms such as social media, search engines, collaborative-economy services and online advertising services. The DSAR would not be a central digital-platform and online-services regulator, but a *central convener* of the European entities performing these regulatory tasks. It would coordinate discussions between different independent regulatory networks with the goal of creating European rules on issues such as online hate speech in social networks, transparency in online political advertising, disinformation campaigns, fairness in e-commerce, content moderation, advertising transparency, and the taxation of digital goods and services.

One institutional component supporting this joint decision-making process could be a DSA Expert Pool (DSA-EP), composed of several hundred experts in different subjects. The various national and subnational regulators would be given the ability to call upon this pool with essentially no added cost to the individual national-level regulators. In other words, the DSAR would provide access to the DSA-EP on a cost-free basis as a means of expanding regulators' in-house capacities. This would mean that the independent regulators could maintain a core internal staff while also drawing from this pool of additional expertise as needed.¹⁰ This would reduce the need to maintain

⁹ For more see: https://edpb.europa.eu/about-edpb/about-edpb_en

¹⁰ Thanks to Christoph Geisler (SWP) for the helpful inspiration on this topic.

large, full-time teams of specialist computer scientists or lawyers at the national or subnational levels, while still giving regulators access to a pool of such expertise for short periods of time.

The range of sectoral issues that should be considered here is broad, and should be defined by the strength of the various sectors' relationships to digital services; for example, EU regulators would be conceivable in the areas of data protection, audiovisual media, electronic communication services, consumer protection, political campaigning and elections, online speech, financial services, the environment and urban mobility, among others. The DSAR would build on existing structures like the EDPB. Additionally, it would help create new structures where they do not yet exist, as in the areas of national election authorities or online-speech authorities, who would need to be involved in European debates about disinformation. The creation of independent regulatory networks for each of these sectoral areas would help to make the regulation process more efficient. It would require a new set of regulators, modelled on DPAs but functioning in other areas.

In contrast to the multistakeholder governance model discussed above, or to existing EU agency models such as the European Union Agency for Cybersecurity (ENISA), the governance model we are proposing here would go beyond advisory boards and the provision of voluntary consultation and advice; instead, it would embody an approach similar to that of the collaboration between the EDPB and the EDPS. However, expanding upon these bodies' current relationship of coordination, we also propose additional co-decision-making mechanisms that would vary depending on which areas were involved. Importantly, we argue that decisions should be made using qualified majorities among participating regulators, thus ensuring that no individual national regulator would be able to block the process entirely.

In summary, the digital governance model proposed here would create a decentralized system. This system would be composed of a set of independent regulators (at the European, regional, national and subnational levels) that address a comprehensive set of sectoral areas in which digitalization has a significant impact (such as data protection, political campaigning and elections, and urban mobility, among many others). The DSAR would serve as a central convening structure that would interface extensively on a daily basis with these independent regulators. Whenever it proved necessary to discuss a specific transversal digital topic (such as disinformation or content moderation in online platforms), it would bring together and coordinate the relevant actors in that matter, providing them with a pool of experts that would support joint decision-making in a process of cross-entity discussion. The DSAR would also be responsible for including other relevant actors, such as civil society groups, the business community, and technical and academic experts. This would create a forum where these actors would be guaranteed to be heard, and where their concerns and input would be considered.

The diagram below (Figure 1) offers a visualization of the digitalization governance model that is being discussed here.

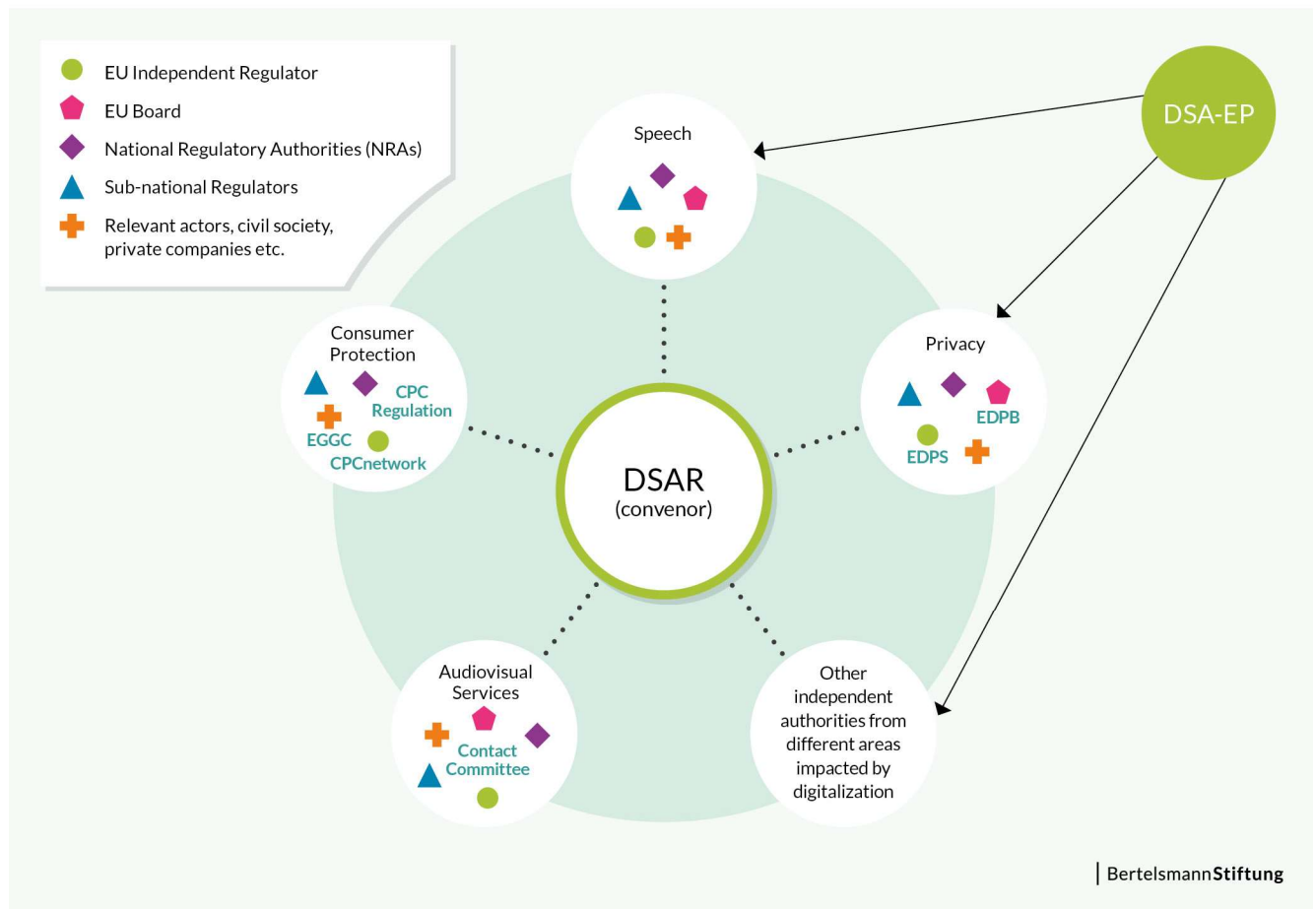


Figure 1 - Decentralized, networked digitalization governance model for a EU Digital Services Act Regulator (DSAR)

To further clarify this proposal, Figure 2 depicts how this model would work in the case of a discussion on the issue of disinformation. Here, the DSAR would convene independent regulators in relevant areas such as political campaigns and elections, data protection and privacy, audiovisual media, and online speech. Initially, the DSAR would coordinate a process of discussion, information exchange, study and research on the topic, at the level of debate and collaboration. In a second phase, the DSAR would coordinate a shift to a decision-making level, where joint decisions could be made. Therefore, depending on the issue and the stage of the discussion process, the degree of involvement by different regulators would vary (e.g., as the process shifted from the collaboration/coordination phase to the decision-making phase). In the diagram, these different layers are identified through the use of differently shaded sections.

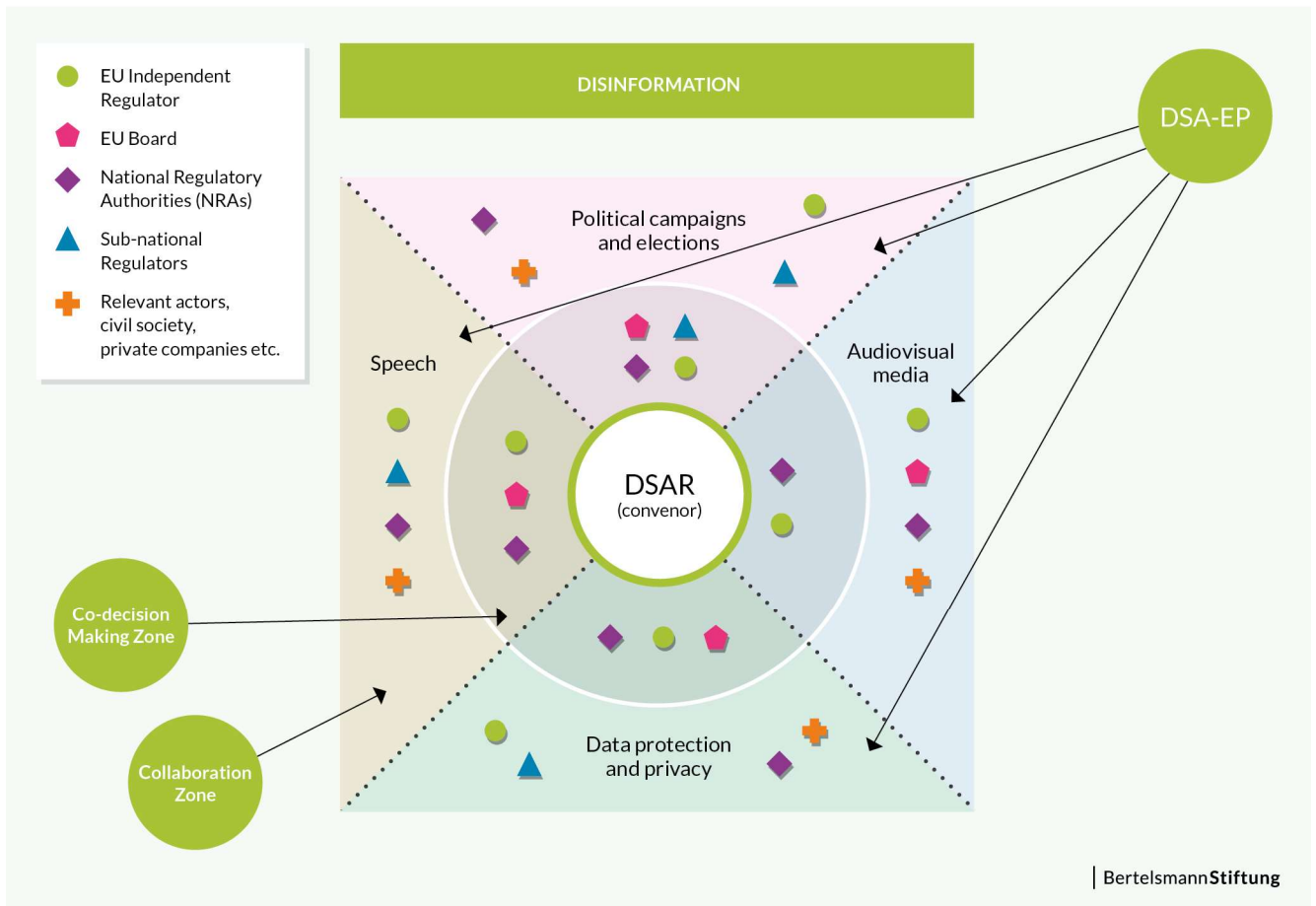


Figure 2 - Decentralized, networked digitalization governance model for a EU Digital Service Act Regulator (DSAR), when discussing disinformation

The newly created agencies (as well as the already existing ones) would need individualized metrics of success that could be externally measured. Thus, an external third party should perform systematic audits of the platform and digital-services regulatory enforcement system. These agencies would also need to be rigorously accountable to EU-level oversight bodies, to national-level authorities and to citizens. Finally, the expense of instituting this system will be considerable. The EU should avoid seeking to obtain the necessary financial resources from companies or through membership fees. Rather, these expenses should be paid out of the general taxation budget in order to ensure independence in decision-making.

Retaining multiple independent regulators in different areas, while tasking the DSAR to serve as a joint decision-making coordinator for specific topics (such as disinformation or hate speech), would ideally help mitigate the conflict of interests that would emerge if these functions were placed within a single institution. Were a unitary structure containing these independent agencies to be created, it would force these disputes to take place inside the institution, making it difficult to mediate conflicts of interest. It would be easier to find a balance between data-protection and freedom-of-expression interests, for instance, if the entities concerned with these issues were independent instead of fighting for prominence within the bureaucratic structure of a single institution. In other words, conflicts between different institutions are preferable to those taking place within an institution. As previously noted, the EU's existing regulatory agencies and the new independent bodies that the DSAR will help to create must go beyond simply interfacing at the networking and coordination levels, engaging also in joint decision-making. Within the DSAR itself, competences would have to be clearly defined. The entity should have the ability to prioritize issues, and must possess mechanisms allowing it to arrive at a definitive decision on what course of action to take within a meaningful space of time.

The EU Commission is considering the creation of a new authority for the regulation of online services using a model entailing a single large European regulator. However, if this new unitary body fails to consider all existing actors, it will do a bad job even as it seeks to promote “good” regulation. We propose instead a model that does not rely on a central body with traditional regulatory powers. Rather, our alternative would be based on an independent set of European regulators each focused on individual online-services sectors, and would promote a cooperative relationship between these EU regulators (both new and previously existing) under the coordination of the DSAR. While this model would entail a certain amount of institutional and procedural complexity, we believe it would ameliorate destructive and distracting tensions inevitable in a unitary agency tasked with overseeing so many different areas.

9 Conclusion

What lessons can be learned from this report? First and foremost, we can see that states are not always unable to govern processes of digitalization but are very frequently reluctant to do so. There is a considerable implementation gap between what states claim to be doing to govern technology and what they are actually doing in practice. In many cases, it seems reasonable to ask whether any of these governance structures, such as the IGF, were ever designed to provide any meaningful kind of digital governance at all.

While the creation of structures promoting the interests of industry actors may be considered a reasonable strategy when an industry is still in its infancy and does not yet have significant influence on society at large, it would be foolish at this point to suggest that the internet industry has not yet matured. If anything, high-tech companies are rapidly shifting the definition of what constitutes a “technology” product or service, in the process assimilating many existing industries at extraordinary speed. Given these clear shifts, the suggestion that large, established technology companies should be treated with a “light-touch” regulatory approach in order to enable innovation and growth is patently absurd.

Of course, this does not imply that any and all regulation is acceptable, but rather that there is an urgent need for states to act if they want to play any meaningful role in governing digital technologies. Currently, the vast majority of governance activities directed at digital spaces are conducted by the private sector, with little state intervention. It is no longer enough for states to claim proudly that they have finally “brought Google to the table,” or are currently negotiating with Facebook on yet another nonbinding self-regulatory policy. States should be governing these companies.

To govern effectively in the way we are describing, oversight institutions must have a true ability to regulate. Institutions co-funded by industry or which feature industry officials sitting on their decision-making boards cannot serve this function, despite their popularity within technology governance circles. Effective governance also demands a genuine willingness within the public sector to create regulatory structures with real force, which push the technology sector to actually follow the law. Upon examination, many of the measures cited in the case studies above seem to be little more than smokescreens, intended to demonstrate that states are acting rather than being actual instruments of governance. While this limited efficacy may in large part be due to successful private-sector lobbying, this does not change the basic fact that regulators must be able to regulate if states want to remain legitimate actors in the area of digital governance.

This report suggests that it is perfectly possible for nation-states to shape regulatory dynamics more effectively – if they take the issue seriously, and are willing to organize a distributed implementation structure. The EU GDPR is perhaps the best current example of a serious effort to impose a rigorous governance structure on a broad, cross-sectoral technological field of activity. The GDPR too could go further and suffers from its own implementation gap. Nevertheless, it goes considerably farther in terms of practical governance than does most other regulation in this area.

Only if the EU is willing to implement GDPR-style legislation, along with a corresponding regulatory structure, across a comprehensive set of regulatory fields, will the kind of regulatory action and enforcement needed to govern digitalization become possible. Policymakers must accept that shaping the future course of digitalization will require effective governance, which in turn will depend upon a robust institutional response. States certainly have the ability and resources to accomplish this. It remains to be seen whether they will actually be willing to do it.

10 References

- Access Now. 2018. Mapping Regulatory Proposals for Artificial Intelligence in Europe. Brussels: Access Now.
- Ackerman, John. 2004. "Co-Governance for Accountability: Beyond 'Exit' and 'Voice'." *World Development* 32(3):447.
- Andreessen, Marc. 2011. "Why Software Is Eating the World." *Wall Street Journal*, August 20.
- Anenberg, Susan C., Joshua Miller, Ray Minjares, Li Du, Daven K. Henze, Forrest Lacey, Christopher S. Malley, Lisa Emberson, Vicente Franco, Zbigniew Klimont, and Chris Heyes. 2017. "Impacts and Mitigation of Excess Diesel-Related NOx Emissions in 11 Major Vehicle Markets." *Nature* 545:467.
- Barnett, Michael and Raymond Duvall. 2005. "Power in International Politics." *International Organization* 59(01).
- Bendiek, Annegret and Ben Wagner. 2012. "Die Verfassung des Internets." *IP - Die Zeitschrift* Jahrgang 2.
- Bolt. 2019. "All Bolt Rides in Europe Are Now 100% Carbon-Neutral." Retrieved 9 October 2019 (<https://blog.bolt.eu/2019/09/all-bolt-rides-in-europe-are-now-carbon-neutral/>).
- Brown, Ian and Christopher T. Marsden. 2013. *Regulating Code: Good Governance and Better Regulation in the Information Age (Information Revolution and Global Politics)*. The MIT Press.
- Cammaerts, Bart and Claudia Padovani. 2006. "Theoretical Reflections on Multi Stakeholderism in Global Policy Processes: The WSIS as a Learning Space." Cairo, Egypt.
- Chapelle, Bertrand de La. 2008. "Multistakeholder Governance – Emergence and Transformational Potential of a New Political Paradigm." Pp. 335–48 in *Managing Complexity: Insights, Concepts, Applications*, edited by D. Helbing. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Chappell, Bill. 2015. "'It Was Installed for This Purpose,' VW's U.S. CEO Tells Congress About Defeat Device." NPR.Org, Retrieved 8 October 2019 (<https://www.npr.org/sections/thetwo-way/2015/10/08/446861855/volkswagen-u-s-ceo-faces-questions-on-capitol-hill>).
- Crawford, Kate and Catharine Lumby. 2013. "Networks of Governance: Users, Platforms, and the Challenges of Networked Media Regulation." *International Journal of Technology Policy and Law* 1(3):270–282.
- Deutsche Welle. 2019. "Germany Fines Facebook for Underreporting Hate Speech Complaints." DW.COM, July 2. Retrieved 8 October 2019 (<https://www.dw.com/en/germany-fines-facebook-for-underreporting-hate-speech-complaints/a-49447820>).
- Diaz, A. 2008. "Through the Google Goggles: Sociopolitical Bias in Search Engine Design." Pp. 11–34 in *Web Search*. Vol. 14, edited by A. Spink and M. Zimmer. Berlin, Heidelberg: Springer Berlin Heidelberg.
- ECA. 2019. "The EU's Response to the 'Dieselgate' Scandal." Briefing Paper. European Court of Auditors (ECA).
- Echikson, William and Olivia Knodt. 2018. "Germany's NetzDG: A Key Test for Combatting Online Hate." SSRN Scholarly Paper. ID 3300636. Rochester, NY: CEPS Policy Insight.
- EDRi. 2019. "More Responsibility to Online Platforms – but at What Cost?" EDRi. Retrieved 4 October 2019 (<https://edri.org/more-responsibility-to-online-platforms-but-at-what-cost/>).
- van Eeten, Michel JG and Milton Mueller. 2012. "Where Is the Governance in Internet Governance?" *New Media &*

Society 15(5):720–36.

- Ermert, Monika. 2019. "Missing Link: Die UN und das Internet – vage Visionen und mangelnde Teilhabe." heise online. Retrieved 21 October 2019 (<https://www.heise.de/newsticker/meldung/Missing-Link-Die-UN-und-das-Internet-vage-Visionen-und-mangelnde-Teilhabe-4475893.html>).
- EU Commission. 2018. "Press Release - New EU Type-Approval Rules for Safer and Cleaner Cars: Frequently Asked Questions." Retrieved 10 October 2019 (https://europa.eu/rapid/press-release_MEMO-18-3652_en.htm).
- EU Commission. 2019. Note on Regulation of Online Platforms.
- European Parliament. 2007. Regulation (EC) No 715/2007 of the European Parliament and of the Council.
- Flyverbom, Mikkel. 2011. *The Power of Networks: Organizing the Global Politics of the Internet*. Cheltenham, UK ; Northampton, MA: Edward Elgar.
- Fountain, Jane E. 2007. "Challenges to Organizational Change: Multi-Level Integrated Information Structures (MIIS)." *Governance and Information Technology: From Electronic Government to Information Government* 1–29.
- Franklin, Marianne. 2013. *Digital Dilemmas: Power, Resistance, and the Internet*. Oxford; New York: Oxford University Press.
- French Government. 2019. "Creating a French Framework to Make Social Media Platforms More Accountable: Acting in France with a European Vision."
- Gardiner, Beth. 2019. "Dirty Lies: How the Car Industry Hid the Truth about Diesel Emissions." *The Guardian*, March 22. Retrieved 10 October 2019 (<https://www.theguardian.com/environment/2019/mar/22/dirty-lies-how-the-car-industry-hid-the-truth-about-diesel-emissions>)
- Gieseke, Jens and Gerben-Jan Gerbrandy. 2017. "REPORT on the Inquiry into Emission Measurements in the Automotive Sector. Committee of Inquiry into Emission Measurements in the Automotive Sector." A8-0049/2017. European Parliament.
- Golledge, Reginald G. 1993. "Chapter 2 Geographical Perspectives on Spatial Cognition." Pp. 16–46 in *Advances in Psychology*. Vol. 96. Elsevier.
- Hintz, Arne. 2007. "Deconstructing Multi-Stakeholderism: The Discourses and Realities of Global Governance at the World Summit on the Information Society (WSIS)."
- van Hoboken, Joris 2012. "Search Engine Freedom: On the Implications of the Right to Freedom of Expression for the Legal Governance of Web Search Engines." PhD Thesis, University of Amsterdam.
- Hubner, Fabian. 2017. "Driving Into Disaster: How the EU's Better Regulation Agenda Fuelled Dieselgate." Corporate Europe Observatory, Friends of the Earth Europe.
- ICCT. 2018. "Changes to the Motor Vehicle Type-Approval System in the European Union." International Council on Clean Transportation.
- Kaesling, Katharina. 2018. "Privatising Law Enforcement in Social Networks: A Comparative Model Analysis" edited by K. Henrard. *Erasmus Law Review* 11(3):151–64.
- Kaye, David. 2019. "Speech Police: The Global Struggle to Govern the Internet." New York: Columbia Global

Reports 17:52.

- Kettemann, Matthias C. 2019. "Stellungnahme Als Sachverstaendiger Fuer Die Oeffentliche Anhoerung Zum Netzwerkdurchsetzungsgesetz Auf Einladung des Ausschusses Fuer Recht und Verbraucherschutz des Deutschen Bundestags," May 15, 2019. Retrieved 10 November 2019 (https://www.hans-bredow-institut.de/uploads/media/default/cms/media/up8o1iq_NetzDG-Stellungnahme-Kettemann190515.pdf)
- Kocher, Eva and Isabell Hensel. 2016. "Herausforderungen Des Arbeitsrechts Durch Digitale Plattformen – Ein Neuer Koordinationsmodus von Erwerbsarbeit." *Neue Zeitschrift Für Arbeitsrecht* (16/2016):984–89.
- Lewandowski, Dirk. 2015. "Suchmaschinen Und Ihre Rolle Als Vermittler von Informationen." Pp. 269–79 in *Suchmaschinen verstehen*. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Milan, Stefania and Niels ten Oever. 2017. "Coding and Encoding Rights in Internet Infrastructure." *Internet Policy Review* 6(1).
- Montello, Daniel R. 1997. "The Perception and Cognition of Environmental Distance: Direct Sources of Information." Pp. 297–311 in *Spatial Information Theory A Theoretical Basis for GIS*. Vol. 1329, edited by S. C. Hirtle and A. U. Frank. Berlin, Heidelberg: Springer Berlin Heidelberg.
- Mueller, Milton. 2010. *Networks and States the Global Politics of Internet Governance*. Cambridge, Mass.: MIT Press.
- Mueller, Milton and Ben Wagner. 2014. "Finding a Formula for Brazil: Representation and Legitimacy in Internet Governance." *Internet Policy Observatory* 31.
- OECD. 2005. "Guiding Principles for Regulatory Quality and Performance." Paris, France: Organisation for Economic Co-operation and Development.
- OECD, ed. 2011. "Regulatory Policy and Governance: Supporting Economic Growth and Serving the Public Interest." Paris, France: Organisation for Economic Co-operation and Development.
- Orth, Wim. 2019. "BfJ: Zwei Millionen Euro Strafe für Facebook." *Behörden Spiegel*. Retrieved 8 November 2019 (www.behoerden-spiegel.de/2019/07/04/bfj-zwei-millionen-euro-strafe-fuer-facebook/).
- Panko, Riley. 2018. "The Popularity of Google Maps: Trends in Navigation Apps in 2018." *The Manifest*. Retrieved 8 October 2019 (<http://themanifest.com/app-development/popularity-google-maps-trends-navigation-apps-2018>).
- Quattrone, Giovanni, Licia Capra, and Pasquale De Meo. 2015. "There's No Such Thing as the Perfect Map: Quantifying Bias in Spatial Crowd-Sourcing Datasets." Pp. 1021–32 in *Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing – CSCW '15*. Vancouver, BC, Canada: ACM Press.
- Rebecca Zipursky. 2019. "Nuts About NETZ: The Network Enforcement Act and Freedom of Expression." *Fordham International Law Journal* 42(4):1325.
- Rudl, Tomas and Alexander Fanta. 2019. "Leaked document: EU Commission mulls new law to regulate online platforms." *netzpolitik.org*. Retrieved 4 October 2019 (<https://netzpolitik.org/2019/leaked-document-eu-commission-mulls-new-law-to-regulate-online-platforms/>).
- Saurwein, Florian, Natascha Just, and Michael Latzer. 2017. "Algorithmische Selektion im Internet: Risiken und Governance automatisierter Auswahlprozesse." *kommunikation @ gesellschaft* 18:1–22.

- Schulz, Wolfgang. 2018. "Regulating Intermediaries to Protect Privacy Online – The Case of the German NetzDG." SSRN Scholarly Paper. ID 3216572. Rochester, NY: Social Science Research Network.
- Statista. 2019. "Attitudes towards Mobility in Germany 2019." Statista. Retrieved 9 October 2019 (www.statista.com/forecasts/998683/attitudes-towards-mobility-in-germany).
- Taylor, Charlie. 2019. "Data Protection Commission 'Disappointed' at Budget Allocation." *The Irish Times*. Retrieved 11 October 2019 (www.irishtimes.com/business/technology/data-protection-commission-disappointed-at-budget-allocation-1.4045248).
- Tufekci, Zeynep. 2015. "Algorithms in Our Midst: Information, Power and Choice When Software Is Everywhere." Pp. 1918–1918 in Proceedings of the 18th ACM Conference on Computer Supported Cooperative Work & Social Computing – CSCW '15. Vancouver, BC, Canada: ACM Press.
- Tworek, Heidi and Paddy Leerssen. 2019. "An Analysis of Germany's NetzDG Law." Working paper. Transatlantic High-Level Working Group on Content Moderation Online and Freedom of Expression.
- Voelsen, Daniel. 2019. "Risse im Fundament des Internets." Berlin: Stiftung Wissenschaft und Politik. doi:10.18449/2019S12
- Volland, Christian. 2019. "Digitalization of the European Union: Blind Spot Human Rights?" Leuphana University Lüneburg, Lüneburg, Germany.
- Wagner, Ben. 2011. 'Freedom of Expression on the Internet: Implications for Foreign Policy'. *Global Information Society Watch* 18–20.
- Wagner, Ben. 2014. 'The Politics of Internet Filtering: The United Kingdom and Germany in a Comparative Perspective'. *Politics* 34(1):58–71.
- Wagner, Ben. 2016a. *Global Free Expression: Governing the Boundaries of Internet Content*. Cham, Switzerland: Springer International Publishing.
- Wagner, Ben. 2016b. "Symbolic Power and Legitimacy Theatre: Constructing Legitimacy in Global Internet Governance." Pp. 157–74 in the *Global Free Expression - Governing the Boundaries of Internet Content, Law, Governance and Technology* series, edited by B. Wagner. Cham: Springer International Publishing.
- Wagner, Ben. 2018. "Can Germany's 'Lex Facebook' Be Saved? A Business and Human Rights Analysis – Global Voices." Global Voices. Retrieved 1 October 2019 (<https://globalvoices.org/2018/03/13/can-germanys-lex-facebook-be-saved-a-business-and-human-rights-analysis/>).
- Wagner, Ben. 2019. "All Codes – No Conduct? Performing the Governing Artificial Intelligence." Sydney, Australia: Center for Law & Public Utilities (CeLPU), Seoul National University; Centre For Media Transition, University of Technology Sydney.
- Wagner, Ben, Krisztina Rozgonyi, Marie-Therese Sekwenz, Jat Singh, and Jennifer Cobbe. 2020. "Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act." Barcelona, Spain: ACM Fairness Accountability and Transparency (FAT).
- WGIG. 2005. Report of the Working Group on Internet Governance.

11 Abbreviations

A29WP	Article 29 Working Party
AfD	Alternative für Deutschland (Alternative for Germany)
API	Application Programming Interface
AVMSD	Audiovisual Media Services Directive
BfJ	Bundesamt für Justiz (Germany's Federal Office of Justice)
DG Connect	Directorate-General for Communications Networks, Content and Technology
DPA's	Data Protection Authorities
DPC	Data Protection Commission
DNS	Domain Name System
DSA	Digital Services Act
DSAR	Digital Services Act Regulator
ECD	E-Commerce Directive
EDPB	European Data Protection Board
EDPS	European Data Protection Supervisor
EDRi	European Digital Rights
EFTA	European Free Trade Association
ENISA	European Union Agency for Cybersecurity
EU	European Union
GAC	Governmental Advisory Committee
GDPR	General Data Protection Regulation
GIS	Geographic information systems
GPS	Global Positioning System
ISA	Intelligent Speed Assistance
ITU	International Telecommunications Union
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forum
JRC	European Commission's Joint Research Centre
KBA	Kraftfahrt-Bundesamt (Germany's Federal Motor Transport Authority)
NetzDG	Netzwerkdurchsetzungsgesetz (German Network Enforcement law)
NOx	Nitrogen Oxide
OECD	Organisation for Economic Co-operation and Development
TSs	Technical Services for testing vehicles emissions
UN	United Nations
U.S.	United States
WCIT	World Conference on International Telecommunications
WSIS	World Summit on the Information Society
W3C	World Wide Web Consortium

12 About the authors

Dr. Carolina Ferro is a human rights consultant and researcher with over fifteen years of experience in academic research, lecturing and management of non-profit organizations. She is a consultant and director at Enabling Digital Rights and Governance, working on digital technologies, governance and human rights.

She previously worked as general coordinator of the Gaspar Garcia Human Rights Centre (Sao Paulo/Brazil) and as research fellow at the Research Centre for Participation, Social Movements and Collective Action at the State University of Campinas (Brazil). She is currently based in Tallinn (Estonia) and holds a Ph.D. in Political Science from the State University of Campinas.

Dr. Ben Wagner is an Assistant Professor and Director of the Privacy & Sustainable Computing Lab at Vienna University of Economics and Business (WU Wien), where his research focuses on technology policy, human rights and accountable information systems. He is an Associate Faculty member at the Complexity Science Hub Vienna, a visiting researcher at the Human Centred Computing Group at the University of Oxford and a member of the Advisory Group of the European Union Agency for Network and Information Security (ENISA).

He previously worked at the Technical University of Berlin, Cambridge University, the University of Pennsylvania and European University Viadrina. He holds a PhD in Political and Social Sciences from European University Institute in Florence.

Address | Contact

Bertelsmann Stiftung
Carl-Bertelsmann-Straße 256
33311 Gütersloh
Telephone +49 5241 81-0

Falk Steiner
Senior Expert Digital Policy
Telephone +49 30 275788-132
falk.steiner@bertelsmann-stiftung.de

Ralph Müller-Eiselt
Director Program Megatrends
Telephone +49 5241 81-81456
ralph.mueller-eiselt@bertelsmann-stiftung.de

www.bertelsmann-stiftung.de