Normsetzung und Entscheidungsverfahren 3

Rita Gsenger | Marie-Therese Sekwenz (Eds.)

Digital Decade

How the EU Shapes Digitalisation Research

Nomos

weizenbaum institut

https://doi.org/10.5771/9783748943990, am 01.07.2025, 11:54:01

Preface

Simon Schrör & Herbert Zech

In 2025, we are in the midst of the European Union's proclaimed "Digital Decade". With its ambitious and multi-layered policy program, the EU Commission is planning a framework - not only regulatory - to accompany and contain Europe's digital transformation. This undertaking alone raises many interesting questions for the legal and social sciences in the broadest sense. After all, as scientists we do not operate in a space untouched by regulation: data protection regulations, data governance, copyright law, AI regulation and many other provisions not only influence our practical everyday work, but also the subjects we research. A certain knowledge of relevant regulations, their genesis, structure and interactions with state law is increasingly necessary, even outside the legal academia, to ensure valid and excellent research.

The EU's digital decade represents a far-reaching transformation process that makes cross-disciplinary research imperative. The complex interactions between technology, society, economy, law and science require a comprehensive approach that goes beyond the boundaries of individual disciplines. Such an approach presents a promising pathway for a comprehensive analysis and normative evaluation of the social, ethical, political, and, not least, scientific implications of digitization (and its regulation). Critical monitoring of EU regulatory proposals is of central scientific importance in this context. It ensures that political decisions are based on sound knowledge and that potential risks are minimized. These are all major demands and challenges facing scientists today.

Until now, however, there has been a lack of interdisciplinary introductory literature to help researchers deal with these new, and often evolving regulations. Rita Gsenger and Marie-Therese Sekwenz, together with the contributors to this volume, are now filling that gap. The edited volume "Digital Decade: How the EU shapes digitalization research" offers introductions to the most important digital regulations of the EU and combines accessibility with in-depth knowledge of the relevant laws and regulations.

It should be emphasized that the genesis of the anthology itself arises from a community that sees interdisciplinary research and transdisci-

plinary dialogue as an important means to a comprehensive understanding of digital regulation and its impact. The editors and authors deserve great thanks for the rapid completion of the book, the contents of which were discussed and compiled at an interdisciplinary workshop at the Weizenbaum Institute in Berlin in the fall of 2024. Readers will find a carefully curated overview and introduction to the most important EU regulatory proposals, as well as methodological notes and research demands.

Table of Contents

Introduction

Rita Gsenger & Marie-Therese Sekwenz

This anthology emerged from many conversations with digitalisation researchers from various disciplines who have encountered European regulations in their work: First, some must adhere to the regulations (e.g., data protection in research experiments), second others have recognised their conceptual impact on their fields. Third, some might simply be interested, as recent regulatory endeavours, such as the Digital Services Act (DSA) or the Artificial Intelligence Act (AIA) have attracted considerable media attention. However, understanding European regulations is challenging, and getting an overview is not easy. Therefore, we collected introductions to the most relevant and crucial legislations to provide an accessible entry point into the complex landscape of EU digitalisation regulations for an interdisciplinary audience.

The principles of the Digital Decade

Europe is facing various economic and political crises in the 21st century—rising populism and scepticism toward the European project resulting in Brexit, the refugee crisis, and the adverse influence of global powers, such as Russia and China. Nevertheless, the European Union retains its "unilateral power to regulate global markets" (Bradford, 2020, pp. xiii-xiv). This regulatory influence is often referred to as the *Brussels Effec*t (Bradford, 2020). Through its regulatory efforts, the EU seeks to uphold European values and fundamental rights. The EU Charter of Fundamental Rights enshrines human dignity (Art. 1), a right to security (Art. 6), the protection of personal data (Art. 8), and freedom of thought (Art. 10) and expression (Art. 11), among others (Charter, 2012) . Protecting fundamental rights while enabling a functioning internal market is key to various regulatory endeavours. EU policy adopted an integrated strategy to create an internal market also in the digital realm. Such a strategy was first introduced in 2005, later expanded as the Digital Agenda 2020, covering the period from 2010 to 2020 (European Parliament, 2024). The second digital agenda for

Europe is set for 2020 to 2030 and aims to enhance the digital skills among adults, ensure high levels of connectivity in EU households, make all public services available online and increase the use of cloud-computing services of businesses. These aims include various new regulations, like the General Data Protection Regulation (2016/679), the Data Governance Act (2022/868), the AI Act (2024/1689), the Digital Services Act (2022/679) and the Digital Markets Act (2022/1925).

In 2023, the European Union published the "European Declaration on Digital Rights and Principles for the Digital Decade" to outline the principles of the so-called Digital Decade.

The principles focus on a human-centric approach to digitalization to foster solidarity and inclusion, guarantee connectivity for everyone, provide digital education, training and skills, and provide fair working conditions for all individuals working in a digital environment. Furthermore, the Declaration aims to ensure equal access to the digital public sphere, including the "accessibility and re-use of public sector information" (European Parliament et al. 2023, p. 4), which should be guaranteed with the Open Data Directive (Regulation 2019/1024) and the Data Governance Act (Regulation 2022/868). The declaration emphasizes the focus of the EU on fundamental rights and ethical approaches, which is also reflected in the AI Act. The rules for AI are outlined in Chapter Three of the declaration, stating that AI "should serve as a tool for people, with the ultimate aim of increasing human well-being" (European Parliament et al, 2023, p. 5). Furthermore, the declaration promises to ensure "human-centric, trustworthy and ethical artificial intelligence" (ibid, p. 5), which will be explored in Chapter 2 of this volume. Moreover, the declaration aims to create a fair digital environment and equal participation in the digital space. The latter includes pluralistic media (see Chapter 11 on the European Media Freedom Act) and the supporting free democratic debate online, which platforms are expected to uphold. The Digital Services Act (Regulation 2022/2065) ensures these principles. Lastly, security is a crucial aspect of the digital environment, which includes access to "products and services that are by design safe, secure, and privacy-protective, resulting in a high level of confidentiality, integrity, availability and authenticity of the information processed". These safeguards are established in the NIS 2 Directive (2016/1148) and the Cyber Resilience Act (2024/2847). Finally, privacy must be protected, as "[e]veryone has the right to privacy and to the protection of their personal data" (European Parliament et al. 2023, p. 6) to confidential communication and self-determination of their digital legacy. These are primarily inscribed in

the General Data Protection Regulation (2016/679). Lastly, the EU aims to protect children, youth, and the environment by guaranteeing sustainable digitalization products (European Parliament et al, 2023).

Structural aspects of European Regulations and Acts

The Treaty on the Functioning of the European Union (TFEU) organises the functioning of the European Union (Art. 1, TFEU). TFEU differentiates between different legal acts of the European Union in Art. 288. The article defines that "a regulation shall have general application. It shall be binding and directly applicable in all Member States." Regulations do not need to be transposed into national law (European Commission, no date). Another type of law is a directive, which "shall be binding, as to the result to be achieved, upon each Member State to which it is addressed" (Art. 288, TFEU). That means Member States need to achieve a particular result by adopting the Directive within their national law, so ultimately, they can decide how to achieve the determined result (Petit et al, 2024). An example is the Copyright Directive (2019/790), which allows press publishers to have more control over their publications, giving them exclusive rights to authorise or restrict the publication of their products on information society service providers (Art. 15). Member States interpret the details of restricting publications by publishers according to Art. 15 differently. Most Member States exclude private uses from such restricted publishing rights, only Belgium, France, the Czech Republic, and Sweden do not exclude private uses of press publications (Nobre, 2024).

Recommendations and opinions, however, are not binding legislative acts. According to Art. 289, TFEU, "[l]egal acts adopted by legislative procedure shall constitute legislative acts". These express the opinion of the European institutions.

Finally, the EU also publishes *delegated acts* and *implementing Acts* especially relevant to laws regulating the digital sphere. These are both legally binding. Delegated acts amend an EU legislative act by detailing measures for example for prescribing rules for researcher data access under the DSA. Implementing acts set conditions for a uniform application of the EU legislation (Petit et al, 2024). An example is the delegated regulation for rules on audits of very large online platforms and search engines under the Digital Services Act (2024/436), detailing how audits should be implemented (European Commission, 2023).

The structure of this book

Each Chapter of this volume provides an overview of an entire piece of legislation, an aspect that is particularly crucial for social scientists and computer scientists, or a particularly contested and highly debated provision. The book is interdisciplinary by nature. Most contributors have a legal background; however, others also have a background in the social sciences or computer sciences.

The first Chapter provides an overview of "Methods of Empirical Legal Studies" by *Catrien Bijleveld*. Based on her introductory book on ELS methods (Bijleveld, 2023), she demonstrates how empirical research can complement doctrinal research and which methods are suitable for understanding regulatory effects. Furthermore, the Chapter provides an overview of the state-of-the-art in empirical legal research, summarizing the most prevalent studies. Bijleveld introduces new ways of thinking about legal regulations aside from doctrinal practices and provides an entry point for more interdisciplinary research.

The book's first part concerns the regulation of Artificial Intelligence (AI) and, more specifically, the European AI Act (Regulation 2024/1689). Two chapters focus on the regulation to provide a comprehensive overview and avenues for further research. *Hannah Ruschemeier* and *Jascha Bareis* outline in their Chapter *"Searching for harmonised rules: Understanding the paradigms, provisions and pressing issues in the final EU AI Act"* the structure, most important provisions and shortcomings of the Act. They approach the subject from an interdisciplinary perspective, combining legal and political analysis. Accordingly, the adoption of the Act is situated in the political structure and strategic geopolitical decisions of the European Union (EU), given the powerful influence of US and Chinese companies, who dominate the AI technology development sector. Against this backdrop, the core provisions are explained, including the risk categorisations of AI systems and which systems are prohibited in the EU. Finally, Ruschemeier and Bareis conclude their chapter with the shortcomings of the AI Act and specify where the AI Act was watered down in the process influenced by industry lobbying.

In the second Chapter on the AI Act, "*Accountable AI: It takes two to tango*", *Jorge Constantino* reflects on how accountable AI can be realized, concluding that deployers and developers of AI systems need to be considered. The Chapter discusses ethical considerations when deploying AI systems for societal tasks, such as detecting social service fraud. The Chapter

details the understanding of accountable AI by the EU and how these were included in the AI Act, focusing on Article 14 and 26 AI Act (Regulation 2024/1689).

The subsequent part of the book introduces various forms of platform regulation. "*The Digital Services Act: Online Risks, Transparency and Data Access*" by *Marie-Therese Sekwenz* and *Rita Gsenger* provides an overview of the most important provisions. First and foremost, transparency mechanisms are introduced, including the reporting obligations for platforms and the so-called flagging of content, i.e., the reporting by users. In this context, trusted flaggers and mechanisms to increase content moderation transparency are presented, such as the terms and conditions database, the statement of reasons database, or the ad library. Furthermore, the risk mechanism in the DSA is introduced, including risk assessment and risk mitigation measures by platforms.

In a second chapter about the DSA, *Pascal Schneiders* and *Lena Auler* focus on "*The Digital Services Act – an appropriate response to online hate speech?",* specifically on illegal content, mainly hate speech. The authors shed light on illegal hate speech and the content moderation measures required by the DSA. These include the notice-and-action mechanisms and the complaint and redress mechanisms outlined in the regulation. Lastly, the Chapter specifies the data access for independent research institutions and transparency measures. Finally, the authors evaluate the measures and their effectiveness, discuss what platforms should do against hate speech, and examine how transparency could be achieved.

The following Chapter, "*The Brave Little Tailor v. Digital Giants: A fairy-tale analysis of the social character of the DMA*" by *Liza Herrmann*, introduces the Digital Markets Act (Regulation 2022/1925). The author first reflects on the complicated relationship between legal studies and social sciences as well as the social character of the law. In the second part of the Chapter, she introduces the DMA, describing its background and the objectives of ensuring the contestability and fairness of markets in the digital sector and ultimately guaranteeing a functioning internal market. Finally, Liza Herrmann assesses the social aspects of the DMA, focussing on the common good as an important element of the principle of proportionality in the regulation.

The seventh Chapter, "*Eyes Shut, Fingers Crossed: The EU's Governance of Terrorist Content Online under Regulation 2021/784*" by Valerie Albus, introduces the Terrorist Content Online Regulation (TCO Regulation) and its key provisions. This Regulation is a crucial precursor to other

online content governance mechanisms, such as the Digital Services Act. The TCO Regulation mandates that hosting services comply with removal orders issued by national competent authorities within one hour. Furthermore, the hosting services must prevent the distribution of terrorist content. However, over-removal might be an issue due to high fines and tight deadlines. Furthermore, determining whether content qualifies as terrorist material is complex. The author emphasizes that the Regulation places full responsibility on platforms, while EU Member States remain largely disengaged.

The eighth Chapter, "*What the Political Advertising Regulation Can Do for Researchers (and Vice Versa)*" by *Max van Drunen*, focuses on the advertising activities covered by the Regulation on the Transparency and Targeting of Political Advertising (PAR) and the access mechanisms it grants to researchers. The scope of the Regulation includes political advertising for and by political actors, as well as referenda and legislation. Various questions remain open regarding targeting in advertisements and voter manipulation, as demonstrated by the Cambridge Analytica scandal in 2018. Therefore, the regulator has introduced some transparency requirements for platforms regarding political advertising. These include ad libraries, public access to data, and data access for researchers. Ad libraries provide information such as the ad's content and the identity of the advertised product, service or brand. Moreover, they contain the dissemination period, funding, reach, targeting, moderation and legal rights it might promote. The PAR also enables data requests for vetted researchers, some members of civil society organisations, political actors, electoral observers, and journalists. They can request ad context, the service provided, and the funding of the advertisements from political advertising service providers. Additionally, controllers using targeting or ad-delivery techniques can be asked to provide internal policies and records on targeting. In the final section of the paper, Max van Drunen offers recommendations for researchers to support political advertising governance and outlines open questions. These include the definition of political ads, which is considered too broad in the PAR, the justifications for prohibiting political ads, and the use of labelling for political advertisements.

The ninth Chapter, "*The EU Directive on Copyright in the Digital Single Market*" by *Lisa Völzmann*, outlines the aims and effects of the Copyright Directive. The author primarily discusses the text and data mining provisions, the press publishers' rights and the liability of intermediaries. Overall, the Directive aims to harmonize copyright regulations in the digital sin-

gle market of the European Union by adjusting the existing copyright laws to create legal certainty and enhance innovation. The author focuses on the most debated provisions, including the Press Publishers' Right (Art. 15), Licensing Obligation, and Intermediary Liability (Art. 17). She concludes with an assessment of the risk of overblocking, a long-standing concern associated with the Copyright Directive.

The Copyright Directive also aims to support the freedom of the press. More importantly, however, the European Media Freedom Act (EMFA), as detailed by *Adelaida Afiliapoaie* and *Heritiana Ranaivoson* in Chapter 10, "*The European Media Freedom Act: A Redoubt for Pluralism in an Increasingly Concentrated Landscape*" addresses media pluralism. The EMFA focuses on the proper functioning of an internal market for media services. It focuses on news media, and Afiliapoaie and Ranaivoson examine Art. 22, which details the assessment of media market concentration by the National Regulatory Authorities. However, the EMFA includes video-sharing platforms and very large online platforms as media service providers, which might revive a discussion regarding editorial control. The chapter details all Art. 22 provisions, focusing on ownership, diversity, editorial independence, and economic sustainability. Overall, they conclude that introducing a pluralism test and media concentration assessments by the National Regulatory Authority is beneficial.

The following Chapter on "*The Data Governance Act – Is "trust" the key for incentivising data sharing?*" by Lucie Antoine details the role of trust in data sharing, namely for data intermediation services and data altruism organisations. Moreover, the DGA examines the rules for re-using data held by the public sector based on a principle of trust. The trust in actors that make the data flow in Europe productive is crucial for the European data economy. The DGA assumes increased user trust facilitates data sharing as it influences user choices. However, the author doubts that data intermediaries can fulfil the expectations that have been placed on them. However, they could contribute to the data economy by providing infrastructure for data sharing and exchange and enforcing data subjects' rights. The reuse of public data is regulated in the Open Data Directive (ODD), which is elaborated in Chapter 12, "*The Open Data Directive: potential and pitfalls for the social sciences*", by *Nik Roeingh* and *David Wagner*. The ODD signifies a milestone in approaching more openness and open government data in the EU. The authors first introduce the concept of open government data, which refers to the public sector providing as much data as possible and as open as possible so others can use them. That

includes the scientific community. The ODD aims to create a single market for data without any disruptions.

Moreover, the Directive promotes innovation with public sector data, especially AI applications. Lastly, it aims to ensure that data reuse contributes to social purposes, accountability, and transparency. The authors then provide an overview of openness categories in the ODD, which are defined by licenses, formats, charges, non-discrimination, and exclusivity arrangements. In the last section, the authors describe how the social sciences can benefit from the ODD and also how they need to adhere to the regulation.

The Data Act (DA) (Regulation 2023/2854) also addresses data access. It intends to increase data sharing, as elaborated in Chapter 13, "*IoT Data within the Context of the Data Act: Between Opportunities and Obstacles*" by *Prisca von Hagen*. The Chapter focuses on data generated by Internet of Things (IoT) products and introduces the different actors and positions regarding data access and ownership-like status. Furthermore, the author doubts the DA's effectiveness due to information asymmetries on the user's side, especially in a B2C relationship. Moreover, the author raises concerns about legal certainties, as data access could be significantly delayed if the parties have disputes and courts need to decide on the access.

Finally, the General Data Protection Regulation (GDPR) elaborates on access to and portability of data as described in Chapter 14, "*EU Data Protection Law in action: Introducing the GDPR*" by *Julia Krämer*. The Chapter reflects on the past six years the Regulation has been in force. It evaluates its effectiveness and whether its key principles, such as lawfulness, fairness and transparency in data processing, have been upheld. The author provides an overview of empirical research investigating various GDPR provisions such as consent, sensitive data, transparency, data minimisation, right to access, and the right to be forgotten. By detailing research on dark patterns and privacy policies, the author concludes that empirical research can be valuable in providing evidence about the effectiveness and consequences of these provisions.

The first of nine sector-specific data spaces, part of the European Data Strategy of 2020, is introduced in Chapter 15, "*European Health Data Space*" by *Lisa Markschies*. The chapter introduces the new framework for primary health data to provide healthcare professionals with the means to treat their patients better. Furthermore, the EHDS aims to empower individuals to take control of their health data. The patient's access to health data should be free of charge, and the data should be legible. Due to the data's sensitivity, the EHDS obliges Member States to create an

appropriate infrastructure. Moreover, the EHDS aims to foster secondary use of health data, for instance, for research. Some secondary use is also explicitly prohibited, such as the use of data for marketing and advertising. The question of consent was highly debated regarding the EHDS, and due to the decreased success of opt-in solutions, no consent for secondary use is required. The Chapter also outlines some open questions, such as the relation between the EHDS and the GDPR, the differences between member States and the data quality, especially for research.

The book's last part covers cybersecurity, which has gained increasing importance recently. First, the Cyber-Resilience Act (CRA) is covered in Chapter 16, "*The CRA and the challenges of regulating cybersecurity in open environments: The case of Free and Open Source Software*" by *Lucas Lasota*. The Chapter investigates the CRA from an interdisciplinary perspective, outlining how the CRA came to be, the necessity for increased security quality of tech products, and the perspective of Free and Open Source Software (FOSS) stakeholders in the public debate. The latter is crucial as the CRA is concerned with embedded and non-embedded software, and almost all software also has open-source elements. The CRA treats cybersecurity as a quality of digital products and aims to increase the level of cybersecurity and also provide better information to consumers. The Chapter subsequently explores the role of FOSS stewards and the role of FOSS in the regulatory process. The Chapter concludes that the CRA still has a long way to go to balance fundamental rights and values while improving cybersecurity.

The final Chapter, "*Unpacking the NIS 2 Directive: Enhancing EU Cybersecurity for the Digital Age*" by *Eyup Kun*, introduces the second Network and Information Systems Directive or NIS, a continuation of the NIS 1 Directive from 2016. The NIS 2 Directive aims to enhance the cybersecurity framework of the EU by solving underinvestment in cybersecurity by private and public actors. These actors are required to ensure the security of networks and information systems, and they are held responsible if they fail to do so. The Chapter additionally details the roles and responsibilities of Member States regarding the NIS 2 Directive, which include the establishment of computer security response teams, collaboration between actors regarding cybersecurity incidents and a national cyber crisis management framework. Aside from national cooperation, the NIS 2 also establishes an EU-wide collaboration with the European Vulnerability Database and EU-CyCLONe, a cyber crisis liaison organisation network. The author

concludes that the NIS 2 Directive focuses on protecting critical sectors and enables an increased investment into cybersecurity.

We are grateful for the support of the Research Group Norm Setting and Decision Processes of the Weizenbaum Institute in Berlin, in particular Jana Pinheiro, Till Häselbarth, Jasmin Bernardy and Mariam Sattorov for the organisation of a Workshop in preparation of this book and all the other organisational tasks that are required for such a volume to be possible. A special thanks goes to Prof. Herbert Zech and Simon Schrör for supporting this idea and the possibility of publishing as part of their ongoing series *Normsetzung und Entscheidungsverfahren – Schriftenreihe des Weizenbaum-Instituts für normative Wissenschaften* at Nomos. Furthermore, we thank Dr. Marco Ganzhorn for the editorial support. Lastly, we thank all the anonymous peer-reviewers who contributed time and effort to increase the quality of the works.

References

Bijleveld, C. (2023) *Research Methods for Empirical Legal Studies: An Introduction*. The Hague: Eleven.

Bradford, A. (2020) *The Brussels Effect*. Oxford: Oxford University Press. Available at: https://doi.org/10.1093/oso/9780190088583.003.0003 [Online] (Accessed: 10 December 2024).

'Charter of Fundamental Rights of the European Union (2012/C 326/02)' [Online]. Available at:https://commission.europa.eu/law/law-making-process/types-eu-law_en (Accessed: 10 December 2024).

'Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC' (2019) *Official Journal* L 130, 17 May, p. 92–125 [Online]. Available at: http://data.europa.eu/eli/dir/2015/1535/oj (Accessed: 3 December 2025).

European Parliament, Council and European Commission (2023) *European Declaration on Digital Rights and Principles for the Digital Decade (2023/C 23/01)* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32023C0123(01) (Accessed: 3 December 2024).

European Commission (2023) COMMISSION DELEGATED REGULATION (EU) …/...of 20.10.2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/delegated-regulation-independent-audits-under-digital-services-act (Accessed: 10 December 2024).

Haack, S. (2014) *Evidence Matters: Science, Proof, and Truth in the Law*. Cambridge: Cambridge University Press.

Nobre, T. (2024) 'The Post-DSM Copyright Report: the press publishers' right', COMMUNIA Association [Online]. Available at: https://communia-association.org/2024/02/19/the-post-dsm-copyright-report-the-press-publishers-right/ (Accessed: 10 December 2024).

Petit A., Wala Z., Ciucci M., Martinello B. (2024) Digital agenda for Europe [Online]. Available at: https://www.europarl.europa.eu/factsheets/en/sheet/64/digital-agenda-for-europe (Accessed: 3 December 2024).

'Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)' (2022) *Official Journal* L 277, 27 October, pp. 1-102. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065 (Accessed: 19 January 2025).

'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)' (2022) *Official Journal* L 265, 12 October, pp. 1-66 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925 (Accessed: 19 January 2025).

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)' (2016) *Official Journal* L 119, 4 May, pp. 1–88, [Online]. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 30 January 2025).

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L, 2024/1689, 12 July [Online]. Available at: http://data.europa.eu/eli/reg/2024/1689/oj (Accessed: 29 January 2025).

'Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)' (2024) *Official Journal* L, 2024/2847, 20 November [Online]. ELI: http://data.europa.eu/eli/reg/2024/2847/oj (Accessed: 10 February 2025).

'Treaty on the Functioning of the European Union' (2012) Official Journal C 326, 26 October, pp. 47-390 [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF (Accessed: 5 December 2024).

Methods for Empirical Legal Research

Catrien Bijleveld

Abstract

This chapter is part of a book that focuses on new EU legislation in areas that link to digitalisation, such as the DSA, the EMFA, and more generally the GDPR. Much of this legislation is relatively new. And most of it is fairly extensive and complex, with, for instance, the DSA (English version) comprising more than one hundred pages. It is therefore more than laudable that the editors of this volume have chosen to bring together scholars to facilitate understanding and research into this legislation.

This Chapter will briefly describe some core principles for carrying out empirical legal research. The introduction to commonly employed empirical research methods will be basic and conceptual. In this chapter, I borrow from Bijleveld (2023), which provides a more extensive, yet easily accessible and conceptual, introduction to Empirical Legal Studies (ELS).

1. What are empirical legal studies

Empirical legal studies, or empirical legal research, is a label given to studies that focus on the law by gathering empirical facts. ELS is, in a sense, a subfield at the fringes or the intersection of law and social sciences. It is also encountered as *empirical legal research* or *legal realism*/*new legal realism*. Similar – but not exactly identical – areas of study are denoted as *law in action* or *legal sociology*. Some (sub)disciplines share properties with empirical legal research: criminology does, and so do legal sociology, law and economics, and legal anthropology.

Questions addressed in ELS all inquire into empirical facts, and can be categorized into three pillars or a "trias ELSica" (Bijleveld, 2023). They focus on the law's assumptions (such as that harm can be repaired by monetary compensation), its operations (such as the time it takes to reach a decision in court cases), or effects (such as whether the DSA is successful in protecting consumers and their fundamental rights). The pillars are intrinsically related. If the assumptions on which laws are built are incorrect,

or if tradition or lack of intrinsic support for new rules stand in the way, then it is very unlikely that the laws would have their desired effect. If the assumptions are correct, but the law is not applied as planned (for instance, cases take extraordinarily longer to process, and judges find the new rules unworkable), it is also unlikely that the foreseen effect would materialize. In that sense, the three pillars form a trias.

ELS is clearly not doctrinal. In doctrinal research, case law, or the extent to which laws and regulations are in line with treaties or supranational law, are studied (see, e.g., Hutchinson, 2013; 2015; Van Boom, Desmet and Mascini, 2018; Van Gestel and Micklitz, 2011). For instance, in jurisprudence analysis, we may be interested in how cases have been dealt with, what arguments have been used to find accused parties liable, and what the threshold is that the Supreme Court employs for finding that there was criminal intent. Scholars who analyse such case law do so in a fairly targeted way. They pick the exemplary case law to prove a point or illustrate a new turn in evidentiary practice. However, it is very conceivable that one legal scholar would arrive at a different conclusion when investigating the same doctrinal issue simply because they regard different cases as pertinent or adopt a different philosophical stance. It then also depends very much on the scholar's authority to what extent the conclusion is regarded as valid.

Contrary to doctrinal research, data collection in ELS is done systematically, according to a well-described and accepted set of rules. In ELS, we gather empirical facts about the law and investigate what occurs in the measurable world around us, what happens within legal practice, and what the effects of laws are. We want the person collecting the relevant facts to serve solely as the vessel through which the data are presented, forming the basis for the conclusion. Formulated conversely, we would not want our understanding of the empirical world around us to depend on what particular scholar carried out the research. The real world is out there, and we would want each scholar who employs the same systematic empirical approach to arrive at approximately the same conclusion about that reality.

However, while ELS is empirical and appears disjunct from doctrinal research as different questions are asked in ELS and different methods are used, the core interest of all ELS *is* the law. What distinguishes ELS from other empirical disciplines such as legal sociology, law and economics, or legal anthropology is that an ELS scholar will always want to translate their findings back to the law. What do the empirical findings mean for how laws have been drafted? What do they mean for legal practice? The core

interest of the ELS scholar is the law and not the testing of an economic or sociological theory.

ELS is, therefore, not disjunct from legal, doctrinal research. Davies (2020) argues that the doctrinal and empirical study of law should, in some way, enrich each other. Van Boom, Desmet and Mascini (2018, pp. 5–6) write that the empirical study of law enriches doctrinal legal research beyond empirical fact-checking because it allows a deeper understanding of not only the plain facts but also the underlying mechanisms of legal interaction, including insight into both explicit reasoning and unconscious processes in legally relevant decision-making. ELS is, therefore, part and parcel of the legal discipline, sometimes indicated by a hyphen as in: *empirical-legal studies*.

What is important at this stage is to note that, from the various definitions, three defining characteristics of empirical legal research emerge, namely that (1) an empirical legal study poses questions about the law, (2) it systematically collects empirical data to answer those questions, and that (3) the answers to the questions are legally relevant. What precisely the latter is remains fairly vague. In general, we mean by this that, in some way, we would want to be able to translate back the research findings to the law and legal practice. For instance, a study might find that an applicability test for social benefits has been formulated so vaguely that wide discrepancies exist between officials in interpreting these norms, thereby threatening equality before the law. The study could then point out that clearer norms or criteria need to be formulated.

Given that ELS evolves around the analysis of the empirical world, empirical methods are used. Empirical methods are used in many empirical disciplines; in that sense, these methods are not particular or new. We encounter both quantitative and qualitative methods. Across the quantitative board, we find univariate methods, such as means, medians and percentages. We find correlational methods, such as simple correlation measures and cross-tabulations, that give a feel for association through chi-square measures and odds ratios. Multivariate methods are mostly used first when we want to predict an outcome from a set of characteristics. Regression analysis can be used to predict sentence length from gravity of the crime, mitigating and aggravating circumstances (see, for instance, Hola et al, 2015). Analysis of variance or ANOVA is often used when we analyse data from vignette studies, where the variables have a specific format. Other, less run-of-the-mill multivariate techniques may be used, such as factor analysis

or multiple correspondence analysis, to identify risk profiles of persons placed under guardianship measures, looking for particular combinations of mental and physical health problems, financial problems and issues in their support network (Nieuwboer et al, 2025). We sometimes encounter methods from other disciplines as they are particularly suited to the type of data we collect for the phenomena we are studying. A technique borrowed from epidemiology, for instance, is generally used if we study disposition times: we then need so-called time-to-event or survival methods (see, Bijleveld, 2023, chapter 6), for which analysis techniques can be univariate, bivariate or multivariate depending on the complexity of the models we are using. Quantitative methods, specifically econometric methods, are almost universally used in Law and Economics, which clearly overlaps with ELS.[1]

Qualitative methods are also widely used, amongst which the most prominent probably is content analysis. It is used to analyse textified material, such as court files, applications, and interview transcripts. Qualitative methods are very flexible and can also be used to analyse behaviour that has been systematically observed (such as courtroom interactions) or captured in video material (such as CCTV-recorded interactions between officials and citizens). The analysis of such materials can be done deductively, that is, departing from a given theoretical framework in which the researcher investigates to what extent certain characteristics are present, or inductively, in which case the researcher approaches the material and seeks for patterns, repetitions and so-called *themes* in the material (see, Bijleveld, 2023, Chapter 7, and Tracy (2013) for textbook introductions, and, specifically on qualitative methods in empirical legal studies, see, Webley (2010)).

Sometimes, particular data collection methods are used because of the nature of the phenomena being studied. For instance, if we are interested in estimating the prevalence of fraud, we must account for the fact that respondents may not be eager to divulge behaviour that they are ashamed of and we may need to employ specific methods for sensitive topics, such as randomized response (see, John et al, 2018, for a non-technical overview, and for some examples, see, Bijleveld, 2023, Chapter 10).

1 The US based Journal of Empirical Legal Studies has numerous examples of the application of such methods. Additionally, Chapter 38 in Cane and Kritzer (2010) gives an overview of quantitative methods in ELS.

2. Doing empirical legal research

If we want to study the assumptions made within the law, its operations, or effects, we mostly use so-called constructs. Constructs are variables that are considered relevant for the research (such as *trust*), but that are not directly observable (which a variable such as *sentence length* would be). Given that a construct is not easily observable, a definition must be given, and it needs to be *operationalised*, it needs to be laid down how exactly we could measure it.

An example of such a construct is *procedural justice* (Tyler, 1990), which is assumed to be an important pillar of legitimacy. The theory of procedural justice posits that if citizens regard the justice process as having been conducted in accordance with fairness principles, they are more likely to comply with the outcome, even when the outcome is unfavourable for them. Formulated differently: The theory posits that how citizens regard the justice system is tied more to the perceived fairness of the justice process (including the manner in which citizens are approached) than to the perceived fairness of the outcome. The construct of procedural justice is generally considered multidimensional, although these dimensions are encountered in the literature in slightly different constellations. Notable dimensions are (1) voice (citizens are given the opportunity to express their side of the story); (2) respect (officials treat parties with dignity and respect); (3) neutrality (the decision-making process is unbiased); and (4) transparency (parties can see the above being done). Other dimensions that may be postulated are (5) understanding (citizens understand the process and how decisions are made); and (6) helpfulness (perception that system players are interested in your personal situation to the extent that the law allows).

Operationalizing is sometimes not straightforward and is relatively easily exemplified with the psychological construct *intelligence*. While the word intelligence is common usage in many languages, the 1981 version of the Wechsler Adult Intelligence Scale, for instance, presented verbal and performance-scales, measured with several subtests, five for verbal and six for performance abilities. Other instruments (such as the Raven test, which is nonverbal) use a conceptual definition that differs or operationalizes intelligence (slightly) differently. If one uses a different conceptual definition of intelligence or a different operational definition, intelligence measurements will differ across definitions. The same goes for constructs used more often in ELS, such as trust or justice. An application of operationalization in the

study of medical malpractice can be found in Van Velthoven (2016), and a nice illustration of how different operationalizations unpack in practice in Haucke, Hoekstra and Van Ravenzwaaij (2021).

Constructs should be operationalized to ensure they provide both a valid and reliable measurement of the property investigated. A *valid measurement* is a measurement that truly, validly represents the property of interest. For example, an intelligence test that measures only arithmetic skills does not represent the entire spectrum of what we suppose intelligence contains. It will produce an invalid measure of our construct intelligence. A test that is very verbose will not be able to measure the intelligence of recent migrants who have not yet mastered the local language. We would also like our test to predict (to a certain extent) school success, as we expect performance to correlate with intelligence. A measure that does all that, we label as *valid*. Comprised in validity is the idea of *reliability*, as the measures should be precise. Again, a counter-example of what we mean by reliability is the following: using an elastic measuring tape would, for instance, make for an unreliable measure of people's height. One time, a person's height would be measured as 170 cm, next as 172, then 167, then 173, etc. If the measurement was done 100 times, the result would likely be, on average, right. However, the measure is considered unreliable because of the variability in the measurements.

A reliability check is often done by having two observers code the same feature independently. If the results from these two raters concur, *interrater reliability* is present. Reliability can be expressed as percentage agreement as well, and other measures exist. Assessment of validity is more complex, although, in general, face validity is often employed (essentially, whether the measures look credible and in accordance with the definition). See Bijleveld (2023, Chapter 2) for a succinct overview and Drost (2011) for a more extensive treatise focused on psychometric research.

Validity and reliability are important in themselves, and also because scientific research needs to be *replicable*. For important conclusions on the operations of the legal system or the effects of the law to be solid, and not a one-off result, we want them to be corroborated by several independent researchers. As said above, different researchers using the same instruments should arrive at roughly the same conclusion about the world. Valid and reliable findings build confidence in the relevance of the findings, and provide a basis for evidence-based policy. Validity (and inherent to it: reliability) is a necessary condition for research to be replicable.

It is not a sufficient condition, however. Mainly for psychology and health research, a *replication crisis* has been identified. Studies have been repeated with the same definitions, measurements, and procedures, but rendering different results. Such different results are, of course, highly problematic. Replicability should not be confused with reproducibility, which is generally understood as different researchers analysing the same data and arriving at the same result. Both reproducibility and replicability are important desiderata, and increasing focus is put on encouraging (or even requiring as a condition for funding) that researchers make their datasets available for re-analysis by others.

3. Empirical legal research: qualitative and quantitative methods

An often-used categorisation of research that we already briefly touched upon is the division into qualitative and quantitative studies. Formulated simplistically, the two can be characterised as follows: while quantitative studies aim to measure the volume or *quantity* of some variable of interest, qualitative studies are geared towards discovering the *quality*, *nature*, *why* or *how* of phenomena.

In a study that uses quantitative methods, the goal is to understand *how often* something occurred, such as: "How often are cases of domestic violence acquitted?" or "What percentage of citizens have trust in the criminal justice system?" or "How many citizens with a certain type of legal problem take their case to court?" Quantitative studies typically follow a fairly strict format (the empirical cycle) in which hypotheses are formulated and where statistical testing is generally employed. Also, samples are generally large in quantitative research, and standardised instruments (such as coding lists or web surveys) are often used. An explicit aim is to generalize findings from the studied sample to a larger population. On the other hand, qualitative methods are used to understand *why* things happen or *how* and to explore new phenomena. Examples of questions we would pose then are: "What are the reasons for taking or not taking a business conflict to court?" or "Under what circumstances are domestic violence filings settled through mediation?" or "What deliberations do judges make in divorce procedures when one parent has accused the other of sexual abuse?" Qualitative studies are generally much less strictly formatted beforehand than quantitative studies. Hypothesis testing is rare, and statistics is therefore used much less often. Qualitative designs differ from quantitative methods: smaller,

not necessarily representative samples are generally used. Open interviews, focus groups and observation are common, and analytic methods are less prescribed and more exploratory, often spread over several iterations.

Quantitative research generally produces a broad, generalizable, quantitative summary of a phenomenon. Qualitative research gives a rich understanding of a particular problem within a particular context. As the two are different methods for answering seemingly different kinds of questions, neither is superior to the other. The adverb *seemingly* is not used without purpose, however, as many questions can be addressed using either quantitative or qualitative methods. The approach may then be different, depending on what type of methods and answers are chosen.

In qualitative research, the aim is much less to produce generalisable quantitative statements but to unravel a number of mechanisms, to *understand* what happened, or to understand the meaning that the research subjects give to the phenomena being studied. As qualitative scholars work from the assumption that all human enterprise is contextual, they tend to study phenomena, and understand phenomena, within a given, particular context. Therefore, qualitative research is inherently less generalisable.

Quantitative studies are sometimes irreverently qualified as shallow. In a quantitative study, only a few factors or variables are investigated. Contextual effects are generally not included but seen as a nuisance: quantitative researchers attempt to isolate the variables they are interested in and control for any contextual noise that might distort the picture. Examples of such studies are experimental studies into the effectiveness of medicines. A group of patients is selected, and the medicine to be tested and a placebo are administered randomly among the group. Any differences between the group that received the medicine and the group that received the placebo are then attributable to the medicine and the medicine only. In such a design, the medicine is *isolated*, and the impact of any contextual effects (such as the expectations patients had, any other medical conditions patients have, their gender, or personality characteristics) is evened out by randomisation.

In summary (and admittedly leaving out nuances), a qualitative study picks a small part of the population of interest, but it delves deep, goes to the bottom of things and generates a rich and contextual understanding. However, whether the same result would have been found elsewhere cannot be guaranteed, as the findings apply only within that particular context. A quantitative study looks at a few aspects of the problem at hand but does so broadly and tries to find the impact of factors regardless of any particular context. That makes the findings of a quantitative study more easily gener-

alisable across contexts. As it largely disregards context, it investigates only a limited number of aspects of the problem at hand.

Why is it important to touch upon this distinction? Because the two traditions or paradigms use partially different methods. Qualitative studies rely more on open interviews, analysis of texts, observations, and immersing oneself in the context to be studied. Samples are generally smaller. Studies can be planned only to a certain extent, as it is uncertain beforehand what will be encountered. The analysis is generally lengthier and iterative. Quantitative studies, on the other hand, rely more heavily on pre-designed measurement instruments, such as scoring protocols or web surveys. Extensive piloting is necessary. Samples are generally larger, and testing, model building and statistics are common.

Many ELS students prefer qualitative methods to quantitative, assuming that qualitative research – without maths and formulas – is easier. The latter is, however, generally not the case. Qualitative research requires strong theoretical skills, hard and good analysis, and perseverance, constituting more often than not a substantive investment (and may entail much more – tedious – work than quantitative research). Whether the outcomes are useful is also often more uncertain beforehand. A solid qualitative study is a feat that requires extensive training and is much harder to learn through textbook recipes which can be used for teaching quantitative skills.

However, what many scholars recommend, and this author is one of them, is to combine the two types of methods whenever possible. As each type of method has its drawbacks, using both types can help to buffer the weaknesses of one through the other. If two different methods are used to answer the same question, this is called *triangulation*. By using multiple methods, we do not rely on one technique only, allowing more confidence in the research findings, their credibility, and their validity. Studies that use multiple methods are also referred to as *mixed methods* studies. Both terms (triangulation and mixed methods) are also used when researchers use different datasets; here, too, the idea is that by not relying on one source of data only, we can be more confident of the findings.

4. Sampling, representativeness and testing

As in all social science research, empirical legal research often involves working with samples due to limited time and resources. A population can be a population in the literal sense, such as all European Union inhabitants,

or all defendants at the International Criminal Court. A population can also consist of non-humans, such as all cases filed at a certain court or all verdicts in homicide cases. The population is the universe of units the researchers are interested in and want to draw conclusions on.

If only a part of that universe is studied, our knowledge of it is incomplete. As not all population members were studied, no assurance can be given that the sample results also pertain to the entire population. While sampling only a part of the population saves a lot of expenses, the flip side of the coin is that in doing so we have introduced *uncertainty*. We are unsure of what is called *external validity*, that is, whether our conclusions about the sample also hold true for the larger population.

However, scrutinizing each and every population member is actually not necessary. By following certain rules and with reasonable precision, conclusions about the entire population can be drawn, even if only a part of it, a *sample*, is investigated. Often, a small part will already do, like a 1% sample, or even less, depending on various factors. Statistics is the science of dealing with the uncertainty that sampling introduces. It provides the rules and procedures and the means to infer levels of uncertainty – or, conversely, confidence – about the conclusions drawn from the sample regarding the population.

4.1 Sample representativeness

A sample's properties resemble the population's properties. In statistics-speak, we want a *representative sample*. The easiest way to ensure that a sample's properties reflect those of the population is to draw that sample by chance or *at random*. In that case, every population member has an equal chance to be part of the sample, which is now called a *probability sample*. For that, a list of all population members is created (the so-called *sampling frame*), population members are numbered, and the desired number of sample members is chosen using some random number-generating tool. When studying case law, for example, a list of all court cases could be compiled, and a *random sample* using such a tool could be drawn. Or, if 20,000 cases are accessible and sufficient time and funds to analyse 500 cases, a random number between 1 and 20,000 is picked, and we sample every 40th case. This is called a *systematic sample*. Another option is to employ a so-called *cluster sample*: in ELS, we often find cases dealt with at different district courts within one country. One could now first draw

a random sample of courts and then, within each court again, a random sample, saving the trouble of having to collect data at each and every court. Such cluster samples are pragmatic but come at a methodological cost (the "design effect", see Bijleveld, 2023, chapter 3).

In practice, however, non-probability samples are often drawn due to a lack of sampling frame, lack of access or resources to go through all the motions of random sampling. While one should always strive for random sampling, non-probability samples may, in fact, be quite useful. They may even be representative, but representativeness is not *guaranteed*. In qualitative research, non-probability samples are frequently used. For instance, interviewing a sample of professionals who were chosen because they have specific expertise in the observation of interactions between parties involved in conflicts dealt with in a court.

In ELS, it is often technically possible to study entire populations. It may be that case law is available online, or all defendants or all litigants can be studied because case files have been digitised and electronic databases are (under some conditions mostly) available for research. The increasing digitisation of case law is a very attractive outlook for ELS. For the near future, practical constraints will make many scholars still resort to sampling, as it may be too time-consuming to study massive amounts of data, even if they have been digitised. However, as more software becomes available for automated text analysis, it is likely that enormous amounts of textified material and in fact entire populations of case law can be analysed (Dyevre, 2021).

4.2 Sample nonresponse

In most practical situations, sample nonresponse occurs, meaning the selected members cannot be assessed or sampled. This is firstly so during citizen surveys. Depending on the topic of the study, the infrastructural possibilities, the persuasive skills of interviewers and the like, survey response rates generally hover between 20% and 40%; higher response rates are rare. Therefore, to aim for a sample of 100 respondents might lead to only 40 completed interviews, a so-called *retention rate* of 40%, and an *attrition rate* of 60%. One might be tempted to think that this is not a real problem, as a larger initial sample of, say, 250 could be drawn, and then the target of 100 interviewed respondents could be reached. Unfortunately, this does not solve the problem that nonresponse generates. The problem

is namely not simply that the survey has fewer respondents. The problem is that nonresponse is generally not accidental, not random, as it is not a coincidence that certain respondents do not end up in the realised interviewed sample. Often, the vulnerable and the elderly who are too ill to be interviewed, the mistrustful, those who are afraid to talk to strangers or the busy bees with 80-hour work weeks refuse to talk to researchers.

Even if the research starts with a randomly drawn list of sample members, the non-random attrition process will lead to a non-random selection of the original random sample. Formulated more loosely: nonresponse messes up the representativeness of a sample. One might be tempted to think that this is a particularly problematic phenomenon when doing surveys with people in person who can be ill and who may decline. Attrition, however, also plays a role when studying, for instance, court files or treatment dossiers. Court files of defendants who have their cases up for review are typically unavailable and not to be found in the archive. The treatment files of recidivists may have been requested for inspection by the investigating psychiatrist or psychologist. Dossiers of withdrawn claims are cleaned earlier than those of cases taken to court. Thus, also here, the particular, atypical files will be missed, and a non-representative part of the original sample will be left for inspection.

Nonresponse is essentially irreparable. One can inspect the resulting sample thoroughly with a so-called *nonresponse analysis* and hope it resembles the population on pertinent characteristics (if known), such as age, gender, type of claim, geographical origin, and the like. If there are no serious differences, that is, if the realized sample resembles the population on such background characteristics, then that is more comforting than if differences were found. However, this background variables check does not contain information on whether the non-responders differ from the responders on the key variables of interest central to the main research question.

Nonresponse rates vary per topic and per type of study object (paper or electronic sample members, such as case files, generally do not generate high nonresponse rates). But nonresponse rates can be so high that generalisation to the population becomes increasingly unrealistic. Especially when the topic is sensitive, response rates as low as 2% have been encountered. Response rates of 40% to 50% are generally perceived as acceptable, even though then one should always check to what extent the non-responders differ from the responders.

4.3 Testing

When quantitative research is conducted, statements such as "this result is significant" or "regular divorce procedures take significantly longer than procedures with mediation" are often made. What is meant by such statements? While a detailed explanation will not be provided here, a brief overview of the concept of statistical testing will be offered.

Take the following example. After drawing a random sample of court rulings in cases of robbery, it can be seen that female defendants are handed down lighter sentences than male defendants. That might be not only the case in that sample but also in the population of all court cases. While confidence about the observation in the sample is high, in fact we are certain of the sample result, certainty about this *generalisation* cannot be postulated, as the entire population could not be observed.

Drawing a sample is a chance phenomenon, so could not the finding be simply attributable to chance, a random result, or coincidence? Because the sample was drawn randomly, the population might be reflected, but even so, uncertainty does remain. In order to deal with this uncertainty, statistical tests are used. There are very many different kinds of tests. However, the basic rationale of these tests is always the same. And this rationale is not difficult, as it follows the kind of reasoning each of us applies in everyday life.

Basically, the reasoning behind statistical testing is as follows: It begins with an assumption about the phenomenon we are interested in drawing conclusions about. Suppose, as an example, that we aim to investigate whether a new divorce procedure that includes mediation makes for shorter conclusion times than the standard divorce procedure. The assumption at the start would be:

H_0: $T_{old} = T_{new}$

In words, the new procedure takes just as long as the old procedure. This assumption is also called the null hypothesis: there is a null effect (also: H_0). We also formulate an alternative assumption, the alternative hypothesis, that is:

H_1: $T_{old} \neq T_{new}$

In words, the times to the conclusion of the new procedure and the old procedure differ. This assumption is also called the alternative hypothesis (also: H_1).

Now, assuming H_0 were true, we calculate the chances of finding our sample outcome. Suppose that that likelihood is very small, in order words: it is really unlikely to encounter such sample findings if H_0 were true, we then no longer assume that H_0 is true and we conclude that H_1 must be true. So, we conclude our findings are incompatible with the conclusion times being equal and the two divorce procedures' conclusion times differ.

While the statistical process may appear very abstract, as said, it is exactly the reasoning used in daily life. For instance, tossing a die 10 times, and each time finding the result of the toss being a six, would lead to the conclusion that the die is not fair. Eating at a canteen several times and falling sick each time would lead to the conclusion that unhealthy food is served there. In both examples, one is not 100% certain that this is the case. It is possible for a die to be tossed 10 times and each time a six ending on top, or, coincidentally, dinner at that canteen may coincide with a flu wave each time. Without measuring the die with a nifty device to see whether it is balanced, or without looking for bacteria in the restaurant food in a petri dish, we are not 100% certain of our conclusion.

We simply find it *too coincidental*. We accept a small risk to draw a wrong conclusion, namely that we conclude that H_1 holds, while actually H_0 is the case. That risk is called the *significance level*. Given that H_0 is formulated as the situation where nothing out of the ordinary is going on (no effect, no difference), this small risk – the significance level – is the likelihood of wrongly concluding that something interesting is going on when actually there is no effect or no difference (a false alarm). Significance levels of 5% are often regarded as acceptable, although this essentially depends on the risk a researcher wants to take in drawing a wrong conclusion here.

A researcher may wrongly conclude that H_1 is true while H_0 is actually true. But the opposite can also occur. If one is very risk-averse and sets the significance level very low (for instance, at 1% or 0.01%), one will simply never reject H_0. If a six was tossed 100 subsequent times and only then the unfairness of the die is assumed, one is so strict that one will almost never be able to conclude that the die is not fair. The test then has low *statistical power,* or briefly, low *power*: it is unable to detect that something out of the ordinary is going on. The power of a test is defined as the chance to decide that H_1 is true if it is true.

A good example to illustrate why statistical power is also important is a fire alarm. A fire alarm is calibrated to sound the alarm above a certain threshold of particles in the air. So, in that a sense it is like a statistical test. It cannot see whether there's a fire. It derives conclusions from sampling the air. Above a certain threshold, it will conclude that there is a fire and start sounding; below, it will remain silent. A false alarm can be very annoying. If one were to fiddle with the threshold (reducing the likelihood of a false alarm) this will the alarm to start screeching less soon. One then however increasing the likelihood of missing out on a fire, something much more problematic than annoying. The latter is the analogue of low statistical power: setting the significance level so low that one does not detect what is going on.

A large sample provides – ceteris paribus – larger power. In general, the chances of drawing the wrong conclusion on the population of interest are reduced when using a larger sample. This is quite logical. If one draws a larger sample out of the population of interest, one has observed a larger chunk out of that population and is therefore surer about what is going on in that population. This can be shown mathematically, but it is also intuitively so.

Much more can be said about statistical sampling. There are numerous kinds of tests and different ways to construct the null and alternative hypotheses, but for sake of brevity in this Chapter, I refer to general statistical textbooks and the non-technical introduction given in Bijleveld (2023, Chapter 7). Importantly, all testing follows the same rationale outlined here, and that that rationale is one we also often use in daily life.

5. Causality

In empirical legal studies, many questions centre around the impact of laws. Are cases concluded more swiftly because procedures were changed? Are rents down because of the new law restricting the rent that rental agencies may charge through a tariff system? Do female defendants get lighter sentences because they are female? These are causal questions. In each example, one would want to know not whether cases are concluded more swiftly before and after a law change but whether they are concluded more swiftly *because of* the law change. In the second example, it is not sufficient to establish that rents went down, what the research question points to is whether that was due to the new tariff system. For the last example,

the research question cannot be answered by establishing whether women receive lighter sentences than male defendants but it must be established whether that is due to their gender.

Pursuing the last example, a simple comparison of sentence lengths for men and women will not answer the question of discrimination. Men and women might commit different crimes, and this difference, in fact, explains any difference in sentence length. Even if we would compare sentence length for men and women within one type of crime only, different so-called *confounders* could be at play, making it impossible to infer anything about the effect of gender on sentence length. For instance, female defendants might be more remorseful, or more male defendants have a criminal record already, which translates to a heftier sentence for them.

The gold standard for assessing causality in empirical research is through an experimental design, where one randomly chosen set of research objects receives some kind of intervention, and another randomly chosen set does not. This type of design is often found in pharmacological research, where questions about whether medicine reduces complaints or vaccination protects against disease are determined. However, simply administering the intervention of interest to one group (the experimental group) and not administering it to the other group (the control group) is not enough to assure that any difference between experimental and control groups is attributable to the intervention. To make the experiment successful, the persons in either group should not be aware of which group they have been placed in, which is usually achieved by administering an empty intervention to the control group (a placebo). The COVID-19 vaccines were tested similarly: one group of randomly chosen volunteers received the real jab, and the other random half received a saline solution. However, in addition to the volunteers being unaware of the condition of the experiment in which they had been placed, the nurses administering the vaccination were unaware of its content and could not in any way unconsciously transmit that information. Such a study is called *double-blind*. This type of design is required to be able to validly conclude that a significant difference in COVID-19 prevalence between the two groups is due to the vaccination, in other words, that the vaccination works.

It will be clear to most readers that this experimental design setting is unrealistic when conducting empirical legal research. Law changes pertain to an entire country or union, and citizens are aware of the change. Also, in many settings, it would simply be impossible to randomise the intervention of interest. In the example above, we cannot randomise gender over court

cases: male or female citizens commit different crimes and have pertinent characteristics and behaviour that impact sentence length. Interviewing judges on whether they sentence male and female defendants differently is like asking them whether they act professionally in a breach of the constitution and is not likely to lead to valid responses.

In some instances, it is possible to investigate the impact of legally relevant phenomena using so-called *vignette studies*. In a vignette study, one presents a set of respondents with realistic but fictitious cases. For the example of gender effects on sentencing, such a vignette could be a police report or a court file in which a defendant has committed a violent crime. For a vignette, two versions of the court file are made: one in which the perpetrator is male and one in which the perpetrator is female. One distributes these different versions of the vignettes to judges and asks the judges what they believe an appropriate sentence would be. Now, the vignette is identical for the male and female defendants. No confounders are present that may explain differential sentencing: if a difference emerges between sentences for men and women, it can *only* be attributable to gender (and chance, obviously). By using testing, the likelihood of observing the sentence disparity by chance can be determined. If that likelihood is very small, we may conclude that gender indeed has an effect. A worked example can be found in Bijleveld et al. (2022). Van den Bos and Hulst (2016) discuss the possibilities and pitfalls of various kinds of experimental methods in empirical legal research.

6. Special topic: Systematic case law analysis

Systematic case law analysis is of particular relevance to ELS scholars. Hall and Wright (2008, p. 64) label it as a distinctly legal form of empiricism and state:

> Using this method, a scholar collects a set of document opinions on a particular subject, and systematically reads them, recording consistent features of each and drawing inferences about their use and meaning. This method comes naturally to legal scholars because it resembles the classic scholarly exercise of reading a collection of cases, finding common threads that link the opinions, and commenting on their significance.

In systematic case law analysis, one selects a sample (or an entire population) of opinions or court rulings, reads and codes the material, and searches to answer the research questions. Codes can be factual categories

such as *type of claim* or *gender of the litigant*, *chamber* or *background of the judge*, but they can also be derived from the material in the cases. Code selection using a large-scale systematic case law analysis is amply demonstrated in the well worked material by Wijntjens (2020).

Wijntjens' study investigated whether offering apologies to victims of harm by the party held liable for that harm induces the risk of being held liable in court. Offering apologies has been labelled as "legally dangerous" (Farmer, 2015, p. 244), as an apologetic statement may be admissible evidence at trial to establish liability or to prove some other element of an offence. Also, it has been noted that insurance companies may instruct the insured to be reticent in offering apologies and to speak only summarily and with great care on what happened, with mention made of lawyers even ordering their clients to remain silent (Cohen, 1999). Wijntjens (2020) studied to what extent the assumption that apologies might amount to an admission of liability in legal proceedings has an empirical basis in legal practice. The study employed systematic case law analysis, which differs from conventional legal analysis – in which issues are presented in one case or a small group of exceptional or weighty cases – in that it examines a large and representative group of cases to find overall patterns. As such, it aims to prove a claim not according to one author's rhetorical power but because the patterns that are found in case law have been uncovered through systematic and transparent empirical analysis of the rulings' content. Moreover, the data collection, data analysis and findings are reproducible.

The study selected court rulings from several databases with court rulings. Using keywords and by reading the rulings, Wijntjens arrived at a selection of 570 rulings in which apologies played a role. All texts were analysed and coded using a coding scheme that had qualitative and quantitative elements. First, the argumentative schemes that the judges used to arrive at their rulings were coded. Wijntjens coded whether apologies played a subordinate role, a conjunct role, or a decisive role in assessing the evidence on which the conclusion about the case would be based that the judge reached.

The results found that in very few rulings, apologies were decisive in the ruling. Out of all 570 coded and rulings analysed, only in seven judgments the court considered that the apologies of the person causing the damage as constituting an acknowledgement of liability. This amounts to 1.2%. Her findings clearly debunked the prevalent idea of the offering of apologies to be risky behaviour. Interestingly, the study also showed that withholding

apologies notably increased the risk of a negative outcome (Wijntjens, 2020).

7. Conclusion

This chapter could touch only very briefly on the various research methods available for empirical legal studies. While empirical research, and especially the more quantitative methods, may be relatively foreign to legal scholars, most are not very difficult to master. Experience teaches that both empirical and legal/doctrinal skills contribute to the production of sound empirical legal findings. Experience also teaches that empirical legal research is generally a journey of discovery, surprise and fun.

References

Bijleveld, C.C.J.H. (2023) *Research Methods for Empirical Legal Studies.* Den Haag: Eleven [Online]. Available at: https://elsacademy.nl/research-methods-for-empirical-legal-studies-an-introduction/ (Accessed: 9 February 2025).

Bijleveld, C.C.J.H., Blažević, M., Bociga Gelvez, D. and Buljubasic, M. (2022). 'Sanctioning Perpetrators of International Crimes: A Vignette Study'. *International Criminal Law Review*, 22, pp. 805-826.

Cane, P. and Kritzer, H. M. (2010) *The Oxford Handbook of Empirical Legal Research.* Oxford: Oxford University Press.

Cohen, J. R. 'Advising Clients to Apologize', *Southern California Law Review*, 72, pp. 1009-1069 [online]. Available at: https://ssrn.com/abstract=1612774 (Accessed: 14 January 2025).

Davies, G. (2020) 'The relationship between empirical legal studies and doctrinal legal research,' *Erasmus Law Review*, *2*, pp. 3–12.

Drost, E.A. (2011) Validity and Reliability in Social Science Research. *Education Research and Perspectives*, 38(1), pp. 105-124.

Dyevre, A. (2021) 'The promise and pitfall of automated text-scaling techniques for the analysis of jurisprudential change', *Artificial Intelligence and Law*, 29, pp. 239–269.

Farmer, C. (2015) 'Striking a Balance: A Proposed Amendment to the Federal Rules of Evidence Excluding Partial Apologies', *Belmont Law Review*, 2(243), pp. 243-267.

Hall, M. and Wright, R. (2008) 'Systematic content analysis of judicial opinions,' *California Law Review*, 96, pp. 63–122.

Haucke M., Hoekstra R. and van Ravenzwaaij D. (2021) *When numbers fail: do researchers agree on operationalization of published research?*, 8(9) [online]. Available at: https://doi.org/10.1098/rsos.191354 (Accessed: 14 January 2025).

Hutchinson, T. (2013) 'Doctrinal research: researching the jury' in Watkins, D. and Burton, M. (eds.) *Research methods in law*. London: Routledge, pp. 7-33.

Hutchinson, T. (2015) 'The Doctrinal Method: Incorporating Interdisciplinary Methods in Reforming the Law', *Erasmus Law Review*, 3, pp. 130-138.

John, L.K., Loewenstein, G., Acquisti, A. and Vosgerau, J. (2018) When and why randomized response techniques (fail to) elicit the truth. *Organizational Behavior and Human Decision Processes, 148*, pp. 101–123.

Tracy, S. (2013) *Qualitative Research Methods*. Chichester: Wiley.

Tyler, T. (1990) *Why People Obey the Law*. New Haven, CT: Yale University Press.

Van Boom, W. H., Desmet, P. and Mascini, P. (2018) 'Empirical legal research. Charting the terrain' in Van Boom, W. H., Desmet, P. and Mascini, P. (eds.) *Empirical Legal Research in Action. Reflections on Methods and Their Applications*. Cheltenham: Edward Elgar, pp. 1– 22.

Van Gestel, R. and Micklitz, H.-W. (2011) 'Revitalising Doctrinal Legal Research in Europe: What About Methodology?', in Neergaard, U., Nielsen, R. and Roseberry, L. (eds.), *European Legal Method – Paradoxes and Revitalisation*. Kopenhagen: Djøf Publishing, pp. 25-73.

Van Velthoven, B.C.J. (2016) 'A Young Person's Guide to Empirical Legal Research. With Illustrations from the Field of Medical Malpractice', *Law and Method*, April 2016 [online]. Available at: https://doi.org/10.5553/REM/.000016 (Accessed: 14 January 2025).

Van den Bos, K. and Hulst, L. (2016) 'On Experiments in Empirical Legal Research', *Law and Method*, March 2016 [online]. Available at: https://doi.org/10.5553/REM/.000014 (Accessed: 14 January 2025).

Webley, L. (2010) 'Qualitative approaches to empirical legal research', in Cane, P. and Kritzer, H. M. (eds.) *The Oxford Handbook of Empirical Legal Research*. Oxford: Oxford University Press, pp. 927–950.

Wijntjens, L. (2020) *Als ik nu sorry zeg, beken ik dan schuld? Over het aanbieden van excuses in de civiele procedure en de medische tuchtprocedure*. The Hague: Boom Uitgevers.

Searching for Harmonised Rules: Understanding the Paradigms, Provisions, and Pressing Issues in the Final EU AI Act

Hannah Ruschemeier & Jascha Bareis

Abstract

This analysis provides an overview of the enactment of the final European regulation about harmonised rules on artificial intelligence (AI Act). The AI Act establishes the first legally binding horizontal regulation on AI. The paper follows an interdisciplinary approach in combining legal scrutiny with political analysis in order to clearly define and explain the rationale, overall structure, and the shortcomings of the provisions. We understand the crafting of the AI Act as a reaction to the growing centralisation and power of non-European platforms in developing and providing AI systems, and the EU's geopolitical and normative aspirations to shape the adoption of this technology. Overall, this analysis seeks to familiarise researchers from other disciplines (from tech to policy) with the complex regulatory structure and logic of the AI Act. The analysis is structured into three major parts: first, analysing the regulatory necessity in introducing a coercive regulatory framework; second, presenting the Act's regulatory concept with its fundamental decisions, core provisions, and risk typology; and, lastly, critically analysing the shortcomings, tensions, and watered-down assessments of the Act.

1. Regulating AI: an introduction[1]

The enactment of the Regulation (2024/1689) about harmonised rules on artificial intelligence (hereafter, the AI Act), adopted on May 21, 2024 by the Council of the 27 EU member states, establishes the first legally binding horizontal act on artificial intelligence (AI). The adoption of enforceable and binding legal requirements relating to the regulatory subject matter of AI marks a milestone in the diverse development of normative require-

1 Many of the legal aspects were first developed in by Ruschemeier (2023).

ments for this nascent technology. Different institutions, and regulatory levels and subjects are involved in the discussion on normative requirements for AI. To date, no country has enacted a comprehensive legal framework for AI following a horizontal approach, and no international treaty providing uniform international guidelines is currently in force.[2] The international regulation of AI is more of a patchwork than a jigsaw puzzle, due to the different approaches of different states, associations of states, non-governmental organisations (NGOs), and other institutions, if only due to the variety of different competences (Ruschemeier, 2023b).

At first glance, AI is not an unusual subject for regulation: legal regulation in particular has always dealt with new technological developments, uncertainties, or global impacts, as exemplified by environmental and technology law. However, there is a growing international consensus that existing rules at different levels are insufficient for the effective regulation of AI. The reasons for this are manifold and lie in the socio-technical implications of AI, the wide individual, systemic, and residual risks that AI systems can embody, the power centralisation around a few developers and providers, and its ever-evolving technical specificities. Current legal and policy initiatives are faced with the difficulties of keeping pace with these challenges. From a regulatory and societal perspective, the dangers of AI systems grow in line with their use, as greater adoption can impact such protected interests as fundamental rights, democratic processes, inclusion, or public safety. These affected legal interests are not new and are not only threatened by AI applications. However, due to AI's growing pervasiveness in everyday spheres of life in the social, legislative, military, health, and intimate domains, regulators must be able to carefully weigh the risks and potentials.

Given this continuity of technological development, AI is not the *new* disruptive force befalling society suggested by certain private and public narratives (Bareis and Katzenbach, 2022). Rather, its uptake depicts a growing societal leaning on algorithmic automation, continuously reshaping human relationships, with new forms of intimacies (e.g., recommender systems in dating apps), social orders (e.g., the power of Big Tech in providing and controlling digital infrastructure), and knowledge authorities (e.g.,

2 Other countries, such as China or the US, have also forwarded AI regulatory initiatives, including the 2023 Chinese "Interim measures of the management of generative artificial intelligence services" or the 2023 US executive order on "Safe, secure and trustworthy AI". However, these interventions address only selective areas, and thus do not have the scope and depth of the horizontal and comprehensive AI Act.

societal trust in large language model (LLM) chatbots, such as ChatGPT, to provide *knowledge*). Unsurprisingly, such a cross-cutting technology as AI impact various areas of law, including product safety law, consumer protection law, copyright law, data protection law, protection of fundamental rights, private liability law, criminal attribution issues, and labour law. Thus, AI is by no means being used in a legal vacuum that now urgently requires new, detailed regulation in every area. For example, the Digital Services Act (DSA) (Regulation 2022/2065) does not explicitly mention AI, but aims to create a "safe and trustworthy" online environment, which is threatened by the way digital platforms operate (Art. 1 DSA). This includes the use of AI to display and moderate content (see, for example, the requirements for recommender system transparency in Art. 27 DSA).

The regulation of AI takes different forms: traditional legal regulation can define preventive prohibitions, repressive sanctions, or requirements to act. It can apply existing regulations or create new ones; early ethical proposals can relate to moral requirements, which can, however, become the basis for legal regulation; technical requirements, such as standardisation norms, often create de facto obligations (Veale, Matus and Gorwa, 2023). Consequently, the need for new legislation must be carefully assessed and, if laid open, regulatory gaps should be filled to meet regulatory objectives. For example, the GDPR (Regulation 2016/679)[3] is reaching its limits in terms of the regulation of data-driven technologies, such as predictive analytics or generative AI, since the regulatory object is the single data processing of data belonging to an identifiable data subject.

Through this chapter, we seek to familiarise researchers from other disciplines with the regulatory structure and key requirements of the AI Act, and to critically reflect and analyse the Regulation's fundamental decisions through our interdisciplinary approach. Our conceptual take to the AI Act combines sociological and political analysis with the legal scrutiny of the provisions, thus making the analysis fruitful to legal, policy, social, and technology scholars. To meet these aims, the analysis is structured into three parts:

- First, *Regulatory necessity* introduces the Act's inception. We open our analysis of the AI Act in recognition of the rise and perpetuation of larger power structures, attested to by the pervasive roll-out of AI through ecosystems of platforms and clouds controlled by a few international

3 For more information about the GDPR, see Chapter 14 'EU data protection law in action: introducing the GDPR' by Julia Krämer.

Big Tech companies (van der Vlist, Helmond and Ferrari, 2024). Given the global influence of US and Chinese tech companies in global AI development, we underpin our legal analysis with a short depiction of the EU's geopolitical and normative aspirations, which influenced the overall crafting of the AI Act.

- This larger political embedding of the AI Act leads us to the second part, *Regulatory concept of the AI Act.* This part presents the Regulation's core provisions in addressing the different scopes of application. Here, we also dive into the various risk-categorisations and their subsequent regulatory prescriptions, reaching from no restrictions to forbidden practices for market deployment.
- Finally, *Critical analysis* reflects upon the shortcomings, tensions, and watered-down assessments of the AI Act. We argue that these largely stem from the Act's overall conflictual aspiration to combine fundamental rights protection with a risk-regulatory assessment of harms for products, while simultaneously aiming towards a harmonised and internationally competitive and resilient common AI market.

2. Part I: Regulatory necessity

2.1 Regulating AI is regulating power

Common regulatory objectives for AI are often described as "fairness", "transparency", "explainability", "trustworthiness", "safety", "protection of fundamental rights", "sustainability" and "fostering innovation" (Hacker, 2018; Malgieri and Pasquale, 2024; Goh and Vinuesa, 2021; Stahl et al, 2022). However, further to these desirable and laudable goals, there is a further rationale to create new regulatory requirements for AI. The regulation of AI is the regulation of societal power, and thus a truly constitutional and public interest issue, because the rule of law serves to simultaneously legitimise and limit power (for a general overview, see Summers, 1998). Power dimensions in AI applications are manifold: the centralisation of infrastructure, AI models, and data appropriation in the hands of a few Big Tech players; the "black boxing" of AI systems, where people cannot understand, explain, or comprehend the path to a system's output which decides upon them; or the individual and highly systemic dangers that AI systems can cause without providers taking accountability (see also Guijarro Santos, 2023).

Firstly, the key players in AI technologies, who have urged state to take action and provoked the legal policy debate on AI regulation in the first place, are large global technology companies. The development and application of AI is not limited to the private sector: open source initiatives, NGOs, government institutions, and scientific research also play key roles in the development and dissemination of AI applications. However, the technologies dominating the market and discussed in public discourse are primarily those developed and deployed by private sector actors and are embedded in their platforms. Therefore, it would be vital to make transparent the purpose of the economic profit of these actors, who all too often foster a deregulatory agenda.

Despite the privatisation of AI, it is by no means impossible that many people (can) benefit from it, or that the technology could be used for the greater common good. However, pervasive power structures are created when states and users are forced to rely on private companies for the use of AI. The current structural dependency on Big Tech players for infrastructure provision, model development, maintenance, and auditing is creating lock-in effects. Indeed, as stated by Whittaker (2021, p. 35): "These companies control the tooling, development environments, languages, and software that define the AI research process – they make the water in which AI research swims". With the recent development towards foundation models – i.e., very large pre-trained models on which such popular applications as ChatGPT or Midjourney run – the centralisation of AI is increasing further (Burkhardt and Rieder, 2024; van der Vlist, Helmond and Ferrari, 2024). Big Tech use their platforms as bottlenecks in AI development and provision, assuming a gatekeeper position to certain apps. For example, the COVID-19 tracing apps could only be successfully launched through the Google and Apple app stores (Bock et al, 2020), or ChatGPT can only be used in the Open AI or Microsoft Azure ecosystems, following Microsoft's investments into Open AI. While the functioning of the tracking apps does not directly fall under the definition of AI under the AI Act (Art. 3 (1)), the risks to digital sovereignty through a heavy reliance on private digital infrastructures is transferable and growing with AI ecosystems. Currently, there are already discussions about the use and implementation of LLMs in the public sector. For instance, Microsoft announced its intension to implement generative AI in many Office 365 applications, a software which is heavily used by public authorities despite its non-compliance with the General Data Protection Regulation (GDPR) – indeed, it is generally perceived as too big to not use (Ruschemeier, no date; EDPS, 2024).

Secondly, the power dimension is present with these Big Tech companies executing data appropriation of users, essentially an *assetisation* of citizens with the lure of free-to-use services, a business model also called *service-for-profile* (Elmer, 2003; Mager, Norocel, and Rogers, 2023). Alphabet (Google's parent company) collects data on the behaviour of users of its various services, allowing it to build detailed profiles and predictions of consumer preferences. These sensitive data can then be sold to third parties and advertisers (Ridgway, 2023). Meta (formerly Facebook, Inc.) personalises its algorithm to display content and collects data to an extent to which users are generally unaware (Arias-Cabarcos, Khalili and Strufe, 2023). Hence, these private players exploit extremely large user bases to fuel and train their AI models to offer service for *free*. This endows them with considerable predictive power, having insights in the most intimate, sensitive social and political spheres – which is historically unprecedented for the private sector – ranging from highly sensitive information, such as creditworthiness, to sexual orientation or health status (Mühlhoff, 2023; Ruschemeier, 2024a; Mühlhoff and Ruschemeier, 2024a; Ruschemeier, no date). Often, consent is not even requested: Open AI's ChatGPT only works as well as it does because it was developed by trawling almost the entire internet for publicly available information on which to train its model (Ruschemeier, 2023c). The European Court of Justice (ECJ) recently ruled that Facebook's business model – namely, financing through individualised advertising – does not in itself constitute a legitimate interest in the mass processing of personal data (Meta v Bundeskartellamt, 2023).

Thirdly, the ubiquity of these digital processes and the proliferation of AI also carry epistemological implications: how are decisions that govern over people procedurally made? How can they be contested? How is knowledge generated and given authority (Ruschemeier, no date; Hong, 2020)? Such production of the perception of knowledge is a pervasive exercise of epistemic power, with users granting excessive trust in machine-based decision suggestions (Ruschemeier, 2023d; Hondrich and Ruschemeier, 2023). Empirical studies have shown that users do so even if they know nothing about the underlying training data or, perhaps more gravely, if they are aware that they are confronted with a biased AI (Krügel, Ostermaier and Uhl, 2022). LLMs provide eloquent sounding answers, and have been pervasively hyped as knowledge models (indeed, ChatGPT's slogan reads: "Ask me anything!"), intentionally leaving the functionality of the probabilistic models working with tokens, and not hermeneutically with meaning, in the dark. (Bareis, 2024). Probabilistic models process data based

on statistical likelihood. These models have no *understanding* of neither the prompts nor outputs they generate, and can thus generate nonsensical content (termed "hallucinations") (Metz, 2023). Moreover, this publicly produced misconception leads to a crisis of knowledge, as synthetically generated content is currently flooding the internet and is being indexed as "knowledge" by search engines. This provokes an epistemological crisis. As argued elsewhere, this could lead to our inability to identify trustworthy information even when we find it (Bareis, 2023c).

The business models, structural dependencies, socio-technical interactions, and, not least, the pervasiveness of scale described above mean that previous regulatory approaches are no longer effective in all cases. Where power is involved, the potential for social improvement is as obvious as the risk of abuse. According to the precautionary principle, certain particularly risky products and processes may be preventatively subject to legal regulation if they threaten important legal and public interests (Sandin, 1999). As with any transformative technology, it has often been argued that the challenge with AI is that some impacts are difficult, impossible, or even unknowable to foresee. However, with these pervasive societal effects of AI already present (and, indeed, known) this argument should not exempt politics from accountability. The law-lagging moment with AI is politically produced and a well-studied case (Doezema and Frahm, 2023). The precautionary principle gives politics the mandate to intervene in the name of public interest. Law must not socially be lagging, but leading.

2.2 EU taking a stance in the geopolitical AI arena

In recent years, a number of initiatives have emerged globally to define values and principles for the ethical development and use of AI. A multitude of international and supranational bodies, such as the Organisation for Economic Co-operation and Development (OECD, 2019), have proposed principles for standards of "trustworthy" AI. Likewise, the United Nations (UN, 2023) published the "Governing AI for humanity" report in late 2023. These reports are mostly based on abstract ethical principles useful for providing orientation on the safeguards, rights, and principles deemed to be protected in the international realm. Still, non-binding recommendations, policy papers, soft law, or ethical principles are often criticised for being ineffective because they are non-binding and therefore unenforceable (Mittelstadt, 2019). So far, the private sector, dominated by US Big

Tech companies, has largely ignored all proposals and lobbied aggressively against regulation, which also became very visible in the final phase of the European AI Act legislative process (Bareis, 2023a; Ruschemeier and Mühlhoff, 2023). Hence, ethical principles give normative orientation, but can quickly be watered down and often lack teeth.

The strivings of the European AI Act are embedded in a global AI race, with nations and their companies identifying AI as a core present and future enabler technology. Moreover, the EU envisions that AI shall transform the common internal market into an international competitive player, competing over global market shares and innovation (Krarup and Horst, 2023; Paul, 2023; Smuha, 2021). States approach AI not as a mere technology, but also as a strategic asset in the geopolitical positioning against rivalling economic (and military) actors, such as China, or the US and their Big Tech companies (Bächle and Bareis, 2022; Bächle and Bareis, 2025; Kello, 2017). When discussing the formation of the AI Act, it should be kept in mind that its formation falls into a global paradigm where tech policy has been highlighted by states as a pivotal realm to advance and harness sovereignty and a claim to first mover clout (Broeders, Cristiano and Kaminska, 2023).

The "European way" of tech-policy is subsumed by the European Commission (EC) as a necessity for achieving its own tech sovereignty. The Council of the European Union defines this strategic autonomy as the "ability to act autonomously when and where necessary and with partners whenever possible" (Mogherini, Timmermans, and Domecq, 2016, p. 4). EC president Ursula von der Leyen referred to this paradigm of strategic autonomy through stressing that: "Tech sovereignty describes the capability that Europe must have to make its own choices, based on its own values, respecting its own rules" (European Commission, 2020a). These statements echo endeavours of a de-risking strategy, essentially acknowledging the fragile balancing act of protecting Europe's AI market without retreating into a paradigm of protectionism in questions of economic trade, sensitive technology exchange, and military development (Rodríguez Codesal, 2024). In this context, the "European Chips Act" (European Commission, 2023) is situated with the proclaimed aim to support Europe's AI infrastructure, subsidising the European semiconductor industry and encouraging companies to invest so as to decrease dependencies on Taiwan, the US, Japan, or China.

For the EU especially, which is a supranational entity unifying 27 sovereign member states under the principle of subsidiarity (Art. 5 (3)

TEU), the harmonisation of standards and policy is a complex and lengthy process. The significant efforts and prioritisation of the EC, which hails itself as the first "geopolitical Commission" (von der Leyen, 2019) to tackle the AI Act, can also be understood as a reaction to the tedious EU constitutional integration process that was substantially gridlocked. The then-curtailed treaty of Lisbon was marked by a multitude of obstacles in the ratification process in the early 2000s, complicating further constitutional integration from an inward union perspective. Hence, on constitutional, military, and geopolitical stances, the EU's power is limited in finding joint positions and reacting quickly and effectively. It is rather by the power of "commanding the weight of the internal market" that the EU can execute "regulatory power in the international domain" (Broeders, Cristiano and Kaminska, 2023, p. 1265). In market policy questions, European integration is, as historically grown from its foundation of a coal and steel community (ECSC), the deepest, with clear delegated roles and coercive power for EU institutions. It is this context where the DSA, DMA, and AI Act are embedded, attempting to strengthen the unity of the European member states with a common AI rule book in order to meet a geopolitical competitive environment. Whether the so-called "Brussels effect" – that is, the hope that EU's AI regulation will have the desired impact on the global diffusion and standard-setting beyond its own borders (Siegmann and Anderljung, 2022) – remains to be seen.

2.3 Coming into being: from ethical guidelines to legal regulation

Next to these imperatives of an *outward* international competitive situation for AI market shares and the political aim for *inwards* legal harmonisation against fragmented national policy, the EU sees itself as a proponent of safeguarding consumer protection within the single market and the fundamental rights of individuals.

This very normative pillar of the EU's self-identity is legally enshrined with the EU charter of Fundamental Rights. Additionally, the ethical alignment is evidenced by the AI's framework of "human-centric ethics", "fundamental rights impact assessment" (see Section 3, below) and the fashion-

ing of *trustworthiness* throughout the European AI documents.[4] Although the ethical considerations are non-binding and not passed via a democratic process, they have influenced the roadmap of AI legislation. Here, the role of high-level ethics groups in sketching the path for AI legislation is particularly noteworthy. The principle setting by expert groups is an important trajectory in understanding how the coercive AI Act came into being. The European Group on Ethics in Science and New Technologies (EGE) published a report (EGE, 2018) on "Artificial intelligence, robotics and 'Autonomous Systems'", calling "for the launch of a process that would pave the way towards a common, internationally recognised ethical and legal framework for the design, production, use and governance of artificial intelligence (...)". In a clearly prescriptive call, the EGE "urges the European Union to place itself at the vanguard of such a process and calls upon the European Commission to launch and support its implementation" (2018). Frahm and Schiølin (2023) understood these early AI ethics reports by convening expert committees as instruments of socio-technical sense-making and ordering of the EU's position on AI, as well as the rise of the principle of "European technological sovereignty", which the EUC henceforth embraced. The subsequent adherence to AI ethical principles and values subsumed under the notion of a "trustworthy AI ecosystem" were adopted by the High-Level Expert Group (HLEG) on AI in 2019 (AI HLEG, 2019) and normatively underpinned the formation of the AI Act.

It is not only in the field of AI that legally binding requirements and ethical proposals influence each other as different dimensions of normativity: ethical standards are based on the legal system, while the law translates ethics into enforceable requirements (Ruschemeier and Mühlhoff, 2023). For example, the HLEG's "Ethical guidelines for trustworthy AI" advance three central criteria that all AI systems should fulfil: legality, ethical compliance, and robustness.[5] At the national level, the German Data Ethics Commission proposed a risk-adaptive regulatory approach in its report (Datenethikkommission, 2019) on algorithmic systems, which is now being implemented in a similar form at the European level.

4 For example, the 2020 Assessment List for Trustworthy AI (ALTAI) (European Commission, 2020b) or the 2020 white paper issued by the EUC (European Commission, 2020c).

5 However, trust is not actually defined in any of the EU documents, which neither reflect whether "trust" is actually the correct term or a conceptual misfit in this context (Bareis, 2024).

In the AI Act, the focus now lies on the protection of health, safety, and fundamental rights, while there are almost no references to ethical guidelines left in the binding part of the Act. Indeed, only Art. 60(3) requires that the testing of high-risk systems in real world conditions should be made without prejudice to any ethical review required by Union or national law, which is a special provision for supporting innovation via regulatory sandboxes. The second mention of ethical considerations can be found in Art. 95, which outlines codes of conducts with specific, but voluntary, requirements. These voluntary guidelines can include applicable elements provided for in Union ethical pillars in order to establish "trustworthy AI" (Art. 95(2) AI Act). Beyond the explicit mentioning of ethical guidelines, the AI Act no longer includes specific ethical considerations, instead remaining silent on value aspects. There remain many open normative questions that wait for instantiation and concretisation. For example, when are biases in AI systems problematic (following which understanding of anti-discrimination?), or what makes an AI system really "fair" (given the myriad contradictory fairness principles) or "trustworthy" (can technology be trustworthy at all, or just reliable?) (see discussions in Bareis, 2024; Laux, Wachter and Mittelstadt, 2023; Orwat et al, 2024; Wong, 2020)?

Despite the provisions, however, the recitals explicitly point out the objective of promoting the European human-centric approach to AI and stress the Union's goal to be a global leader in the development of "secure, trustworthy and ethical AI", as stated by the European Council. It ensures the protection of ethical principles, as specifically requested by the European Parliament (Recital 8). Recital 27 refers and explains the ethical guidelines for trustworthy AI developed by the HLEG (human agency and oversight; technical robustness and safety; privacy; data governance; transparency; diversity, non-discrimination and fairness; societal and environmental well-being; and accountability). The recital states that: "Without prejudice to the legally binding requirements of this Regulation and any other applicable Union law, those guidelines contribute to the design of coherent, trustworthy and human-centric AI, in line with the Charter and with the values on which the Union is founded". However, it should be noted that these recitals do not form part of the Regulation's bind text, but are rather used for interpretation and guidance. Some obligations for high-risk systems *can* be linked to the ethical considerations, such as the provisions on human oversight or data governance. However, these will ultimately be specified by the private standardisation organisations (for a more detailed discussion, see Sections part III, 3, 3.1). Recital 28 also

refers primarily to codes of conduct, although, again, these can be used on a voluntary basis. Despite being explicitly mentioned, the impact of the ethical guidelines as an interpretative guide is rather limited. It is striking how little of the ethical pillars, initially greatly stressed by the HLEG, is left in the final AI Act and incorporated into binding law.

3. Part II: Regulatory concept of the AI Act

The following section introduces the regulatory concept of the AI Act by explaining its regulatory structure (3.1), the scope of application (3.2), the important categories of forbidden and high-risk systems (3.3), and the oversight and governance structure (3.4).

The AI Act constitutes a legislative act of the EU in the form of the Regulation (Art. 288(2) TFEU). From this, it follows that the normative provisions are entirely binding and directly applicable in all Member States. EU regulations take precedence over national laws in case of conflict. Most aspects of the AI Act are fully harmonised, but there are opening clauses for the Member States, such as on the prohibition of certain systems under national law.

3.1 Regulatory structure

The general goal of the AI Act is to set harmonised rules for the development, use, and marketisation of AI in the European single market. Its regulatory aim is described as:

> ... to promote the uptake of human centric and trustworthy artificial intelligence (AI) while ensuring a high level of protection of health, safety, fundamental rights as enshrined in the Charter of Fundamental Rights of the European Union (the "Charter"), including democracy, the rule of law and environmental protection, to protect against the harmful effects of AI systems in the Union, and to support innovation. This Regulation ensures the free movement, cross-border, of AI-based goods and services, thus preventing Member States from imposing restrictions on the development, marketing and use of AI systems, unless explicitly authorised by this Regulation. (Recital 1, AI Act)

The explicit reference to health and safety shows how the Act is mostly a product safety regime with additional references to fundamental rights due to its heavy references to the harmonised framework of product safety law

in the EU, especially the New Legislative Framework[6] (NLF) (European Commission, 2008). Consequently, the AI Act is part of a larger package to further regulate product safety for AI and other products, such as the new Machine Regulation (Council of the EU, 2023) or the Toys Directive (Directive 2009/48/EC)).

Furthermore, the AI Act is part of the Commission's digital strategy (European Commission, 2024), which includes other important legislative acts, such as the DSA and the Digital Markets Act (DMA). While its legislation was mostly parallel to the discussion and enactment of the DSA and DMA, the latter two regulations are fundamentally different. The DSA and DMA aim to regulate such intermediaries as social media platforms and search engines in the digital sphere, and create special obligations for very large online platforms and search engines, such as Meta, Instagram, TikTok, Bing, and Google (see Art. 33 et seq. and Art. 3 DMA addressing "gatekeepers"). The AI Act, on the other hand, does not primarily address Big Tech players, but rather focuses on public sector applications, (cf.[7] Annex III). This raises the question of whether the Regulation sufficiently addresses the power aspects of private actors. Additionally, the AI Act does not specifically consider the position of the actors, unlike the regulatory categories of "very large online platforms" (DSA) or "gatekeepers" (DMA), but regulates regarding contexts of use, such as AI systems for public services or law enforcement. The particular relationship of the AI Act towards other legal acts on the Union level has yet to be fully clarified, however, it is important to note that the Act will not replace the GDPR, but will have significant overlaps when AI systems process personal data. Art. 2(7) states that Union law on the protection of personal data, privacy, and the confidentiality of communications applies to personal data processed in connection with the rights and obligations laid down in the AI Act, which shall not affect the GDPR.

The AI Act follows a risk-based regulatory approach and the creation of a horizontal (as opposed to sectoral) legal framework. From this, AI systems are to be classified into four risk categories: unacceptable (Art. 5), high (Art. 6, 7, Annex III), low (Art. 50), and systemic (Art. 52) for the category

6 NLF refers to a revision and harmonisation of technical standards for the internal union market. It addresses market surveillance, accreditation, conformity assessments, and labelling (e.g., CE marking). After more than 20 years, the "New approach" was revised and updated, with the so-called NLF adopted in 2008. It came into force in January 2010 (European Commission, 2008).

7 cf. stemming from Latin *confer*, meaning "compare".

of general-purpose AI systems. Depending on the risk classification, different obligations for providers and deployers apply. On the one hand, very low risk systems, such as email spam filters, are not subject to regulation. On the other, unacceptable risk systems, such as manipulative AI, social scoring, and remote biometric identification are banned, the latter of which is subject to broad exemptions for judicial and law enforcement authorities (cf. Art. 5 AI Act). Practically speaking, high-risk systems represent the most important category, since the majority of the Act's provisions address them. The Commission assumes that 5–15% of the AI systems on the market will fall under the high-risk category (European Commission, 2021).

The AI Act has 13 chapters and follows the classical formation of a European regulation starting with general provisions (I), followed by the prohibited practices (II), standards for high-risk systems (III), transparency obligations (IV), general-purpose models (V), measures in support of innovation (VI), governance (VII), requirements for the EU database for high-risk systems (VIII), post market monitoring and market surveillance (IX), codes of conduct (X), delegation of power (XI), confidentiality and penalties (XII) and, lastly, final provisions (XIII).

3.2 Scope of application

The scope of application of the AI Act is divided into the territorial and material scope of application, following the requirements from article 2 of the Act.

3.2.1 Material scope of application

Firstly, the AI Act's material scope must apply. The material scope describes the subject matter of regulation, such as the regulatory objects (AI systems and models) and actions (putting an AI system on the market). It can be limited by exceptions. The material scope of application of the AI Act includes placing AI systems on the market or putting them in service. While AI as a regulatory object is disputed, the definition of an AI system in Art. 3(1) requires levels of autonomy and outputs that influence physical or digital environments (see the critical discussion of the term AI system in section C I). As such, this rather broad definition includes many AI systems based on machine learning (ML), or simpler algorithmic decision-making systems (ADMs).

3.2.2 High-risk classification as the relevant regulatory definition

Considering the Act's overall structure, most of its provisions address high-risk systems. Perhaps counterintuitively, the relevant regulatory definition for the material scope is the high-risk classification (cf. Art. 6, 7, Annex III AI Act) or prohibition in Art. 5 and the general-purpose qualification (Art. 51) instead of the actual definition of the AI system. According to the Act, placing an AI system on the market involves first of all making the system or general-purpose AI model available on the Union market (Art. 3(9)). Here, a system is put into service for customers when it is supplied for first use directly to the deployer or for its own use in the Union for its intended purpose (Art. 3(11)).

AI systems can be classified as high-risk under Art. 6 in two ways: first, when they are products or safety components of products covered by the Union harmonisation legislation (detailed in Annex I), and, second, due to their relevance for possibly infringing on fundamental rights regarding the context of use (covered by Annex III). The reference to Union harmonisation legislation in the area of product safety law in Annex I itself is subdivided into Sections A and B. Section A refers to the NLF, while Section B refers mostly to vehicle and traffic provisions, such as the regulation on the approval and market surveillance of two- or three-wheel vehicles and quadricycles (Annex I B(14)). These harmonised rules are not part of the NLF, but part of the older Union legislation which follows the concept of detailed harmonisation, and can thus not be easily synchronised with the new AI Act. Most of the requirements of the AI Act do not apply to products under the old regulatory regime, as the old regime and the NLF follow fundamentally different approaches and metrics for product safety regulation – e.g., the old concepts established only government standards and the review of requirements by government agencies. This creates friction with the requirements of the AI Act, which is largely based on newly implemented standards established through private standardisation organisations, internal conformity assessment procedures, or procedures of a private notifying body (cf. Art. 43 et seq.). Art. 2(2) thus states that, for these systems under the old regime, only Art. 6(1), Art. 102–109, and Art. 112 apply. Art. 6 lays down the classification of high risk systems, while Art. 102 et seq. are final provisions amending other regulations and directives. Art. 57 sets the requirement to establish regulatory sandboxes for the testing of AI systems and applies only insofar as the requirements for

high-risk AI systems under this Regulation have been integrated in that Union harmonisation legislation.

3.2.3 Exceptions in the material scope

There are several exceptions in the material scope of the AI Act applications. Art. 2 names some of them: AI systems and models that are specifically developed and put into service for the sole purpose of scientific research and development are not covered by the regulation. In the EU rationale, this is because the aim of the AI Act is to foster innovation and support research. Recital 25 explicitly states that the AI Act shall not affect research or scientific freedom. The prerequisite for this exception is that the models are specifically developed and used for the sole purpose of research, which naturally leaves room for interpretation, given that many commercial start-ups in the AI sector stem from, or are connected to, university research. Furthermore, private funding for AI university research by Big Tech is especially prevalent in the Anglo-American context, but also increasingly in Europe, with Meta, for example, financing an AI ethics centre at the technical university of Munich (Kreiß, 2019). Moreover, training data for scientific research is often taken from the public rather than from research, such as with ChatGPT or other LLMs being trained on online content. As it stands, the private research departments of the Big Tech companies that aim at developing and improving products may not fall under the definition of solely research purposes, but how the AI Act applies in detail here remains to be seen in practice.

Beyond science, the AI Act does not apply to product-oriented research, testing and development activity regarding AI systems or models prior to those systems, and models being put into service or placed on the market (Art. 2(8)), except for testing under real-world conditions as part of the regulatory sandboxes of Chapter VI. Regulatory sandboxes are a testing environment for AI systems, such as finance apps and other applications, that can, for instance, affect customers. The AI Act defines regulatory sandboxes as controlled frameworks established by competent authorities which offer (prospective) providers of AI systems the possibility to develop, train, validate, and test innovative AI systems, where appropriate in real-world conditions, pursuant to a sandbox plan for a limited time under regulatory supervision (Art. 3(55)) (Ruschemeier, 2024b). Consequently, the training of AI systems and models does not fall within the scope of the AI Act. Additionally, the Act does not apply to obligations of deployers who are

natural persons (humans, not legal entities) using AI systems in the course of a purely personal non-professional activity, since these are understood as typically low risk, and thus not subject to regulation.

The AI Act excludes AI systems that are released under free and open-source licences unless they are placed on the market or put into service as high-risk AI systems or those which fall under Art. 5 or 50. Art. 5 regulates the forbidden AI systems that pose unacceptable risks and are therefore prohibited, while Art. 50 lays down transparency obligations for providers and users of certain AI systems and general-purpose AI models. The provisions on the latter have been implemented very late in the legislative process as a reaction to the rising popularity of generative models running chatbots, such as ChatGPT. Art. 3(63) defines a general-purpose AI system as:

> an AI model, including where such an AI model is trained with a large amount of data using self-supervision at scale, that displays significant generality and is capable of competently performing a wide range of distinct tasks regardless of the way the model is placed on the market and that can be integrated into a variety of downstream systems or applications, except AI models that are used for research, development or prototyping activities before they are placed on the market.

The exception for open-source systems is rightfully limited to those that are not prohibited or general-purpose AI, deepfakes, and those interacting with natural persons (Art. 50). Nevertheless, excluding open-source models from the legislation should not obscure the fact that these models can also harbour risks, e.g., when used in Annex III contexts (Mühlhoff and Ruschemeier, 2024d).

Finally, it is worth noting that the Act entirely excludes the military application of AI. This is a striking omission given the dual-use applicability of civil/military AI innovation and the research capabilities and use of AI in the military sector – as seen with the unhalted development of autonomous weapon systems (Bhuta, Beck and Liu, 2016). Especially in the US, state agencies cooperate with major technology corporations contributing to national military and intelligence imperatives. This is also the case with some European states (Germany, France, Spain), who cooperate with the private sector and heavily invest into military AI with the development of the European Future Combat Air System (FCAS), aiming to develop "combat clouds" with the implementation of communication hubs or real-time data analytics for synchronising their military forces (see Ernst, forthcoming).

Given the fragile current world political situation, military supremacy is trending high on many national geostrategic security agendas. The global regulatory debate on autonomous systems is being held at the UN Convention on Certain Conventional Weapons (CCW), where the compliance to International Humanitarian Law applies, but is currently gridlocked (Bächle and Bareis, 2022). EU Member States seemingly do not want to relinquish control of military AI use to the EU, thus leaving a significant loophole for unchecked AI development and use.[8]

3.3 Personal scope of application

The AI Act addresses different entities in the AI lifecycle (Art. 2(1)). Firstly, it applies to providers of AI systems that are placing them on the market or putting them into service (Art. 2(1a)). Secondly, it addresses deployers, providers, importers and distributors, product manufacturers, authorised representatives of providers, and affected persons (Art.22 (1) a–g). Thirdly, obligations also extend to importers and distributors (Art. 23–27) in a manner akin to the product safety regime, aiming to prevent dangerous products manufactured outside the EU from entering its market. Nonetheless, the primary actor upon whom these obligations are imposed is the provider (Edwards, 2022c).

3.4 Territorial scope of application

Akin to the GDPR, the AI Act follows the domestic-market principle (Koloßa, 2020), meaning that it applies to placing AI models on the EU market, regardless of whether the providers are established or located within the Union or in a third country (Art, 2(1a)). Furthermore, it is already sufficient that the output of the AI system is used in the Union when providers and deployers of systems are located in a third country for Art. 2(1c) to be

8 A detrimental use of current military AI can be witnessed in the Gaza strip, where the Israel Defense Forces (IDF) are using AI in the military operations in Gaza following Hamas's terrorist attack of 7 October, 2023. Investigations about the "Lavender" and "Habsora" scoring system show how target recommendation of "militant suspects" is automated by the IDF, and air strikes are largely conducted without a human in the loop (Abraham, 2024). This has caused gross human rights violations in the massive bombing of the Gaza strip. The case strikingly shows that AI recommender systems being largely applied in the public domain can also be used for military purposes.

applicable. Following this, the relevant data (e.g., to train the AI system) can be processed outside the Union, as long as the results of the system are used within the single market. Additionally, the AI Act applies to deployers of AI systems established or registered within the Union (Art. 2(1b). Even if this wording is misleading, the scope of application with regard to users only refers to the spatial boundaries of the 27 Member States (Gless and Janal, 2023, p.30). The establishment refers to the deployers rather than to the AI systems, meaning that the former must be within the Union. Art. 3(4) defines a deployer as a "natural or legal person, public authority, agency or other body using an AI system under its authority except where the AI system is used in the course of a personal non-professional activity". As such, this broad definition of the scope is convincing as AI is a digital technology whose impact does not stop at national borders.

4. Forbidden high-risk systems and systemic risks

The AI Act establishes different levels of regulatory measures according to the risk classification of the system. Art. (5) prohibits the use of certain systems (4.1), Art. 6 classifies high-risks systems (4.2), and Art. 50 et seq. establish specific provisions for general-purpose AI systems (4.3).

4.1 Prohibited AI practices

Art. 5 prohibits certain types of AI systems which can be classified into eight categories: 1) subliminal techniques, 2) exploitation of vulnerabilities, 3) social scoring, 4) person-based predictive policing, 5) the creation of facial recognition databases via untargeted scraping, 6) biometric categorisation systems, 7) the emotional recognition systems in the workplace, and 8) real-time biometric identification.

First, the putting into service or use of an AI system that deploys subliminal techniques beyond a person's consciousness, or purposefully manipulative or deceptive techniques are forbidden. The term "subliminal techniques" is itself problematic, since there is no clear evidence or history of non-valid experiments in this field (Neuwirth, 2023). These techniques should include the objective or effect of materially distorting the behaviour of a person or group of persons by appreciably impairing their ability to make informed decisions, thereby causing them to take decisions they

would otherwise not have taken. This refers to the reasonable likelihood to cause that person, another person or group of persons, significant harm (Art. 5(1a). Recital 29 names audio, image, and video stimuli that persons cannot perceive (by being beyond human perception), or other manipulative or deceptive techniques that subvert or impair a person's autonomy, decision-making, or free choice in ways that people are not consciously aware of or, where they are aware of them, can still be deceived or are unable to control or resist them as examples for subliminal techniques. Concrete facilitation could be by machine-brain interfaces or virtual reality as they allow for a higher degree of control of what stimuli are presented to persons, insofar as they may materially distort their behaviour in a significantly harmful manner (Recital 29). Another concrete example of concerns resulting from subliminal and supraliminal messages in the field of cybersecurity are the so-called "social engineering attacks", such as phishing, that refer to means of "manipulating people into performing actions or divulging confidential information" (Neuwirth, 2023).

Secondly, systems that exploit any of the vulnerabilities of a natural person or a specific group of persons due to their age, disability, or specific social or economic situations, with the objective, or effect, of materially distorting their behaviour in a manner that causes (or is reasonably likely to cause) significant harm are prohibited under Art. 5(1b). The "Unfair commercial practices directive" establishes a similar provision (art. 5 UPD; Directive 2005/29/EC). Regarding the AI Act, the specific characteristics exclude other characteristics, such as race, sex, religion, or ethnicity. Smuha et al (2021) suggested expanding these to all of the characteristics protected under EU equality law as laid down in Art. 21 of the EU Charter on Fundamental Rights. It is not yet clear which specific practical examples are included. The specific exploitation of vulnerability leading to a change in behaviour may already be the purchase of an overpriced product or, for example, in-app purchases of video games for children. In general, the secondary use of sensitive data, such as health or other data relating to the specific vulnerabilities for commercial purposes is highly problematic (Mühlhoff and Ruschemeier, 2024c, 2024d). In these cases, however, it is questionable whether, for example, financially disadvantageous purchases fall under the concept of significant harm, which may only be assumed in the area of criminal disproportionality.

Third, systems for social scoring are prohibited under Art. 5(1c). Social scoring systems are used to evaluate or classify natural persons or groups over a certain period of time based on their social behaviour or known, in-

ferred, or predicted personal or personality characteristics. The social score leads to either or both of the following: (i) the detrimental or unfavourable treatment of certain natural persons or groups of persons in social contexts unrelated to the contexts in which the data were originally generated or collected; and (ii) the detrimental or unfavourable treatment of certain natural persons or groups of persons that is unjustified or disproportionate to their social behaviour or its gravity. The practical reference is China's social scoring system, where camera surveillance, consumer data analytics, and geo-tracking are used to form a disciplining scoring system (Qian et al, 2022). Scoring systems with different characteristics are also used by other countries, such as in the UK's (UK Parliament, 2021) concept of digital identity. During the legislative process, the prohibition was extended to private actors. Risk-scoring practices by private actors are essentially ubiquitous, ranging from the calculation of healthcare insurance premiums to creditworthiness scoring (Citron and Pasquale, 2014). Here too, the regulatory hurdle is again the consequence of these practices, which on the one hand must be proven and on the other unjustified. The associated Recital 31 does not state any use cases or concrete examples.

The fourth prohibition addresses predictive policing techniques related to natural persons in order to assess or predict their risk of committing a criminal offence, based solely on the profiling of a natural person or on assessing their personality traits and characteristics. As per Art. 5(1d), this prohibition shall not apply to AI systems used to support the human assessment of the involvement of a person in a criminal activity, which is already based on objective and verifiable facts directly linked to a criminal activity.

As a reaction to the business practices of Clearview and other facial recognition databases not compliant with the GDPR (Pathak, 2022), but still hard to come by because of the structural enforcement deficits towards malicious actors, Art. 5(1d) prohibits systems that create or expand facial recognition databases through the untargeted scraping of facial images from the internet or CCTV footage. Clearview and PimmEyes have illegally, and essentially secretly, scraped social media platforms and many other websites for images of faces to build huge databases for the private use of facial recognition. These databases can be used by any individual and by public authorities for a certain fee to identify almost every person whose picture can be found online – indeed, as of 2021, the Clearview database contained 10 billion pictures (Dul, 2022). Accordingly, these business practices aim at abolishing any privacy and personal integrity. Persons

can be easily identified with AI-powered facial recognition technology, where uploaded pictures of individuals show results within seconds, including links to the websites from which the pictures were scraped (Hill, 2022; Rezende, 2020).

The sixth prohibition includes the use of AI systems to infer a natural person's emotions in the workplace and educational institutions, except where the use of the AI system is intended to be put in place or into the market for medical or safety reasons (Art. 5(f)). Emotion recognition systems are designed to measure, for example, whether content has been understood by students or whether employees are productive and satisfied. The reliability or even effectiveness of emotion recognition systems has yet to be scientifically demonstrated (Heaven, 2020). It is therefore welcome that the AI Act bans these systems, at least in the context of work and training – but their general use remains questionable. Human emotions should not be used for performance reviews, as their scoring depicts a strong risk of abuse (see above with the "Clearview" case).

The seventh prohibition includes the use of biometric categorisation systems that individually categorise natural persons based on their biometric data to deduce or infer their race, political opinions, trade union membership, religious or philosophical beliefs, and sexual lives or orientation. This prohibition does not cover any labelling or filtering of lawfully acquired biometric datasets, such as images, based on biometric data or the categorising of biometric data in the area of law enforcement (Art. 5(1g)).

Finally, the eighth prohibition includes the use of "real-time" remote biometric identification systems in publicly accessible spaces for the purposes of law enforcement (Art. 5(1h)). The scope of the ban on biometric recognition systems was one of the most debated issues in the legislative process, and is beyond the scope of this paper (see, for example, Edwards, 2022a; Barkane, 2022; Veale and Borgesius, 2021). Biometric surveillance systems carry a high risk of mass surveillance, including those used for social scoring and predictive policing, as discussed above (Wendehorst and Duller, 2021). Art. 5 names a broad number of exceptions of the use of biometric systems in publicly accessible spaces for different objectives of law enforcement, which render the scope of application of the actual prohibition very narrow (Ebers et al, 2021). These exceptions include: (i) the targeted search for specific victims of abduction, trafficking, or sexual exploitation of human beings, as well as the search for missing persons; (ii) the prevention of a specific, substantial, and imminent threat to the life or physical safety of natural persons, or a genuine, present, or foreseeable

threat of a terrorist attack; and (iii) the localisation or identification of a person suspected of having committed a criminal offence, for the purpose of conducting a criminal investigation or prosecution, or executing a criminal penalty for offences referred to in Annex II and punishable in the Member State by a custodial sentence or detention order for a maximum period of at least four years. Point (h) of the first subparagraph is without prejudice to Art. 9 of the GDPR for the processing of biometric data for purposes other than law enforcement.

4.2 High-risk systems

Art. 6 concerns the requirements for categorising high-risk systems and is thus a central requirement of the Regulation. The requirements for risk classification are of considerable practical significance, as many AI systems of relevance (will) fall into the category of high-risk systems. The standard is closely linked to the harmonisation provisions listed in Annex I, which largely determine the requirements for risk determination in the context of product safety law in accordance with the AI Act's first paragraph. In the Regulation's structure, Art. 6 follows the second section on prohibited practices of AI, which contains only one provision (Art. 5). The categorisation as a high-risk system under Art. 6 triggers the obligations under Art. 9 et seq., such as the requirements for human oversight (Art. 14) or data governance (Art. 10). The addressees of the AI Act (providers) are the same as those of the new legal framework for product manufacturers (Ruschemeier, forthcoming).

The first approach for classifying AI systems as high risk is established in Art. 6(1) with references to already existing product safety law. To be classified as high risk, the AI system must either be intended to be used as a safety component of a product or is itself a product, as covered by the Union harmonisation legislation listed in Annex I. A safety component of a product is defined in Art. 3(14) as a component of a product or of an AI system which fulfils a safety function for said product or system, or the failure or malfunctioning of which endangers the health and safety of persons or property. For example, an AI system used as a safety component could be an automatic detection of the need for lift maintenance. Additionally, the system as a product itself or as a safety component of a product must be required to undergo a third-party conformity assessment, with a view to the placing on the market or the putting into service of said

product pursuant to the Union harmonisation legislation listed in Annex I. Under product safety law, a third-party conformity assessment is required for products with a higher risk, while other products can be self-assessed by the provider. This first variety of high-risk classification is aligned with the system of European product safety law, and is thus not a new regulatory approach under the AI Act.

Nonetheless, the second approach for classifying AI systems as high risk establishes a new assessment of fundamental rights implications. Under Art. 6(2), systems are classified as high risk if they are used in the application contexts listed in Annex III. According to Paragraph 2, the systems to be covered are those which, by virtue of their purpose, pose a high risk of harming the health and safety or fundamental rights of persons, taking into account both the severity of the potential harm and its likelihood to occur. They have to fall within the scope of Annex III. This important annex lists eight different areas of applications for high-risk AI systems: 1) biometrics (which are not already prohibited under Art. 5); 2) critical infrastructure; 3) education and vocational training; 4) employment, workers management, and access to self-employment; 5) access to and enjoyment of essential private and public services and benefits; 6) law enforcement, insofar as their use is permitted under relevant Union or national law; 7) migration, asylum, and border control management, insofar as their use is permitted under relevant Union or national law; and 8) administration of justice and democratic processes. Biometric systems under Annex III no. 1 include remote biometric systems, which are: (a) systems intended to be used for biometric categorisation, according to sensitive or protected attributes or characteristics based on their inferences; (b) systems intended to be used for emotion recognition; and (c) those which go beyond the prohibition of the use of such systems in the workplace or educational institutions prohibited in Art. 5. Critical infrastructure under Annex III no. 2 includes critical digital infrastructure, road traffic, or in the supply of water, gas, heating, or electricity.

The area of education and vocational training classifies systems intended to be used to evaluate learning outcomes, including when said outcomes are used to steer the learning process of natural persons in all levels of educational and vocational training institutions, assessing the appropriate level of education that an individual will receive or be able to access, and for monitoring and detecting prohibited behaviour of students during tests in the context of, or within, educational and vocational training institutions at all levels. Furthermore, the fourth category refers to employment and

workplace systems, especially AI systems in recruitment and those that make decisions in work-related relationships, such as regarding promotions or performance evaluations.

Of key importance here is the access to essential private and public services under Annex III (5), including AI systems intended to be used by, or on behalf of, public authorities to evaluate the eligibility of natural persons for essential public assistance benefits and services, including healthcare services, as well as to grant, reduce, revoke, or reclaim such benefits and services, AI systems for credit scoring, risk assessment for life and health insurances, and the classification of emergency calls.

Categories 6 and 7 refer to the use of AI systems in law enforcement and border control. It is important to note that the AI Act only adds another regulatory layer here since these systems must be permitted under national or Union law. Examples include the assessment of the risk of a natural person becoming the victim of criminal offences, the use of polygraphs or similar tools, predictive policing, profiling, or assessments of such risks as those regarding security, irregular migration, or health by natural persons who intend to enter (or have done so) the territory of a Member State. Further areas are the assistance to competent public authorities for the examination of applications for asylum, visa, or residence permits, as well as for associated complaints regarding the eligibility to apply for a status, including related assessments of the reliability of evidence and for the purpose of detecting, recognising, or identifying natural persons, with the exception of the verification of travel documents.

High-risk systems in the fields of administration of justice and democratic processes include the assistance of a judicial authority in researching and interpreting facts and the law, and in applying the law to a concrete set of facts, or a similar use in alternative dispute resolution, and systems used for influencing the outcome of an election.

Art. 6(3) standardises exceptions to the risk classification of Paragraph 2, according to which it is assumed that, in the case of the areas of application listed in Annex III, the AI systems used present a high risk. By way of derogation, such AI systems shall not be considered high risk if they do not pose a significant risk "to the health, safety or fundamental rights of natural persons, even if they significantly influence the outcome or significantly the outcome of a decision".

4.3 Systemic risks for general-purpose AI

Further to the categories of prohibited practices, high-risk, and limited and low-risk systems, a third risk category was added in the final stages of negotiations on the AI Act: the systemic risk of general-purpose AI models. The central Art. 51 is, to some extent, the counterpart of Art. 6 in that it qualifies general-purpose AI systems under the category of "systemic risks". However, the concept of systemic risk in Art. 51 is fundamentally different from that of Art. 6(1–2), thereby introducing a further categorisation of risks. Systemic risks are defined under Art. 3(65) as "a risk that is specific to the high-impact capabilities of general-purpose AI models, having a significant impact on the Union market due to their reach, or due to actual or reasonably foreseeable negative effects on public health, safety, public security, fundamental rights, or the society as a whole, that can be propagated at scale across the value chain". However, the systemic risks of Art. 51 tend not to be determined according to product safety law or the relevance of fundamental rights, but rather to their cause of action and the criteria set out in Annex XIII. If a general-purpose model exceeds the threshold of 10^25 FLOPs (Floating Point Operations per Second) in terms of the cumulative number of calculations used for training, it constitutes a systemic risk (Art. 51(2)). Overall, the rationale behind this technical threshold, implying that model power under it indicates less societal risk, remains unclear from the legislator (see Mühlhoff and Ruschemeier, 2024c). This calculation threshold has little in common with the risk categorisation of Art. 6, which relates to product safety law or the impact on fundamental rights, even if it can be assumed that larger and more powerful models and the number of end users (Annex XII) can be indicators of the relevance of fundamental rights. The relationship between Arts. 6 and 51 is not explicitly clarified by the legislator; the wording suggests that providers whose model is both a high-risk system under Art. 6 and carries systemic risk under Art. 51 must comply with both obligations cumulatively (Ruschemeier, forthcoming).

5. Oversight and governance

Chapter VII of the AI Act regulates the corresponding governance structures divided into the governance at the Union level (Arts. 64–69) and the national competent authorities (Art. 70). On the Union level, the new AI Office is established at the Commission (Art. 64). Art. 3(47) defines the

AI Office as the "Commission's function of contributing to the implementation, monitoring and supervision of AI systems and general-purpose AI models, and AI governance", provided for in the Commission Decision of 24 January, 2024. References in this Regulation to the AI Office shall be construed as references to the Commission. One should note that, although the AI Office has been formed, many details, practicalities, and tensions in law enforcement have, for the moment at least, been left open. As it stands, the AI Office shall have different tasks, such as monitoring general-purpose AI systems, establishing codes of practice, or assisting market surveillance authorities.

Additionally, Art. 65 establishes the European Artificial Intelligence Board (AI Board), which is composed of one representative per Member State and the European Data Protection Supervisor as an observer. The participation of the AI Office is required, but it will not vote. Furthermore, the AI Board establishes two standing sub-groups to provide a platform for cooperation and exchange among market surveillance authorities, and notify them of issues related to market surveillance and notified bodies, respectively. The aim of the AI Board is to ensure cooperation and coordination between the Member States and the relevant Union bodies. To this end, the AI Board shall advise and assist the Commission and the Member States in order to facilitate the consistent and effective application of the AI Act (Art. 66(1)). Article 66 establishes different detailed tasks, such as the collection and sharing of technical expertise (Section b), the contribution to the harmonisation of administrative practices in the Member States (Section d), or supporting the Commission in promoting AI literacy, and the public's awareness and comprehension of the benefits, risks, safeguards, and rights and obligations in relation to the use of AI systems (Section f). In addition to the AI board, an advisory forum shall be established (under Art. 67) to provide technical expertise, scientifically advise the Board and Commission, and contribute to their tasks. The members shall represent a balanced selection of stakeholders, including those of industry, start-ups, small and medium-sized enterprises (SMEs), civil society, and academia. The membership of the advisory forum shall be balanced in terms of commercial and non-commercial interests and, within the category of the former, regarding SMEs and other undertakings (Art. 67(2)). Members are appointed by the Commission. Moreover, the Fundamental Rights Agency, ENISA, the European Committee for Standardization (CEN), the European Committee for Electrotechnical Standardization (CENELEC),

and the European Telecommunications Standards Institute (ETSI) are permanent members of the advisory board.

Besides the AI Office and Board, the Commission shall establish a scientific panel of independent experts to support the enforcement of activities under Art. 68 of the AI Act. This is implemented by the Commission following Art. 98's process on the committee procedure (2), and is thus not included in the AI Act itself. The goal of the scientific panel is to ensure independent scientific and technical expertise in the field of AI to support the AI Office, such as by alerting it to possible systemic risks or providing advice on the classification of various general-purpose AI models and systems (Art. 68(3)). Given the unclarity and open questions in these realms, such independent scientific expertise seems urgently needed, particularly in the still developing categories for the regulation of general-purpose AI. On the national level, the Member States can call upon the experts of the scientific panel to support their enforcement activities under Art. 69.

Furthermore, Art. 70 requires the designation of Member States' national competent authorities to enforce the Regulation's provisions. Art. 70 requires the establishment of one notifying authority responsible for establishing and undertaking the procedures necessary for assessing, designating, and notifying conformity assessment bodies. As mentioned above, these private conformity assessment bodies (e.g., equal to the TÜV in Germany for product safety assessment) are active for high-risk systems only. Their monitoring is laid down in Art. 28 et seq., foreseeing that one market surveillance authority supervises the other obligations of the AI Act on a national level.

On the execution level, the AI Act provides for various penalties and fines. Art. 99(1) states that Member States shall lay down the rules on penalties and other enforcement measures, which may also include warnings and non-monetary measures, applicable to infringements of this Regulation by operators, and shall take all measures necessary to ensure their proper and effective implementation. Furthermore, Art. 99(3) states that the non-compliance with the prohibition of the AI practices referred to in Art. 5 shall be subject to administrative fines of up to 35,000,000 EUR or, if the offender is an enterprise, up to 7% of its total worldwide annual turnover for the preceding financial year, whichever is higher. The non-compliance with obligations in Arts. 16, 22, 23, 24, 26, 31, 33(1, 3, 4), 34, and 50 is subject to administrative fines of up to 15,000,000 EUR or, if the offender is an enterprise, up to 3% of its total worldwide annual turnover for the preceding financial year, whichever is higher (Art. 99(4)). The supply of

incorrect, incomplete, or misleading information to notified bodies or national competent authorities in reply to a request shall be subject to administrative fines of up to 7,500,000 EUR or, if the offender is an enterprise, up to 1% of its total worldwide annual turnover for the preceding financial year, whichever is higher (Art. 99(5)). For SMEs and start-ups, the lower percentage or amount should be applied. The rules on administrative fines are imposed by the relevant competent authorities of the Member States, such as by courts or other bodies. In Germany, for example, the competent authority would be the national market surveillance authority.

Furthermore, Art. 100 lays down provisions on administrative fines on Union institutions, agencies, and bodies imposed by the European Data Protection Supervisor (EDPS). Finally, Art. 101 establishes fines for providers of general-purpose AI models not exceeding 3% of their annual total worldwide turnover in the preceding financial year, or 15,000,000 EUR, whichever is higher. Fined violations are, for example, such procedural failures as not complying to a request for documentation or information under Art. 91 or the material infringements with relevant provisions of the AI.

6. Part III: critical analysis

6.1 Definition of AI in the AI Act: inclusive but negating AI as a socio-technical phenomenon

Addressing AI directly as an object of regulation is complex due to the multitude of views on what AI *actually* is. In the modern field – stemming from computer science, cybernetic, and mathematical approaches of the 1940s – AI tends to be used as an umbrella term for different applications and has changed throughout the decades and hype circles. Given the complexity and unclarity in the academic field of AI, not every AI-related regulation directly names the technology (e.g., the DSA). The AI Regulation explicitly addresses "AI systems", but, in its first versions, defined them so broadly that practically any software was covered.

6.1.1 Towards the final AI definition

From a legal and regulatory perspective, the definition of the Regulation's subject matter is vital as it determines its scope. A concise instantiation

of the regulatory object is pivotal for avoiding legal loopholes. Moreover, the requirements of legal certainty, precision, and practicability must be met. However, due to the wide range of societal segments and sciences that are directly or indirectly affected by AI, each perspective leads to its own definition of what AI is and means for the respective area. Normative regulation and social sciences do not follow a purely technical understanding of AI, but have stressed that the context of use, the social phenomena it produces, and the protected goods and interests it affects are as important as the instantiating of the technical functionality (Bareis, 2024; Ruschemeier, 2023a). It can thus be expected from the legislator to narrow down a definition that, while not necessarily encompassing the complexity of the entire scientific debate, at least serves the regulatory purpose and does justice to the individual and societal harms present with AI.

In the subsequent legislative process of the draft Regulation, the AI definition was actually changed several times. Indeed, the European Parliament's proposal of June 2023 reads: "AI system means a machine-based system that is designed to operate with varying degrees of autonomy and that can generate outputs such as predictions, recommendations or decisions that influence physical or virtual environments for explicit or implicit goals". This definition also raises follow-up questions, such as what autonomy really entails, with its notions being contested due to always being situated (Suchman, 2023; Weber and Suchman, 2016). Instead, we argued that the risk profile of AI systems can only be determined from the interplay between the technical functionality *and* the application context (i.e., a social domain), thus pointing to a necessary revision of the Act's definition of AI.

The emphasis on the regulatory filter in the Regulation's draft was not adopted as the final definition. The EU arrived at the following final reading of AI (Art. 3(1) AI Act):

> "AI system" is a machine-based system designed to operate with varying levels of autonomy and that may exhibit adaptiveness after deployment and that, for explicit or implicit objectives, infers, from the input it receives, how to generate outputs such as predictions, content, recommendations, or decisions that can influence physical or virtual environments.

Notably this rather broad definition seeks to cope with the AI field's rapid pace of technical innovation. The definition actually includes simpler ADMs that have "explicit objectives" (but which nowadays hardly carry the denotation of AI in the debate) as much as the latest ML-run applications that are highly data intensive and yield unexpected (even if deterministic)

results through statistical reasoning in unsupervised learning. This broad scope is, on the one hand, problematic, as unclarity may lead to legal loopholes. On the other, the definition can also be interpreted as welcomingly broad in encompassing algorithmic systems at large.

6.1.2 Beyond technical AI: understanding AI as a socio-technical phenomenon

Despite this definition's breadth, it fails to grasp AI as a *social* phenomenon instead of a purely technical one. It is not that AI "decisions (...) can influence physical or virtual environments" only, but particularly *social* ones as well. There are two scandals connected to public agencies which effectively illustrate this point.

There are already very rudimentary algorithmic systems that can cause great societal damage. For example, the rather simple "Robodebt" scheme was installed in Australia to identify welfare fraud and overpayments in tax declarations. The scheme was not run by ML, but rather with a simple algorithm that cross-referenced payment data with annual income data provided by the Australian Tax Office (Murray, Cheong and Paterson, 2023). Robodebt was ruled unlawful and scrapped in 2020 because of the simple fact that it relied on imprecise income averaging and violated basic principles of procedural fairness and contestability, marking welfare recipients (i.e., structurally disadvantaged people) as potential cheaters.

Likewise, in the Netherlands, in the childcare benefits scandal ("*kinderopvangtoeslagenaffaire*") approximately 26,000 parents were wrongly accused by algorithmic flagging of fraudulent financial benefit applications and allowances had to be repaid to the Dutch financial ministry in full (see also Ruschemeier, 2024b). Some of the repayments totalled several tens of thousands of euros, which led to personal bankruptcies, the withdrawal of custody rights, and, ultimately, several suicides. The Dutch Data Protection authority investigated the tax and customs administration and ruled (Autoriteit Persoonsgegevens, 2020) that "the whole system was set up in a discriminatory way. [...] There was permanent and structural unnecessary negative attention for the nationality and dual citizenship of the applicants" (own translation). The scandal ultimately led to the resignation of the Rutte government and new elections in 2021.

These two public agency scandals, based on rather simple algorithmic recommender systems, show that complex statistical inference[9] or chatbots based on the latest LLMs (what is currently referred to as AI in the public debate) are not necessarily needed to provoke massive individual and structural damage in societies. Powerful AI systems simply complicate the situation even further, as larger datasets, accelerating computing power, complex models, and server infrastructures owned and shielded by Big Tech companies can further aggravate the opacity of AI systems and distort political accountability if such errors as unrightful bias or privacy violations occur.

In their daily interactions, users never actually see code, databases, or backends of AI applications. As argued elsewhere (Bareis, 2024), AI is hardly perceived and approached as a clearly articulated, delimited, and external "thing", "model", or "tool" like the technical AI Act definition suggests. In essence, policymakers must consider that users are being presented with an AI end product that remains completely closed and opaque in its design process, operating mechanisms, and underlying normative choices. Rather than approaching AI as a self-standing entity that can be generalised (i.e., "AI is x"), recent sociological scholarship argues that AI is better understood as woven and negotiated in the everyday realities of users and society (Bodó, 2021; Suchman, 2023; Weber and Suchman 2016; Mackenzie, 2015), with its applications mediating human relationships, producing intimacies and alienations, social orders, and knowledge authorities. Here, the Australian Robodebt scheme and the Dutch childcare benefits scandal are highly indicative. AI systems (or simple ADMs) are increasingly penetrating into all spheres of society and are beginning to *mediate* and *rule* over social matters. They can enable social interaction on social media feeds with friends, but also execute physical violence (see the above-listed examples), as well as epistemic violence (derogatively portraying certain groups in society and damaging their reputations). The definition within the AI Act misses this *social* component identified by recent scholarship. Due to this technical reading, the AI Act also fails to clearly address and regulate some fundamental social risks caused by AI (see analysis in III). A less abstract and more empirical and hands-on approach understands

9 See, for example, the debate on the more complex US recidivism score system used in the US judiciary that uses the probability of criminals reoffending in its recommendations for or against parole, called the "Correctional Offender Management Profiling for Alternative Sanctions system" (COMPAS) (Angwin et al, 2022).

AI not only as algorithmic performativity, but also includes the social phenomena it produces, and the *meaning* ascribed to them. Such a perspective would clearly make the EU AI regulatory framework more accessible and closer to every-day user experiences. Given that European standardisation bodies are currently trying to implement the AI Act on the Member State level (Gamito and Marsden, 2024), it remains to be determined how these social and epistemic risk dimensions can be entangled in a process of quantification the creation of risk scores (discussed in greater detail below).

6.2 Dualistic regulatory structure: the misfit of applying product safety law on fundamental rights protection[10]

The AI Regulation aims to not only improve the functioning of the internal market, but also to promote human-centred and trustworthy AI and ensure a high level of protection against harmful effects on health, safety, fundamental rights, democracy, the rule of law, and the environment – all while simultaneously promoting innovation (Recital 1).

The different duties the AI Act seeks to fulfil resemble an ambitious attempt to politically square the circle. It aims to satisfy various interests which are at odds with each other: the trustworthy and fundamental rights pillar to protect human-centred rights needs to accommodate the economic interest to which the vast profit potential of user data points – just to finally include all pillars in a harmonised but competitive free-market approach. Here, it remains to be seen whether these objectives – in particular, the protection of fundamental rights – can be achieved through a regulatory structure based on product safety law and risk-based governance. A growing number of scholars have rightly criticised this regulatory approach (Almada and Petit, 2023; Guijarro, 2023; Smuha et al, 2021; Veale and Borgesius, 2021). Although the adoption of an existing regulatory structure offers the advantage of established models and concepts, AI systems themselves are fundamentally different from the products on which the concept of product safety law and the tradition of risk-based governance are based. Such is also the understanding of risk in the protection of fundamental rights and product safety law.

10 The following critique (6.2-6.3) is an English version of the arguments made in Ruschemeier (forthcoming).

6.2.1 Physicality and actors: AI systems are no fixed products

The regulation is characterised by the idea of a certain physicality of AI systems. Their purposes shall be determined ex ante and their changes accompanied by delegated acts. However, the extent to which the particularities of more and evolving complex systems can be captured is doubtful (Edwards, 2022b). This is because AI systems change as a result of new data creation and processing (see the current rise of synthetical data), steady model development (as with foundation models), or the growing platformisation and infrastructural integration of other possible systems (centralisation). The regulatory strand of product safety law, on the other hand, is based on assumptions that do not correspond to how AI systems function, even if software can be categorised as a product under the new legislation. AI systems are not products that are manufactured once and then placed on the market, and used only for fixed purposes in specific contexts. Instead, they are increasingly being used dynamically in different contexts with different effects on individuals and groups (Edwards, 2022b). The actors involved are also fundamentally different: product manufacturers tend to be experts in their production processes and are rightly the addressees of safety requirements. Moreover, the development of AI systems also differs, often involving different actors and institutions, with smaller developers in particular relying on building blocks, datasets, and other resources than larger companies in order to develop their own products, especially given the recent turn to the platformisation of AI. The *downstream* use of AI systems can therefore look very different from a system's original development.

6.3 Different understanding of risks and harms depict paradigms that are not compatible

In addition, product safety law is based on a specific understanding of risk that cannot be transferred to the socio-technical hazards and risks posed by AI systems. Therefore, it is unlikely for these risks to be adequately capture by a regulatory system based on the categories of product safety law. The understanding of risk in product safety law, as part of private law, is based on the reference to potential damage, which is then compensated through such claims as damages for injury to bodily integrity. Firstly, product safety law and the protection of fundamental rights are based on differ-

ent concepts of risk. Furthermore, normative safeguards of freedom, such as human autonomy, cannot be measured exclusively in numerical terms and translated into metrics or standards, but always depend on a case-by-case assessment. The AI Act neither addresses the gaps between different regulations, such as data protection and discrimination law, nor clarifies important concepts, but could even exacerbate the problem (Adams-Prassl, 2022). In practice, the requirements of the AI Regulation itself are undermined by the presumption of compatibility under Articles 40 et seq.

This categorical tension in the regulatory approach stems from the dominance of a "risk-based" regulatory assessment paradigm that began to dominate the Anglo-Saxon world in the 1980s–1990s (Black, 2005; Hood, Rothstein and Baldwin, 2001) and has ever since influenced the EU in such areas as safety standardisation for the chemical and food industries, or in environmental impact assessments (Orwat et al, 2024; Paul, 2021). The paradigm of risk-based regulation resembles a shift away from a rather prescriptive approach based on formal legal statutes and normative principles. Instead, risk-based regulation promises empirically based and adaptive "cost-benefit" practices, requiring numerical assessments and classifications (Black, 2010). This paradigm not only implies that risks must be measurable (hence, "quantifiable"), but also that they can be managed and, to some degree, accepted: it is not about *avoiding* harms, but about their acceptable and bearable societal *handling*, ranging from acceptable to unacceptable harms, and deriving the appropriate levels of such regulatory measures as tests, benchmarking, approvals, requirements, bans, or moratoria. The ideal outcome is to find the right balance between over- and under-regulation. However, as argued elsewhere, risk-based regulation needs "sufficiently unambiguous and concrete criteria or principles for what constitutes relevant risks" (Orwat et al, 2024, p. 11). As such, finding the right risk scheme for AI is a particular challenge.

The problem with the EUC's reliance on this product safety risk-regulatory rationale with AI (for a critical reconstruction, see Paul, 2023) is that the nature and understanding of risk in the context of the protection of fundamental rights is by no means uniform. The risk to fundamental rights is not synonymous with potential harm from, for instance, chemicals in food or radiation, but lies in the potential violation of the fundamental right, which in turn does not necessarily presuppose harm. The understanding of constitutional protection of fundamental rights follows a precautionary principle, e.g., data protection is "protection beforehand" – that is, in advance of the actual danger. There has been an increase in the number of

proposals emerging which use risk regulatory metrics and thresholds to represent elusive values, such as "fairness", "justice", or "privacy" in order to make them manageable. However, given the strong contextualisation of anti-discrimination law, for example, the ability to translate normative values into numerical measures is limited from the outset (Ruschemeier, 2023b). See, for example, the AIEI report (Hallensleben and Hustedt, 2020) "From principles to practice", which exactly aims at establishing those metrics. However, it has been (somewhat problematically) suggested that rights and normative values can be quantified or even "cleared" with each other. Here, rights become labelled like washing machines, suggesting a legal clarity which is not the case. Factors of contextuality, residual risks, or intangible subjective harms, such as reputational damage, become completely neglected in this reductionist approach.

6.4 Watered down Fundamental Rights Impact Assessment

There are also concerns about the dual regulatory strategy's ability to strike a suitable balance between minimising risk and fostering innovation for applications in the public interest. AI systems used in the medical field (and subject to the MDR) will always be high-risk systems, while such lifestyle applications as smartwatches or fitness trackers will be subject to the requirements for high-risk systems, but may not even be subject to the general requirements of Art. 50. Such applications can pose significant risks, for example, with regard to the collection of health data. Health tracking has the potential to aggravate the individualisation of risk under the disguise of algorithmic and profit efficiency, thus undermining a system of public service and solidarity with weaker social-economic strata. There is a high likelihood that, under the logic of cost-efficiency, these strata will have to pay higher fees for premiums as the neighbourhoods in which they live provide aggregate health, education, or crime data. With the ongoing privatisation of the health and insurance sector in many countries, it is reasonable to assume that this will result in advantages for companies with considerable economic resources to challenge high-risk classifications, as expressly provided for in Art. 6 para. 3.

The AI Act establishes a Fundamental Rights Impact Assessment (FRIA) in Art. 27, which was included after an intervention of various academics in the legislative process (Mantelero, 2022; Liberties, ECF and ECNL, 2023). It reflects the impacts on fundamental rights to a certain degree. However,

the provision was watered down during the legislative process and now only applies to deployers that are bodies governed by public law, or private entities providing public services, and deployers of high-risk AI systems referred to in points 5(b) and (c) (credit and insurance scoring) of Annex III. This is unfortunate since all the other use cases listed in Annex III can have heavy implications and inferences with fundamental rights. Moreover, it does not seem particularly clear why the FRIA specifically addresses public entities (which are bound by fundamental rights anyway) and not private actors, who have no such binds (see also Mantelero, 2024). The insufficiency of the FRIA is one of the most significant misses of the AI Act.

7. Governance and the imbalance between private and public interest

7.1 Democratically unsupervised private standardisation procedures

In practice, the risk classification of Art. 6 and the subsequent obligations of the Regulation's third section are significantly influenced by the standardisation norms of Arts. 40 et seq. When harmonised standards are established, it is assumed that the corresponding AI systems comply with the requirements of Chapter 2 of Part 3 of the Regulation (Arts. 8–15). These requirements include, for example, obligations for risk management systems (Art. 9), data governance (Art. 10), technical documentation (Art. 11), and human oversight (Art. 14).

Standardisation procedures are well known and established in product safety law. However, the Regulation also stipulates that high-risk AI systems must meet certain mandatory requirements that align with the European interests of health, safety, and the protection of fundamental rights, such as risk and data management, transparency, and human oversight. It should then be possible to implement these requirements in harmonised standards developed by the European standardisation bodies. Regarding the relevance of systems to fundamental rights, there is no experience at the level of EU regulation of how these can be standardised. Standardisation focuses on areas where the state of the art is particularly relevant, and therefore the consideration of fundamental rights is not given prima facie. In this context, the development of standards cannot be purely technical (i.e., based on computer science and engineering). It must have a social dimension linked to considerations and findings from the humanities and social sciences, including law.

Moreover, this far-reaching power of definition, from which Member States can only deviate in individual cases by means of a single authorisation (according to Art. 47), does not correspond to democratic legitimation, but lies exclusively with private standardisation organisations. This standardisation is not subject to parliamentary debate, but is limited to the adoption of a consensus by the interest groups of each draft standard, clearly pointing to a democratic deficit. In practice, these interest groups are dominated by the leading international economic players most affected by the standard in question, mirroring an imbalance with the absent public interest actors. At least, the ECJ has now ruled that harmonised technical standards must be freely accessible and thus available free of charge (Public.Resource.Org, Inc. and Right to Know CLG v European Commission, 2024). However, the obligation to assess the impact on fundamental rights in Art. 27 does not change this state of affairs. This is because it does not lay down any requirements for the standardisation process, but solely obliges certain operators (Art. 3(4)) to conduct an impact assessment on how the system affects "fundamental rights" in certain cases. Given the Regulation's objective, this obligation would have been desirable in principle for *all* AI systems, but was considerably weakened in the legislative process. The obligation now only applies to public bodies or private operators providing public services and operators of systems under Annex III No. 5 lit. b) (credit scoring with the exception of financial fraud detection).

The different understandings of harm and risk by product safety law and fundamental rights protection are compounded by the enforcement and governance structures of the AI Regulation. The Regulation's lofty goals of protecting fundamental rights are largely dependent on private standardisation organisations (CEN and CENELEC) and procedures (see here Gamito and Marsden, 2024).[11] The product safety approach of technical standards, coupled with the presumption of conformity of Arts. 40 ff., is intended to both provide flexibility and avoid overburdening the supervisory authorities. This is convincing for the area of product safety law, where there is expertise and practical experience regarding standardisation and the implementation of safety in technical standards. However, when

11 Although they are not mentioned by name in the text of the Regulation, the standardisation organisations will have a crucial role to play. The Commission has already issued the first standardisation mandate (C(2023)3215) in support of Union policy on AI, which has been accepted by CEN and CENELEC (European Commission, no date). According to Art. 1 of the Implementing Decision, the standards shall be developed by 30 April, 2025.

assessing the risk to fundamental rights, technical standardisation is highly problematic.

The classification for high-risk systems shall be based on a preliminary self-assessment, so the law is likely to exacerbate the problem of developers deliberately misclassifying their innovations so as to circumvent having to comply with the strict requirements. Suppliers who consider that their system is not high risk according to their own assessments (which falls under the use cases of Annex III para. 3), must first document this assessment before placing the system on the market (Ruschemeier, no date).

7.2 Missing participation of affected subjects

Moreover, the perspective of fundamental rights holders is not even considered in the AI Act; however, the relevance of fundamental rights cannot be examined in a supposedly technical vacuum, but only in relation to the affected subjects. It is unclear to what extent private standardisation organisations, which have neither the expertise nor the structures to assess fundamental rights, should be able to do this. It is doubtful whether fundamental rights implications can be adequately taken into account within this framework, despite all of the possibilities related to stakeholder participation. Collective dimensions, such as those that play a role in labour law, are not mentioned in the AI Act (Adams-Prassl, 2022). Nor does it contain a provision equivalent to Art. 88 of the GDPR, which would allow Member States to adopt more specific national provisions for the employment context, which would further limit their willingness to experiment with regulation.

7.3 The problem of algorithmic discrimination escaping the categories of anti-discrimination

The joint opinion of the European Data Protection Board and the European Data Protection Supervisor on the AI Act (European Data Protection Board, 2021) rightly points out that risks to groups of individuals or to society as a whole, such as group discrimination or the freedom of political expression, are not adequately addressed in the AI Act. This also applies to the specific risks of discrimination against individuals by data-intensive technologies. The AI Act mentions discrimination and social risks in sever-

al places and calls for studies on prohibited discrimination in the context of data governance (Art. 10 para. 2 lit. f). Further references can only be found in Art. 77 and Annex IV on supervision and technical documentation. The AI Act does not decide when further discrimination is undesirable or risky, which is highly relevant in terms of fundamental rights. The problem of algorithmic discrimination escaping the categories of anti-discrimination law remains unresolved (Wachter, 2023). In terms of supra-individual effects, Annex III categorises the areas of administration of justice and democratic processes as high-risk areas, not regarding expression, but in terms of systems intended to influence the outcome of an election or the voting behaviour of natural persons. While this is certainly welcome, it only addresses part of the problem.

7.4 The loophole of addressing recommendation systems on platforms as high-risk systems

The risk of influencing elections through political advertising should also be regulated. However, the proposed Regulation provides for the possibility of political targeting based on the consent of the data subject (Art. 18(1)(b)). However, this consent-instrument cannot consistently protect fundamental rights in the digital context as the large flood of information is simply not comprehensible or deliberately difficult to access in platform option settings (e.g., when seeking to obtain consent from hundreds of different data processors; Ruschemeier, 2022). The parliamentary proposal on the risk category of recommendation systems of very large online platforms and search engines under the DSA was deleted in the final version. As such, a large part of the AI systems that most people interact with on a daily basis are not covered by the AI Act as high-risk systems. Considering how much time citizens spend on social media – with global interactions averaging 2.31 hours per day (and up to 5.01 on smartphones) in 2023 – the impact of the consumed and widely disseminated content is not to be underestimated (Kemp, 2023). These numbers are all the more worrying for democratic processes in societies given that prior research has clearly pointed to a growing polarisation, political fragmentation, and self-reinforcing of political (often populist or extremist) opinion through echo chambers on social media platforms (Barberá, 2020; Fisher, 2022). Problematically, this has also affected how the DSA tackles misinformation (Arts. 14, 14 III, 19), as: "when polarization is high, misinformation quickly proliferates" (Cinelli et

al, 2021, p. 5). Considering the rate at which synthetically generated data is currently flooding the internet and social media, problematic and extremist content is likely to increase in scale and quality.

The AI Act does not address the dissemination and information power asymmetry of large platform companies, which contributes significantly to AI risks (Mühlhoff and Ruschemeier, 2024b). The deletion of the high-risk categorisation also prevents the important interaction between the DSA and the AI Act in the overall European regulatory framework, where it would have been informative to examine how the obligations under the DSA and the AI Act relate to very large providers.

7.5 Lobbying and the risk of tech-solutionism[12]

Some of the AI systems classified as high-risk under the AI Act are highly problematic. Indeed, certain systems which are not scientifically researched or validated, and have no clear or beneficial use for individuals or the public, can ultimately be mainstreamed or normalised. First, it is unclear why systems that are intended to be used to influence the outcome of an election (Annex III 8(b)) are even legal in the first place. Elections should be free and uninfluenced in order to be democratically legitimate, and AI systems which influence their results have no legitimate purpose in democratic states and should be banned. Systematically, it is not understandable why the use of AI by judicial authorities is not subject to national legal reservation, such as law enforcement, since both areas of use are highly influenced by national legislation. The (highly) scientifically questionable use of polygraphs in 1(c), 6(b), and 7(a) are legitimised as high-risk systems without any indication for their effectiveness (lie detectors have absolutely no scientific grounding, and can thus be termed pseudo-science). Many of the more restrictive takes on high-risk systems and general-purpose AI have been lowered throughout the legislative process. Consequently, the overall protection of fundamental rights throughout the AI Act has suffered substantially.

Reports by the Corporate Europe Observatory (Schyns, 2023) and Transparency International (Kergueno et al, 2021) have proven how Big Tech, corporate think tanks, and trade and business associations have been disproportionately active in blocking and watering down AI regulation in

12 Parts of this section are taken from Bareis (2023b, 2024).

Brussels. As discussed elsewhere on the final trilogue between the Commission, Parliament, and Council in late 2023, Big Tech efforts on the AI Act have been substantial (Bareis, 2023b). In 2023 alone, industry lobbyists had by far the most meetings with the EU commission on the AI Act, with 86% (73 out of 98) of all behind-closed-door meetings, and were most active in agenda and standard setting (Corporate Europe Observatory, 2023; Kergueno et al, 2021). For the AI Act, "tech companies have reduced safety obligations, sidelined human rights and anti-discrimination concerns" (Schyns, 2023, p. 3). Leaked documents strikingly show how companies have tried to pressure policy makers with their deregulatory agendas by staging such narratives as "Big tech is 'irreplaceable' when it comes to problem solving", "we're just defending SMEs and consumers", or "Europe wins the tech race against China, or it falls back into the Stone Age" (Bank et al, 2021, p. 27). This tech-solutionist take on AI is converting AI into an inevitability, catering to a narrative that suggests "only advancement in AI technology can assure that the current level of living can be maintained and future prosperity secured" (Bareis and Katzenbach, 2022, p. 868). With such an AI hype and the argumentative force of the TINA (there-is-not-alternative) mindset, politics becomes pressured towards an unreflective and unchecked uptake of AI across society. Instead, politics should act like a critical watchdog given the public's mandate, and clearly and effectively address the chances and risks of this multifaceted technology for the benefit of all.

In the final round of discussions on the AI Act, lobbying efforts have been directed against the designation of general-purpose AI as a "high risk" category, with industry representatives fearing that it would overburden and stifle innovation with strict conformity assessments. Such European startups as Mistral and Aleph Alpha joined forces with US Big Tech companies and derailed, with direct ties to political executives in France or Germany, the policy-making process in the last metres. Industry managed to water down the binding fundamental right assessment proposed by the European Parliament on general-purpose AI into mere transparency rules (Corporate Europe Observatory, 2023; Hartmann, 2023).

8. Conclusion and outlook

Despite all the criticism, the adoption of the AI Act is a milestone in digital regulation at the European level. It is important that the EU legislator

has recognised and regulated many problematic practices, such as the ban on indiscriminate scraping to create facial recognition databases, emotion recognition systems, and the risks of insurance and credit scoring.

However, we argue that the AI Act also has major caveats to effectively regulate AI in the service of the public interest of European citizens. The Regulation's enforcement is currently underway in the 27 EU Member States and transfers a great deal of power to private standard-setting organisations. As we have argued, this is problematic from the perspective of democratic legitimacy, as private organisations are given too much discretion in deciding upon sensitive rights and trade-offs of privileges and burdens in our society with respect to AI. Adding to the perspective of democratic inclusion, a stronger participation of affected subjects, a deeper understanding of anti-discrimination, and a more hands-on definition of AI, doing justice to the *social* phenomena it produces, would significantly contribute to the overall acceptance of the Regulation and help close its current loopholes.

While some of these points could be potentially revised in the aftermath of the AI Act's implementation, there are some decisions on the overall structure and design of the Regulation that seem unsuited to its overall purpose. The AI Act applies product safety law for the sake of fundamental rights protection. However, such a legal framework is ill-equipped to cover the socio-technical hazards and risks posed by AI systems. These systems are fundamentally different from the products on which the concept of product safety law and the tradition of risk governance are based. Risk regulation originates from safety standard setting of clearly measurable physical harms, such as those from chemicals or radiation. However, normative safeguards, rights, and political threats to democracy cannot be measured exclusively in numerical terms and translated into metrics or standards. The next few years will show to what extent the ambitious approach of combining product safety law with the protection of fundamental rights can be effectively implemented in practice.

It thus remains, seemingly by design, why recommendation systems on platforms are not marked as high-risk systems, given the very individual and structural damage they can inflict on reputations, cause democratic polarisation, and further exacerbate the power of Big Tech companies. These companies are currently some of the world's most profitable and have, time and again, proven that they aim for big profit, and not for the public good.

All of this shows that the (European) discussion about AI regulation cannot end with the AI Act. The aim of our contribution is to further stimulate the discussion about the social risks and sensible applications in order to revise and improve the AI legal policy frameworks currently implemented around the world. Law, acting as a powerful instrument to distribute the benefits and burdens of this technology for the greater social good, must not lag behind Big Tech's consistently questionable endeavours. It must be socially leading.

References

Abraham, Y. (2024) '"Lavender": the AI machine directing Israel's bombing spree in Gaza'. *+972 Magazine*, 3 April [Online]. Available at: https://www.972mag.com/lavender-ai-israeli-army-gaza/ (Accessed: 28 January 2025).

Adams-Prassl, J. (2022). 'Regulating algorithms at work: lessons for a "European approach to artificial intelligence"', *European Labour Law Journal*, 13(1), pp. 30–50.

AI HLEG (2019) *Ethics guidelines for trustworthy AI*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Accessed: 28 January 2025).

AI HLEG (2020) *Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (Accessed: 28 January 2025).

Almada, M. and Petit, N. (2023) *The EU AI Act : a medley of product safety and fundamental rights?* Working Paper. European University Institute [Online]. Available at: https://cadmus.eui.eu/handle/1814/75982 (Accessed: 28 January 2025).

Angwin, J., Larson, J., Mattu, S. and Kirchner, L. (2022) 'Machine bias' in Martin, K. (ed.) *Ethics of data and analytics. Concepts and Cases.* New York: Auerbach Publications, pp. 254-264.

Arias-Cabarcos, P., Khalili, S. and Strufe, T. (2023) '"Surprised, shocked, worried": user reactions to Facebook data collection from third parties', in *Proceedings on Privacy Enhancing Technologies* 2023(1), pp. 384–399.

Autoriteit Persoonsgegevens (2020) *Werkwijze Belastingdienst in Strijd Met de Wet En Discriminerend*. Den Haag [Online]. Available at: https://web.archive.org/web/20200719043135/https://autoriteitpersoonsgegevens.nl/nl/nieuws/werkwijze-belastingdienst-strijd-met-de-wet-en-discriminerend (Accessed: 28 January 2025).

Bächle, T. C. and Bareis, J. (Eds.). (2025). *The Realities of Autonomous Weapons*. Bristol University Press.

Bächle, T.C. and Bareis, J. (2022) '"Autonomous weapons" as a geopolitical signifier in a national power play: analysing AI imaginaries in Chinese and US military policies', *European Journal of Futures Research*, 10(20), pp. 1-18.

Bank, M., Duffy, F., Leyendecker, V. and Silva, M. (2021) *The lobby network: Big Tech's web of influence in the EU*. Brussels and Cologne: Corporate Europe Observatory and LobbyControl.

Barberá, P. (2020) *Social media, echo chambers, and political polarization*. Cambridge: Cambridge University Press.

Bareis, J. (2024). *Ask Me Anything!* 😈 *How ChatGPT Got Hyped Into Being* (preprint). Center for Open Science [Online]. Available at: https://doi.org/10.31235/osf.io/jzde2 (Accessed: 28 January 2025).

Bareis, J. (2023a) 'BigTech's efforts to derail the AI Act', *Verfassungsblog* [Online]. Available at: https://verfassungsblog.de/bigtechs-efforts-to-derail-the-ai-act/ (Accessed: 28 January 2025).

Bareis, J. (2023b) 'Die EU und Big Tech riskieren eine Krise des Wissens', *Der Standard*, 27 December [Online]. Available at: https://www.derstandard.at/story/3000000200822/die-eu-und-bigtech-riskieren-eine-krise-des-wissens (Accessed: 28 January 2025).

Bareis, J. (2024) 'The trustification of AI. Disclosing the bridging pillars that tie trust and AI together', *Big Data and Society*, 11(2), [Online]. Available at: https://doi.org/10.1177/20539517241249430 (Accessed: 28 January 2025).

Bareis, J. and Katzenbach, C. (2022) 'Talking AI into being: the narratives and imaginaries of national AI strategies and their performative politics', *Science, Technology, and Human Values*, 47(5), pp. 855–881.

Barkane, I. (2022) 'Questioning the EU proposal for an Artificial Intelligence Act: the need for prohibitions and a stricter approach to biometric surveillance', *Information Polity*, 27(2), pp. 147–162.

Bhuta, N., Beck, S. and Liu, H.-Y. (2016) *Autonomous weapons systems: law, ethics, policy*. Cambridge: Cambridge University Press.

Black, J. (2005) The emergence of risk-based regulation and the new public risk management in the United Kingdom. *Public Law*, Autumn, pp. 510–546.

Black, J. (2010) "Risk-Based Regulation: Choices, Practices and Lessons Being Learnt." Paris: OECD [Online]. Available at: https://doi.org/10.1787/9789264082939-11-en (Accessed: 28 January 2025).

Bock, K., Kühne, C.R., Mühlhoff, R., Ost, R.M., Pohle, J. and Rehak, R. (2020) 'Data protection impact assessment for the Corona App'. *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.3588172 (Accessed: 28 January 2025).

Bodó, B. (2021) 'Mediated trust: a theoretical framework to address the trustworthiness of technological trust mediators', *New Media and Society*, 23(9), pp. 2668–2690.

Broeders, D., Cristiano, F. and Kaminska, M. (2023). 'In search of digital sovereignty and strategic autonomy: normative power Europe to the test of its geopolitical ambitions', *Journal of Common Market Studies*, 61(5), pp. 1261–1280.

Burkhardt, S. and Rieder, B. (2024) 'Foundation models are platform models: prompting and the political economy of AI', *Big Data and Society*, 11(2), pp. 1–15.

Cinelli, M., De Francisci Morales, G., Galeazzi, A., Quattrociocchi, W. and Starnini, M. (2021). 'The echo chamber effect on social media', *Proceedings of the National Academy of Sciences*, 118(9) [Online]. Available at: https://doi.org/10.1073/pnas.2023301118 (Accessed: 28 January 2025).

Citron, D. and Pasquale, F. (2014) 'The scored society: due process for automated predictions', *Washington Law Review*, 89(1), pp. 1–33.

Corporate Europe Observatory. (2023) *Byte by byte*. Corporate Europe Observatory [Online], 17 November. Available at: https://corporateeurope.org/en/2023/11/byte-byte (Accessed: 28 January 2025).

Council of the EU. (2023) *New rules for machinery: Council gives its final approval*. Council of the EU [Press release], 22 May [Online]. Available at: https://www.consilium.europa.eu/en/press/press-releases/2023/05/22/new-rules-for-machinery-council-gives-its-final-approval/ (Accessed: 28 January 2025).

Datenethikkommission (2019) *Opinion of the Data Ethics Commission*. Datenethikkommission [Online]. Available at: https://www.bmi.bund.de/SharedDocs/downloads/EN/themen/it-digital-policy/datenethikkommission-abschlussgutachten-kurz.pdf;jsessionid=7D05795C3957AB73E7DAE2D912B49757.live861?__blob=publicationFileandv=3 (Accessed: 28 January 2025).

'Directive 2005/29/EC of the European Parliament and of the Council of 11 May 2005 concerning unfair business-to-consumer commercial practices in the internal market and amending Council Directive 84/450/EEC, Directives 97/7/EC, 98/27/EC and 2002/65/EC of the European Parliament and of the Council and Regulation (EC) No 2006/2004 of the European Parliament and of the Council ('Unfair Commercial Practices Directive')' (2005) *Official Journal* L 149, 11.6.2005, pp. 22–39 [Online]. Available at: http://data.europa.eu/eli/dir/2005/29/oj (Accessed: 29 January 2025).

'Directive 2009/48/EC of the European Parliament and of the Council of 18 June 2009 on the safety of toys' (2009) *Official Journal L 170, 30 June, pp. 1–37* [Online]. Available at: http://data.europa.eu/eli/dir/2009/48/oj (Accessed: 28 January 2025).

Doezema, T. and Frahm, N. (2023) 'The law isn't lagging behind AI. It's leading it', *The New Atlantis*. Available at: https://www.thenewatlantis.com/publications/how-the-state-built-this-ai-moment (Accessed: 28 January 2025).

Dul, C. (2022) 'Facial recognition technology vs privacy: the case of Clearview AI', *Queen Mary Law Journal*, 3, pp. 1–24.

Ebers, M., Hoch, V.R.S., Rosenkranz, F., Ruschemeier, H. and Steinrötter, B. (2021) 'The European Commission's proposal for an Artificial Intelligence Act – a critical assessment by members of the Robotics and AI Law Society (RAILS)', *J*, 4(4), pp. 589–603.

EDPS (2024, May 24) *European Commission's use of Microsoft 365 infringes data protection law for EU institutions and bodies*. EDPS [Online]. Available at: https://www.edps.europa.eu/press-publications/press-news/press-releases/2024/european-commissions-use-microsoft-365-infringes-data-protection-law-eu-institutions-and-bodies (Accessed: 28 January 2025).

Edwards, L. (2022a) *Expert explainer: the EU AI Act proposal*. Ada Lovelace Institute, 8 April [Online]. Available at: https://www.adalovelaceinstitute.org/resource/eu-ai-act-explainer/ (Accessed: 28 January 2025).

Edwards, L. (2022b) *Expert opinion: regulating AI in Europe*. Ada Lovelace Institute, 31 March [Online]. Available at: https://www.adalovelaceinstitute.org/report/regulating-ai-in-europe/ (Accessed: 28 January 2025).

Edwards, L. (2022c) *The EU AI Act: a summary of its significance and scope*. Ada Lovelace Institute [Online]. Available at: https://www.adalovelaceinstitute.org/ (Accessed: 28 January 2025).

Elmer, G. (2003) *Profiling machines. Mapping the Personal Information Economy.* Cambridge (MA): The MIT Press.

Ernst, C. (forthcoming) In *The Realities of Autonomous Weapon Systems*, in Bächle, T.C. and Bareis, J. (eds.) Bristol: Bristol University Press.

European Commission (2008) *New legislative framework*. European Commission [Online]. Available at: https://single-market-economy.ec.europa.eu/single-market/goods/new-legislative-framework_en (Accessed: 28 January 2025).

European Commission (2020a) *Op-ed by Commission President von Der Leyen*. European Commission [Online], 19 February. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ac_20_260 (Accessed: 28 January 2025).

European Commission (2020b) Assessment List for Trustworthy Artificial Intelligence (ALTAI) for self-assessment. Available at: https://digital-strategy.ec.europa.eu/en/library/assessment-list-trustworthy-artificial-intelligence-altai-self-assessment (Accessed: 28 January 2025).

European Commission (2020c) *White paper on artificial intelligence: a European approach to excellence and trust*. European Commission [Online]. Available at: https://commission.europa.eu/publications/white-paper-artificial-intelligence-european-approach-excellence-and-trust_en (Accessed: 28 January 2025).

European Commission (2021) *Commission staff working document proposal for a Regulation of the European Parliament and of the Council, SWD/2021/84 Final*. European Commission [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52021SC0084 (Accessed: 28 January 2025).

European Commission (2023) *European Chips Act*. European Commission, 21 September [Online]. Available at: https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en (Accessed: 28 January 2025).

European Commission (2024, April 21) *Shaping Europe's digital future*. European Commission [Press release] [Online]. Available at: https://digital-strategy.ec.europa.eu/en (Accessed: 28 January 2025).

European Commission (no date) *C(2023)3215 – Standardisation request M/593* [Online] Available at: https://ec.europa.eu/growth/tools-databases/enorm/mandate/593_en (Accessed: 28 January 2025).

European Data Protection Board (2021) *EDPB-EDPS joint opinion 5/2021 on the proposal for a regulation of the European Parliament and of the Council laying down harmonised rules on artificial intelligence (Artificial Intelligence Act).* European Data Protection Board, 18 June [Online]. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/edpbedps-joint-opinion/edpb-edps-joint-opinion-52021-proposal_en (Accessed: 28 January 2025).

European Group on Ethics in Science and New Technologies (2018) *Artificial intelligence, robotics and 'autonomous' systems*. European Commission [Online]. Available at: https://lefis.unizar.es/wp-content/uploads/EGE_Artificial-Intelligence_Statement_2018.pdf (Accessed: 28 January 2025).

Fisher, M. (2022) *The chaos machine: the inside story of how social media rewired our minds and our world*. Boston and New York: Little Brown and Company.

Frahm, N. and Schiølin, K. (2023) 'Toward an "ever closer union": the making of AI-ethics in the EU', *STS Encounters*, 15(2) [Online]. Available at: https://doi.org/10.7146/stse.v15i2.139808 (Accessed: 28 January 2025).

Gamito, M.C. and Marsden, C. T. (2024) Artificial intelligence co-regulation? The role of standards in the EU AI Act. *International Journal of Law and Information Technology*, *32*(1) [Online]. Available at: https://doi.org/10.1093/ijlit/eaae011 (Accessed: 28 January 2025).

Gless, S. and Janal, R. (2023) '§ 2 Anwendungsbereich und Adressaten' in E. Hilgendorf and D. Roth-Isigkeit (eds.) *Die neue Verordnung der EU zur Künstlichen Intelligenz: Rechtsfragen und Compliance*. Munich: C.H. Beck, pp. 15-33.

Goh, H.-H. and Vinuesa, R. (2021) 'Regulating artificial-intelligence applications to achieve the sustainable development goals', *Discover Sustainability*, 2(52) [Online]. Available at: https://doi.org/10.1007/s43621-021-00064-5 (Accessed: 28 January 2025).

Guijarro Santos, V. (2023) 'Nicht Besser als Nichts. Ein Kommentar zum KI Verordnungsentwurf', *Zeitschrift Für Digitalisierung Und Recht*, 1, pp. 23–42.

Hacker, P. (2018) 'Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law', *Common Market Law Review*, 55(4), pp. 1143–1185.

Hallensleben, S. and Hustedt, S. (2020) *From principles to practice. An interdisciplinary framework to operationalise AI ethics*. Bertelsmann Stiftung [Online]. Available at: https://www.bertelsmann-stiftung.de/fileadmin/files/BSt/Publikationen/GrauePublikationen/WKIO_2020_final.pdf (Accessed: 28 January 2025).

Hartmann, T. (2023) *AI Act: French government accused of being influenced by lobbyist with conflict of interests*. Euractiv, 21 December [Online]. Available at: https://www.euractiv.com/section/artificial-intelligence/news/ai-act-french-government-accused-of-being-influenced-by-lobbyist-with-conflict-of-interests/ (Accessed: 28 January 2025).

Heaven, D. (2020) 'Why faces don't always tell the truth about feelings', *Nature*, 578(7796), pp. 502–504.

Hill, K. (2022) 'The secretive company that might end privacy as we know it' in Martin, K. (ed.) *Ethics of Data and Analytics. Concepts and Cases.* New York: Auerbach Publications, pp. 170-178.

Hood, C., Rothstein, H. and Baldwin, R. (2001) *The government of risk: understanding risk regulation regimes*. Oxford: Oxford University Press.

Hong, S.-H. (2020) *Technologies of speculation*. New York: New York University Press.

Kello, L. (2017) *The virtual weapon and international order*. New Haven: Yale University Press.

Kemp, S. (2023) *Digital 2023: Global overview report* [Online]. Available at: https://datareportal.com/reports/digital-2023-global-overview-report (Accessed: 28 January 2025).

Kergueno, R., Aiossa, R., Pearson, L., Corser, N.S., Teixeira, V. and van Hulten, M. (2021b) *Deep pockets, open doors*. Transparency International EU [Online]. Available at: https://transparency.eu/wp-content/uploads/2024/10/Deep_pockets_open_doors_report.pdf (Accessed: 28 January 2025).

Koloßa, S. (2020) 'The GDPR's extra-territorial scope. Data protection in the context of international law and human rights law', *ZaöRV*, 4, pp. 791–818.

Krarup, T. and Horst, M. (2023) 'European artificial intelligence policy as digital single market making', *Big Data and Society*, 10(1) [Online]. Available at: https://doi.org/10.1177/20539517231153811 (Accessed: 28 January 2025).

Kreiß, C. (2019) 'Ethik-Institut an der TU München: Ein vielsagender geheimer Vertrag mit Facebook', *Der Tagesspiegel Online*, 19 December [Online]. Available at: https://www.tagesspiegel.de/wissen/ein-vielsagender-geheimer-vertrag-mit-facebook-4129213.html (Accessed: 28 January 2025).

Krügel, S., Ostermaier, A. and Uhl, M. (2022) 'Zombies in the loop? Humans trust untrustworthy AI-advisors for ethical decisions', *Philosophy and Technology*, 35(1), pp. 1–37.

Laux, S., Wachter, J. and Mittelstadt, B. (2023) 'Trustworthy artificial intelligence and the European Union AI Act: on the conflation of trustworthiness and acceptability of risk', *Regulation and Governance*, 18(1), pp. 3–32.

Von der Leyen, U. (2019) *Speech by President-elect Ursula von der Leyen at the 2019 Paris Peace Forum* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/speech_19_6270 (Accessed: 28 January 2025).

Liberties, ECF and ECNL (2023) *Open Letter. The AI Act must protect the rule of law* [Online]. Available at: https://ecnl.org/sites/default/files/2023-09/AI_and_RoL_Open_Letter_final_27092023.pdf (Accessed: 28 January 2025).

Mackenzie, A. (2015) 'The production of prediction: what does machine learning want?' *European Journal of Cultural Studies*, 18(4–5), pp. 429–45.

Mager, A., Norocel, O.C. and Rogers, R. (2023) 'Advancing search engine studies: the evolution of Google critique and intervention', *Big Data and Society*, 10(2) [Online]. Available at: https://doi.org/10.1177/20539517231191528 (Accessed: 28 January 2025).

Malgieri, G. and Pasquale, F. (2024) 'Licensing high-risk artificial intelligence: toward ex ante justification for a disruptive technology', *Computer Law and Security Review*, 52(105899) [Online]. Available at: https://doi.org/10.1016/j.clsr.2023.105899 (Accessed: 28 January 2025).

Mantelero, A. (2024) 'The Fundamental Rights Impact Assessment (FRIA) in the AI Act: Roots, legal obligations and key elements for a model template', *Computer Law & Security Review*, *54*(106020) [Online]. Available at: https://doi.org/10.1016/j.clsr.2024.106020 (Accessed: 28 January 2025).

Mantelero, A. (2022) 'Fundamental rights impact assessments in the DSA', *Verfassungsblog*, November [Online]. Available at: https://doi.org/10.17176/20221101-220006-0 (Accessed: 28 January 2025).

'Meta Platforms Inc and Others v Bundeskartellamt' (2023) Judgment of the Court (Grand Chamber) of 4 July 2023. Case C-252/21. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252 (Accessed: 29 January 2025).

Metz, C. (2023) 'Chatbots may "hallucinate" more often than many realize', *The New York Times*, 6 November [Online]. Available at: https://www.nytimes.com/2023/11/06/technology/chatbots-hallucination-rates.html (Accessed: 28 January 2025).

Mittelstadt, B. (2019) 'Principles alone cannot guarantee ethical AI', *Nature Machine Intelligence*, 1(11), pp. 501–507.

Mogherini, F., Timmermans, F. and Domecq, J. (2016) *Implementation plan on security and defence. Note 14392/16*. Council of the European Union [Online]. Available at: https://www.consilium.europa.eu/media/22460/eugs-implementation-plan-st14392en16.pdf (Accessed: 28 January 2025).

Mühlhoff, R. (2023) 'Predictive privacy: collective data protection in the context of artificial intelligence and big data', *Big Data and Society*, 10(1), [Online]. Available at: https://doi.org/10.1177/20539517231166886. (Accessed: 28 January 2025).

Mühlhoff, R. and Ruschemeier, H. (2024a) 'Predictive analytics and the collective dimensions of data protection', *Law, Innovation and Technology*, 16(1), pp. 261–292.

Mühlhoff, R. and Ruschemeier, H. (2024b) 'Regulating AI with purpose limitation for models', *Journal of AI Law and Regulation*, 1(1), pp. 24–39.

Mühlhoff, R. and Ruschemeier, H. (2024c) 'Updating purpose limitation for AI: a normative approach from law and philosophy'. *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.4711621 (Accessed: 28 January 2025).

Mühlhoff, R. and Ruschemeier, H. (2024d). 'KI-Regulierung durch Zweckbindung für Modelle', ZfDR (4), pp. 337-364.

Murray, T., Cheong, M. and Paterson, J. (2023, July 10) *The flawed algorithm at the heart of Robodebt*. Pursuit [Online]. Available at: https://pursuit.unimelb.edu.au/articles/the-flawed-algorithm-at-the-heart-of-robodebt (Accessed: 28 January 2025).

Neuwirth, R.J. (2023) 'Prohibited artificial intelligence practices in the proposed EU Artificial Intelligence Act (AIA)', *Computer Law and Security Review*, 48(April), [Online]. Available at: https://doi.org/10.1016/j.clsr.2023.105798 (Accessed: 28 January 2025).

Orwat, C., Bareis, J., Folberth, A., Jahnel, J. and Wadephul, C. (2024). Normative challenges of risk regulation of artificial intelligence. *NanoEthics*, *18*(11) [Online]. Available at: https://doi.org/10.1007/s11569-024-00454-9 (Accessed: 28 January 2025).

OECD (2019) *AI principles overview*. OECD [Online]. Available at: https://oecd.ai/en/principles (Accessed: 28 January 2025).

Pathak, G. (2022) 'Manifestly made public: Clearview and GDPR', *European Data Protection Law Review (EDPL)*, 8(3), pp. 419-422.

Paul, R. (2021) *Varieties of risk analysis in public administrations: Problem-solving and polity policies in Europe*. New York: Routledge.

Paul, R. (2023) 'European artificial intelligence "trusted throughout the world": risk-based regulation and the fashioning of a competitive common AI market', *Regulation and Governance*, 18(4), pp. 1065–1082.

'Public.Resource.Org, Inc. and Right to Know CLG v European Commission' (2024) Judgment of the Court (Grand Chamber) of 5 March 2024. Case C-588/21 P. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62021CJ0588 (Accessed: 29 January 2025).

Qian, I., Xiao, M., Mozur, P. and Cardia, A. (2022) 'Four takeaways from a *Times* investigation into China's expanding surveillance state', *The New York Times*, 21 June [Online]. Available at: https://www.nytimes.com/2022/06/21/world/asia/china-surveillance-investigation.html (Accessed: 28 January 2025).

'Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October, 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)' (2022) *Official Journal* L 277, 27 October [Online]. Available at: http://data.europa.eu/eli/reg/2022/2065/oj (Accessed: 29 January 2025).

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L, 2024/1689, 12 July [Online]. Available at: http://data.europa.eu/eli/reg/2024/1689/oj (Accessed: 29 January 2025).

Rezende, I.N. (2020) 'Facial recognition in police hands: assessing the "Clearview Case" from a European perspective', *New Journal of European Criminal Law*, 11(3), pp. 375–389.

Ridgway, R. (2023) 'Deleterious consequences: how Google's original sociotechnical affordances ultimately shaped "trusted users" in surveillance capitalism', *Big Data and Society*, 10(1) [Online]. Available at: https://doi.org/10.1177/20539517231171058 (Accessed: 28 January 2025).

Rodríguez Codesal, P. (2024) '*"De-risking". Approach to the concept and study of the possible consequences of a strategically autonomous policy of the European Union*. Repositoria Comillas [Online]. Available at: https://repositorio.comillas.edu/xmlui/handle/11531/79540 (Accessed: 28 January 2025).

Ruschemeier, H. (2022) 'Privacy als Paradox? Rechtliche Implikationen verhaltenspsychologischer Erkenntnisse' in Friedewald, M. et al. (eds), *Künstliche Intelligenz, Demokratie und Privatheit*. Baden-Baden: Nomos, pp. 211–238.

Ruschemeier, H. (2023a) 'AI as a challenge for legal regulation – the scope of application of the Artificial Intelligence Act proposal', *ERA Forum*, 23(3), pp. 361–376.

Ruschemeier, H. (2023b) *Regulierung von KI*. Bundeszentrale für politische Bildung [Online]. Available at: https://www.bpb.de/shop/zeitschriften/apuz/kuenstliche-intelligenz-2023/541498/regulierung-von-ki/ (Accessed: 28 January 2025).

Ruschemeier, H. (2023d) 'Squaring the circle: ChatGPT and data protection', *Verfassungsblog*, 7 April [Online]. Available at: https://verfassungsblog.de/squaring-the-circle/ (Accessed: 28 January 2025).

Ruschemeier, H. (2023e) 'The problems of the automation bias in the public sector: a legal perspective', *Weizenbaum Conference Proceedings 2023. AI, Big Data, Social Media, and People on the Move*, Weizenbaum Institute, pp. 59–69 [Online]. Available at: https://doi.org/10.34669/wi.cp/5.6 (Accessed: 28 January 2025).

Ruschemeier, H. (2024a) 'Generative AI and data protection'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=4814999 (Accessed: 28 January 2025).

Ruschemeier, H. (2024b) 'Prediction power as a challenge for the rule of law'. *SSRN* [Online]. Available at: https://ssrn.com/abstract=4888087 (Accessed: 28 January 2025).

Ruschemeier, H. (2024c) 'Thinking Outside the Box?' in Steffen, B. (ed) *Bridging the Gap Between AI and Reality. First International Conference, AISoLA 2023, Crete, Greece, October 23–28, 2023, Proceedings*. Cham: Springer, pp. 318-332.

Ruschemeier, H. and Hondrich, L. (2024) 'Automation bias in public administration – an interdisciplinary perspective from law and psychology'. *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.4736646 (Accessed: 29 January 2025).

Ruschemeier, H. and Mühlhoff, R. (2023) 'Daten, Werte Und Der AI Act: Warum Wir Mehr Ethik Für Bessere KI-Regulierung Brauchen', *Verfassungsblog*, 15 December [Online]. Available at: https://verfassungsblog.de/daten-werte-und-der-ai-act/ (Accessed: 29 January 2025).

Sandin, P. (1999) 'Dimensions of the precautionary principle', *Human and Ecological Risk Assessment: An International Journal*, 5(5), pp. 889–907.

Schyns, C. (2023) *The lobbying ghost in the machine: Big Tech's covert defanging of Europe's AI Act*. Brussels: Corporate Europe Observatory.

Siegmann, C. and Anderljung, M. (2022) *The Brussels effect and artificial intelligence: How EU regulation will impact the global AI market*. Centre for the Governance of AI [Online]. Available at: http://arxiv.org/abs/2208.12645 (Accessed: 29 January 2025).

Smuha, N.A. (2021) 'From a "race to AI" to a "race to AI regulation": regulatory competition for artificial intelligence', *Law, Innovation and Technology*, 13(1), pp. 57–84.

Smuha, N.A., Ahmed-Rengers, E., Harkens, A., Li, W., MacLaren, J., Piselli, R. and Yeung, K. (2021) 'How the EU can achieve legally trustworthy AI: a response to the European Commission's proposal for an Artificial Intelligence Act', *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.3899991 (Accessed: 29 January 2025).

Stahl, B.C., Rodrigues, R., Santiago, N. and Macnish, K. (2022) 'A European agency for artificial intelligence: Protecting fundamental rights and ethical values', *Computer Law and Security Review*, 45(July) 105661 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105661 (Accessed: 29 January 2025).

Suchman, L. (2023) 'The uncontroversial "thingness" of AI', *Big Data and Society*, 10(2) [Online]. Available at: https://doi.org/10.1177/20539517231206794 (Accessed: 29 January 2025).

Summers, R.S. (1998) 'Principles of the rule of law', *Notre Dame Law Review*, 74, pp. 1691–1712.

'Treaty on the Functioning of the European Union' (2012) *Official Journal* C 326, 26 October, pp. 47-390 [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF (Accessed: 29 January 2025).

UK Government (2021) *How to score attributes*. Gov.uk [Online]. Available at: https://www.gov.uk/government/publications/attributes-in-the-uk-digital-identity-and-attributes-trust-framework/how-to-score-attributes (Accessed: 29 January 2025).

United Nations (2023) *Interim report: governing AI for humanity*. United Nations [Online]. Available at: https://www.un.org/en/ai-advisory-body (Accessed: 29 January 2025).

Veale, M. and Borgesius, F.Z. (2021) 'Demystifying the draft EU Artificial Intelligence Act – analysing the good, the bad, and the unclear elements of the proposed approach', *Computer Law Review International*, 22(4), pp. 97–112.

Veale, M., Matus, K. and Gorwa, R. (2023) 'AI and global governance: modalities, rationales, tensions', *Annual Review of Law and Social Science*, 19(October), pp. 255–275.

Van der Vlist, F., Helmond, A. and Ferrari, F. (2024) 'Big AI: cloud infrastructure dependence and the industrialisation of artificial intelligence', *Big Data and Society*, 11(1), pp. 1–16.

Wachter, S. (2023) 'The theory of artificial immutability: protecting algorithmic groups under anti-discrimination law', *Tulane Law Review*, 97(2) [Online]. Available at: https://www.tulanelawreview.org/pub/artificial-immutability (Accessed: 29 January 2025).

Weber, J. and Suchman, L. (2016) 'Human–machine autonomies' in Bhuta, N., Beck, S., Geiβ, R., Liu, H.-Y. and Kreβ, C. (eds.) *Autonomous weapons systems*. Cambridge: Cambridge University Press, pp. 75–102.

Wendehorst, C. and Duller, Y. (2021) 'Biometric recognition and behavioral detection'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=4087455 (Accessed: 29 January 2025).

Whittaker, M. (2021) 'The steep cost of capture', *Interactions*, 28(6), pp. 50–55.

Wong, P.-H. (2020) 'Democratizing algorithmic fairness', *Philosophy and Technology*, 33(2), pp. 225–244.

Accountable AI: It Takes Two to Tango

Jorge Constantino

Abstract

This Chapter argues that accountable artificial intelligence (AI) requires examining the role of humans in AI development and deployment. Hence, it discusses the importance of addressing the obligations of deployers and developers of AI systems to achieve accountable AI. The EU AI Act has implemented measures such as transparency or technical obligations to achieve such accountability. Similarly, it has implemented human oversight requirements outlined in Arts. 14 and 26 against high-risk AI systems. Some scholars and practitioners may argue that Art. 14 only applies to developers of AI systems. However, we understand that human oversight requirements govern both actors. Human oversight cannot be applied in isolation by requiring compliance of only one party. Otherwise, it would defeat the purpose of adding human control features to prevent AI systems from harming fundamental rights. Based on this perspective, we propose that (at least) two actors are required to make accountable AI more tangible. Nonetheless, we are conscious that this legislation is in its infancy, and only time will tell how human oversight obligations (Arts. 14 and 26) are to be applied – whether in isolation or in conjunction.

1. An introduction to AI systems

Artificial intelligence (AI) is currently used in the public and private sectors in such fields as policing, the judicial system, employment, taxes and finances, retailers, media, and entertainment (Maclure, 2020, pp. 2–3; Sipola et al, 2024, p. 5). The definition or conceptualisation of AI is far from settled (Kuziemski and Misuraca, 2020, p. 2). For instance, AI may be simply defined as computers or machines showing human-like intelligence (Simmons and Chappell, 1988, p. 14) (DK, 2023, p. 7). Alternatively, some academics have described AI as the umbrella term that refers to a set of algorithmic models, methods, or instructions given to a computer

system to simulate human intelligence (Köchling and Wehner, 2020, p. 798; Muthukrishnan et al, 2020, p. 393). Thus, for the purpose of this study, it may be helpful to refer to the definition of AI found in the EU's AI Act (Regulation 2024/1689), which refers to a machine-learning system designed with different levels of autonomy that requires inputs to produce outputs influencing the physical or virtual environment with which they interact.[1] Similarly, according to Muthukrishnan et al (2020, pp. 394–395), machine learning is a subfield of AI that involves some form of learning using data samples.

Following the AI Act's proposed definition, we may agree that AI comes in different *forms* and *shapes*; for example, machine learning, not being fully autonomous, requires human intervention to learn from algorithms or datasets and be able to solve tasks (Kowalski, 1979, p. 424; Hill, 2016, pp. 35–36, 58). Thus, while some AI advocates may preach that AI resembles (or even surpasses) human intelligence, the reality is that AI (or, at least, machine learning) is not always fully autonomous. We may argue that human intervention will always be needed for an AI system to come alive and work as an "intelligent" thing (Lennox, 2020, pp. 53–61). Nonetheless, the "intelligence" of such systems is not the focus of this Chapter. Rather, our argument is that to examine accountable AI systems, it is necessary to analyse the human factor in the process of their development and deployment. For instance, what would be the cause and result of AI failures: designers, deployers, or the machine itself? (Edwards, Schafer and Harbinja, 2020, p. 310) Thus, to guide our analysis, we have formulated the following question: "what accountability measures has the European AI Act implemented to protect fundamental rights against harmful AI?" In the following paragraphs, we attempt to provide some answers, arguing that, at this very stage, machines or AI systems have no legal capacity to be held accountable themselves. Thus, at least for now, accountable AI requires examining the roles of two human actors: developers and deployers (Constantino, 2022, p. 2). Thus, we argue that it takes two to tango in accountable AI.

2. AI systems in our societies: good and bad AI?

AI systems can positively impact our societies (Henao, 2021), help fight crime (Eligon and Williams, 2015), assist in having more efficient services

1 This is an adapted definition from the European AI Act. Please refer to Art. 3 EU AI Act for a full definition.

(Linden, 2021, p. 2), be more cost-effective (Le Sueur, 2015, pp. 3, 18), and even – as some have argued – offer less discriminatory results compared to human decision-makers (Chander, 2017, p. 1027; Clifford, 2017, p. 94; Hacker, 2018, p. 3). Similarly, AI systems can be used to establish risk scores regarding tax and welfare fraud and unlawful immigration (Maclure, 2020, pp. 2–3).

AI systems are currently used in the public sector to make the bureaucratic system more responsive and simpler to citizens seeking social security assistance or lodging tax returns (Le Sueur, 2015, p. 3). From the broad use (or deployment) of AI systems in public sectors in different countries, we may come across two contested cases of their deployment in government: the Dutch experience with the *System Risico Indicatie* (SyRI) and the Australian experience with *Robodebt*. In the former, the SyRI deployed AI tools to identify citizens who may have potentially committed or may represent a risk of committing social security fraud (Wisman, 2020). SyRI had the legal and technological power to link and analyse citizens' personal data concerning work data, administrative fines, tax data, real estate and personal assets, housing, civic integration data, education data, social benefits, and subsidies (NJCM et al v. The Dutch State, 2020, p. 4.17). SyRI had the task of collecting and analysing citizens' data, preparing reports based on profiling people and providing a risk score regarding certain citizens, thereby warning the Dutch authorities of potential social services fraud (NJCM et al. v. The Dutch State, 2020, p. 4.17). As defended by the Dutch government, the implementation of the SyRI provided an advantage in targeting those who were committing fraud, and thereby damaging the country's economy and social security service (NJCM et al v. The Dutch State, 2020, p. 6.3, 6.76). However, the SyRI was found to be unlawful for numerous reasons, such as breaching human rights and privacy laws and the lack of transparency on the part of the Dutch government to reveal the inner workings and purpose of the AI system in use (NJCM et al v. The Dutch State, 2020, p. 6.5, 6.27, 6.32, 6.41).

A similar case occurred in Australia in 2016; the federal government rolled out an AI system labelled *Robodebt* to detect citizens who apparently received social security overpayments (Whiteford, 2021, p. 340). The *Robodebt* system collected data from former and current welfare beneficiaries and compared it against their annual tax income assessment to automatically ascertain any overpayment (Whiteford, 2021, pp. 341–342). Unfortunately, the automated system was built with inaccurate algorithms, leading to miscalculations. *Robodebt* shifted the burden of proof onto citi-

zens to demonstrate they were not overpaid; if a citizen could not prove that the automated system was incorrect, the system would generate a debt against that citizen (Human Rights Law Centre, 2021). In November 2019, the Australian Federal Court ruled that the *Robodebt* system was unlawful and ordered the Australian government to return the money unlawfully collected to recipients of welfare payments (Whiteford, 2021, p. 347). The Court held that the Australian government failed in its duty to citizens to oversee the correct functioning of *Robodebt*, and that the government had blindly relied upon the automated system without putting in place any human intervention to verify the accuracy of the AI system (Human Rights Law Centre, 2021).

AI systems are also being deployed in the private sector across different markets. For example, financial organisations use AI systems to assign risk score credit to applicants before deciding on whether to grant loans (Pasquale, 2015, p. 1; Chander, 2017, p. 1024). Amazon built an AI system to assist its human resources department in choosing the top five candidates out of hundreds of applicants (Winick, 2018). However, it has been reported that Amazon realised that its AI system negatively discriminated against women and preferred men as suitable candidates (Winick, 2018). Google offers AI systems that can help users collect, categorise, and automatically tag uploaded photos to simplify users' lives (Dougherty, 2015). However, it has been reported that Google's face recognition algorithm mistakenly labelled black people as gorillas due to insufficient training data on recognising black faces (Hacker, 2018, p. 7). Furthermore, in recent years, researchers have developed AI-supported care robots to monitor the elderly and assist with such basic tasks as reducing loneliness or ensuring that prescriptions are taken at the right time (Johansson-Pajala and Gustafsson, 2020, p. 167). For example, the robot PARO assists the elderly with dementia and Alzheimer's (Kelly et al, 2021). It is claimed that PARO can help in reducing stress and anxiety (Kang et al, 2020) and can detect patients' body temperature (Kang et al, 2020). However, as these medical devices are part of the Internet of Things (IoT), their functionality depends on data exchanges to connect with other compatible networks to support their operation (Ray, 2016, pp. 9489–9491). Thus, these medical devices are unfortunately exposed to cybersecurity vulnerabilities, such as patients' data being stolen by cybercriminals (Drukarch, Calleja and Fosch Villaronga, 2023, pp. 15–16).

Further to the above, there are numerous other examples of AI developments and deployments covering various applications across different

sectors, such as AI systems for intelligence, military, and national security purposes (Constantino and van der Linden, 2024, pp. 1–5; Barzashka, 2023, pp. 26–27), video surveillance through smart technology in the workplace to monitor production, safety, and control of employees entering and leaving the workplace (Rosenblat, Kneese and Boyd, 2014, pp. 2–3, 7–10). However, the above examples may be enough to illustrate the complexities and risks of AI systems in our societies, whether in Europe, the US, or Australia.

We can observe that AI systems may help fight fraud or crime. However, if an AI system is developed with inaccurate data or inherent bias from human developers, it is likely to pose a risk of discrimination or unfairness during its deployment (Edwards, Schafer and Harbinja, 2020, p. 238). For example, inaccurate data that feeds AI systems can contain prejudicial stigmas against certain groups of people, can contain racial discrimination, and can occasionally be tainted by unlawful practices (Richardson Schultz, and Crawford, 2019, p. 15). Historical data provided to AI systems can lead to discriminatory results, such as insufficient data or lack of robust data (Edwards, Schafer and Harbinja, 2020, p. 238; Chander, 2017, p. 1036). AI systems can capture and reproduce negative discrimination in their outputs and be contaminated by training data and natural operations in the real world, thereby leading to the reproduction of real-world negative discrimination towards citizens (Hacker, 2018, pp. 34–35). Moreover, even when AI systems are designed in a "neutral" manner, there is no guarantee that they will behave flawlessly (Hacker, 2018, p. 11). This begs the question, how lawful are these AI systems? Are faulty AI systems the result of reckless programming or poor deployment? (Richardson Schultz and Crawford, 2019, pp. 15, 48).

From the examples provided, we may argue that the SyRI reinforced further disparity and discrimination against those living in poverty and needing welfare assistance (Appelman, Ó Fathaigh and van Hoboken, 2021, p. 341). Faulty AI systems can harm society, and particularly its most vulnerable members (Maclure, 2020, p. 1044). Similarly, an AI system without the proper supervision of capable and willing humans is also likely to pose a risk to citizens who come into contact with it. For example, appropriate human oversight measures in the *Robodebt* system may have prevented fatal consequences that had endangered human life (Whiteford, 2021, p. 341). Without adequate measures to develop and deploy AI systems that support the core of human dignity, we may be left in a society where AI systems

are employed to oppress and target vulnerable citizens (Whiteford, 2021, p. 356).

Furthermore, AI systems deployed in our societies may pose other risks to fundamental rights, such as the right to privacy and data protection. For instance, surveillance in the workplace may be used for ill, such as in the harassment or exploitation of employees (Sykes, 2000). Deploying invasive technologies affects employees' right to privacy, even if deployed inside the workplace, because the employee is not expected to be monitored in the workplace (European Data Protection Board (EDPB), 2020, p. 13). Similarly, the healthcare industry will likely face AI challenges regarding liability when deploying care robots supported by AI systems, when being threatened by cyber-attacks (e.g., data breaches), putting patients' right to privacy at risk (Stephenson and Acklam, 2019, p. 282; Hage, 2017, pp. 255–271). These challenges affect, for instance, the right to respect for private life outlined by Art. 8 of the European Convention on Human Rights (ECHR). These issues not only affect individuals, but also societies, particularly where fundamental rights are at stake (Johansson-Pajala and Gustafsson, 2020, p. 170).[2] Thus, who is liable: the developer or the deployer? (Holzinger, 2016, pp. 119–131).

Lastly, the perspective that AI systems may be fully autonomous may lead to cunning legal arguments to escape developers' and deployers' responsibility (and liability), thereby shifting responsibility to AI systems that lack the legal personality to face accountability (Panezi, 2021, pp. 18–19). Therefore, we argue that, in the course of AI regulation, AI systems should not be viewed as machines acting independently. Rather, in order to prevent faulty AI systems, it is necessary to take a closer look at human participation in this complex ecosystem, which may offer, for now, appropriate accountability solutions (Maclure, 2020, p. 4). In the following section, we examine some key features of accountable AI revealed under the AI Act framework, and discuss whether they may be sufficient to adequately protect fundamental rights.

3. The approach of the EU AI Act to accountable AI

Before examining the AI Act's approach to regulating or introducing accountability measures to protect fundamental rights against harmful AI,

2 For further reading on the duty of governments to protect citizens' fundamental rights, see Barkhuysen and Van Emmerik (2019).

it may be helpful to briefly revise the different definitions or conceptualisations of accountability.

Accountability may have different meanings or interpretations across different jurisdictions and fields (Bovens, 2010, p. 949). Legal scholars may interpret accountability as responsibility, answerability, or liability (Docksey and Propp, 2023, pp. 2–3), while ethicists may frame it as a moral obligation of private and public organisations to provide an account for their actions (van de Poel et al, 2012, pp. 3–4). Moreover, accountability applied to public administration may be regarded as the government's (and its employees') obligation to exhibit high standards in public service (Newberry, 2015, p. 371). The AI Act itself does not go on to define or conceptualise accountability. However, it does acknowledge the conceptualisation of accountability found in the "Ethics Guidelines for Trustworthy AI" proposed by the High-Level Expert Group (HLEG) (Recital 27 AI Act). The HLEG establishes that accountability requires mechanisms to ensure responsibility for the outcomes of AI systems, both before and after development and deployment (European Commission, 2019, pp. 2, 19). Similarly, the OECD Council on AI has established that accountability in AI regulates the behaviour of actors to develop and deploy AI systems that fully comply with respect for fundamental rights (OECD, 2024, p. 5). Thus, we may argue that the view of accountability, not expressly stated but endorsed by the AI Act, is that accountability relates to the responsibility of developers and deployers to introduce AI systems into the European market that are not contrary to human dignity. This view of accountability is also close to the perspective of legal scholars who regard accountability as the legal responsibility of actors. We may take the opportunity to propose that accountability is essential in society to ensure actors' ownership of their actions. In a societal setting governed by the rule of law, accountability must apply to all actors without exceptions (Constantino and Wagner, 2024, p. 3).

Accountability mechanisms contemplated by the AI Act may include, for instance, introducing human agency and oversight binding requirements, where AI systems are developed and deployed as tools which respect human dignity (Recital 27 AI Act). This approach allows us to infer that the emphasis on providing accountable AI systems is on the human factor to develop and deploy AI systems aligned with human dignity (which, for example, respect fundamental rights). Accountable AI requires developers to build or place AI systems that can be appropriately controlled and overseen by humans (the deployers) (Recital 27 AI Act). Thus, it takes

two to tango: the developer to provide functioning AI systems and the deployer (user) to be able to conduct meaningful oversight by controlling or assessing the system and reporting malfunctions (Verdiesen, Santoni de Sio and Dignum, 2021, pp. 143–150, 159). At this stage, it may be worth highlighting that the scope of the AI Act applies to (or is binding on) providers, importers, manufacturers, and deployers (or users) of AI systems used in the EU (Art. 2 AI Act). For the purpose of our analysis, we group developers, importers, and manufacturers under the same category (i.e., developers), and categorise deployers as those organisations or persons that use AI systems for different tasks (e.g., public or private services).

When analysing the human factor in the discussion of accountable AI systems, we may think of humans from two different perspectives. The first relates to human responsibility as a developer of AI systems, considering that AI systems need human intervention as they cannot program themselves or emerge independently (MacKay, 2003). Hence, one may think of AI designers' obligation, or responsibility, to require them to develop products that are not harmful to fundamental rights. A second perspective is the human responsibility as a deployer of AI systems tasked with oversight duties during the deployment of AI systems to prevent or minimise their harmful outputs. This would mean that, in practice, or at least until a court case appears, human oversight responsibilities require human deployers to undertake effective continuous oversight to question and override wrongful AI outputs.

Accordingly, we note that the AI Act has implemented some binding requirements to foster an environment of accountability among the actors involved (developers and deployers). For instance, these requirements may compel developers to follow a risk-based approach to AI systems, where such systems could be categorised into prohibited tools (i.e., those which should not be brought to market), high-risk AI systems, and AI systems with limited risk to fundamental rights and European values (Hanif et al, 2023, pp. 353–354). Some other legislative measures that may promote accountability are the requirements of technical documentation (Art. 11 AI Act), record-keeping (Art. 12 AI Act), accuracy and robustness, and cybersecurity obligations (Art. 15 AI Act). Turning to the binding obligations of AI developers, we can see that, for example, Art. 15 of the AI Act seeks to promote robust AI systems to mitigate risks against citizens' health or other fundamental rights (e.g., data and privacy protection) (Recitals 59 and 75 AI Act). Perhaps the term "robustness", as used by the Act, also refers to accurate AI systems proven to be resilient against cyberattacks

(cybersecurity). The robustness of AI systems may also include appropriate datasets and non-bias (OECD, 2024, p. 9). Thus, we understand that Art. 15 interprets robustness as the system's resilience against cyberattacks and ability to provide accurate results, thus preventing errors, faults, or biased outputs that ultimately affect natural persons (Constantino, 2024, p. 404). We may interpret Art. 15 as an attempt to promote a playfield of accountability in innovation, at least binding on deployers (Mahler, 2021, p. 259; Novelli, Taddeo and Floridi, 2022, p. 9). However, there is still much to be seen in practice about the effectiveness (and consequences) of imposing these technical requirements when developing AI systems (Cooper et al, 2022, p. 864). The AI Act has left some gaps or unregulated areas where accountability is crucial. For instance, the Act has not regulated the development and deployment of AI in the intelligence, security, or defence sectors (Constantino and van der Linden, 2024, p. 1), thereby leaving room for different interpretations and standards regarding accountable practices regarding AI systems in these sectors and their effects on society.

The current literature has paid insufficient attention to the duties or responsibilities of deployers of AI systems under the AI Act – particularly the role and qualities of human oversight. In the following paragraphs, we dedicate some time to this matter. For instance, it is thought that Art. 14 only applies to developers of AI systems (Wachter, 2024, pp. 682–683; Demircan, 2023). However, what would be the purpose of introducing human oversight requirements only for developers of AI systems and exempting deployers? In this analysis, we argue that Art. 14 on human oversight obligations does – or, at least, should – apply to both developers and deployers of high-risk AI systems (Koivisto, Koulu and Larsson, 2024, pp. 14–19).[3] Thus, Art. 14 can be read in conjunction with the human oversight obligations outlined in Art. 26(2). For the purpose of our argument, it may be appropriate to read the wording of Art. 14 of the AI Act:

Article 14

Human oversight

1. High-risk AI systems shall be designed and developed in such a way, including with appropriate human-machine interface tools, that they can

3 Please note that Art. 14 obligations are connected to high-risk AI systems. Thus, the landscape for other AI systems not considered high-risk is not governed by human oversight obligations per Art. 14.

be effectively overseen by natural persons during the period in which they are in use.

2. Human oversight shall aim to prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system is used in accordance with its intended purpose or under conditions of reasonably foreseeable misuse, in particular where such risks persist despite the application of other requirements set out in this Section.
3. The oversight measures shall be commensurate with the risks, level of autonomy and context of use of the high-risk AI system, and shall be ensured through either one or both of the following types of measures:

   -(a) measures identified and built, when technically feasible, into the high-risk AI system by the provider before it is placed on the market or put into service; (b) measures identified by the provider before placing the high-risk AI system on the market or putting it into service and that are appropriate to be implemented by the deployer.
4. For the purpose of implementing paragraphs 1, 2 and 3, the high-risk AI system shall be provided to the deployer in such a way that natural persons to whom human oversight is assigned are enabled, as appropriate and proportionate:
   (a) to properly understand the relevant capacities and limitations of the high-risk AI system and be able to duly monitor its operation, including in view of detecting and addressing anomalies, dysfunctions and unexpected performance;
   (b) to remain aware of the possible tendency of automatically relying or over-relying on the output produced by a high-risk AI system (automation bias), in particular for high-risk AI systems used to provide information or recommendations for decisions to be taken by natural persons;
   (c) to correctly interpret the high-risk AI system's output, taking into account, for example, the interpretation tools and methods available;
   (d) to decide, in any particular situation, not to use the high-risk AI system or to otherwise disregard, override or reverse the output of the high-risk AI system;
   (e) to intervene in the operation of the high-risk AI system or interrupt the system through a "stop" button or a similar procedure that allows the system to come to a halt in a safe state.
5. For high-risk AI systems referred to in point 1(a) of Annex III, the measures referred to in paragraph 3 of this Article shall be such as to ensure that, in addition, no action or decision is taken by the deployer

> on the basis of the identification resulting from the system unless that identification has been separately verified and confirmed by at least two natural persons with the necessary competence, training and authority. The requirement for a separate verification by at least two natural persons shall not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control or asylum, where Union or national law considers the application of this requirement to be disproportionate.

The wording of Section 1 of Art. 14 is straightforward. It requires developers to design AI systems that allow human intervention. We may agree that this piece of legislation effectively compels designers to develop tools or processes to allow deployers to conduct effective human oversight to avoid harmful AI that may jeopardise fundamental rights (European Commission, 2019, p. 4). Interestingly, this section refers to natural persons (humans in the loop) to effectively oversee AI systems during deployment. Thus, in principle, Art. 14(1) targets deployers (or designers) of AI systems. However, human oversight requires two actors in this equation in order to have effective human oversight. It is worth noting that the EU legislator is unclear about what "effective" oversight by natural persons means or what responsibilities or actions humans in the loop need to take to make human oversight effective (See Art. 14(1) of the AI Act). Nonetheless, human oversight responsibilities cannot be charged or tasked to one actor, otherwise, it would be pointless to require AI systems built with human oversight interface capabilities but not having actual humans tasked to execute or operationalise them. The previous statement may be supported by the wording of Art. 26(2), which sets an obligation on deployers of AI systems to "assign human oversight to natural persons".[4] Moving forward, Art. 14(2) establishes that the aim of having humans in the loop is to "prevent or minimise the risks to health, safety or fundamental rights that may emerge when a high-risk AI system [are in] used… under conditions of reasonably foreseeable misuse" (Art. 14(2)). The wording provided by the legislator is quite interesting. Firstly, it establishes that "humans in the loop" are there to minimise or prevent the possible harms of high-risk AI systems. Art. 14(2) does not say that AI systems should be built with *self-human-oversight* capabilities to minimise or prevent risks to health, safety, or fundamental rights. Instead, it says that humans have the responsibility to exercise such

4 See Art. 26(2): "Deployers shall assign human oversight to natural persons who have the necessary competence, training and authority, as well as the necessary support".

control. Secondly, the article chooses an intriguing phrase, "reasonably foreseeable", which refers to a doctrine that has been primarily applied to the duty of humans (particularly in tort law) to foresee potential risks (Leiman, 2021, p. 252).

Thus, it is unlikely that an AI system with no legal personality or that is incapable of "thinking" outside the box will be tasked with reasonableness and foreseeability (Kowert, 2017, pp. 182–185; Leiman, 2021, pp. 251–253). Hence, it appears that this piece of legislative instrument, at least, paves the way to ascertain the responsibility of deployers to conduct or engage with human oversight. Of course, we are of the view that the framework for human oversight responsibilities established in Art. 14 is to be read in conjunction with Art. 26(2). As the AI Act is very new legislation, there is still room to test Art. 14(2) in court to argue that it provides legal scope to require deployers (users) of AI systems to oversee AI systems to avoid risks to health, safety, and fundamental rights. Art. 14(3) is straightforward and outlines developers' responsibilities to build AI systems that can allow human-machine interface tools to support human oversight or enable deployers to fulfil their human oversight duties. It may be worth questioning what would happen if a deployer could not conduct human oversight due to the system not having been designed or developed with such technical measures. Then, it is plausible that, under Art. 14(3), deployers may claim non-responsibility for operationalising human oversight obligations.

To complicate the fulfilment of human oversight to foster accountable AI, Art. 14(4) is being drafted almost like a spaghetti. This piece of legislation outlines that human oversight is assigned to natural persons deploying high-risk systems; however, this task (which includes preventing or minimising risks to health, safety, or fundamental rights) is subject to the developer's ability to build high-risk AI systems that enable such natural persons to conduct human oversight. Art. 14(4) almost implies that developers are solely responsible for enabling or allowing compliance with human oversight duties. For instance, Art. 14(4) establishes that understanding the limitations of the high-risk AI and being able to duly monitor them (lit a), remain aware of overreliance (automation bias) (lit b), decide whether to use, disregard, or question high-risk AI system's outputs, would depend on how said systems are built (lit d). The binding obligations set out in Art. 14(4) are, arguably, contradictory to Art. 4, which clearly establishes that it is the responsibility of both "*providers and deployers* of AI systems [to] take measures to ensure, to their best extent, a sufficient level of *AI literacy* of their *staff and other persons* dealing with the operation and use

[or deployment] of AI systems on their behalf, taking into account their technical knowledge, experience, *education and training* and the context the AI systems are to be used [deployed] in, and considering the persons or groups of persons on whom the AI systems are to be used [deployed]." Thus, it may be appropriate to remind deployers and developers of their obligations, at least under Art. 4, to compel them to employ humans (developers and deployers) with a minimum level of AI literacy (e.g., understanding the ins and outs of algorithmic behaviour) to enable effective human oversight (Neumann, Guirguis and Steiner, 2022, p. 5). The reasoning behind enforcing AI literacy requirements is to have developers and deployers aware of AI capabilities and flaws so they can take appropriate human oversight measures that satisfy an environment of accountability (Green, 2022, pp. 1–3; see also Recitals 20 and 91 AI Act). Lastly, Art. 14(5) also emphasises the requirement of having (at least two) natural persons with the necessary "competence, training and authority" (Article 14(5) AI Act), to conduct oversight in cases of high-risk AI systems outlined in Annex III, point 1(a). This final piece of Art. 14 would allow us to argue that deployers are responsible for including natural persons as part of the human oversight framework. Strangely enough, Art. 14(5) does not apply to high-risk AI systems used for the purposes of law enforcement, migration, border control, or asylum.

To conclude, it may be fair to state that applying Art. 14 of the AI Act will present accountability challenges, such as at what stage and how humans in the loop (deployers) are to intervene or conduct oversight to prevent undesirable AI outputs (Constantino, 2022, p. 12). There is still uncertainty regarding the scope of human oversight for both developers and deployers. Blame shifting may arise and perhaps result in there being too many actors involved in the AI chain, leading to accountability loopholes or gaps (Van de Poel et al, 2012, p. 50). However, fostering AI awareness or education among deployers may provide positive steps toward effective human oversight. AI awareness promotes having more skilled humans who can be prepared to question the AI system, humans who can divert from AI outputs, even in cases where a developer fails or forgets to add technical measures to foster human oversight. Thus, the developer and deployer are responsible for enabling or fostering AI literacy that contributes to effective human oversight. There are no straightforward answers about the *perfect* solution to accountable AI. However, to alleviate current accountability loopholes, promoting and adopting a culture of accountability may be welcomed where the different actors involved in the AI chain can hold each other

accountable for their actions (Wagner, de Gooyert and Veeneman, 2023, p. 6). We should also welcome continuous independent human oversight that focuses not on blaming other humans for the faults of AI systems, but rather on an approach that educates others on the acceptable practices regarding the development and deployment of AI systems (Constantino and Wagner, 2024, pp. 8, 14–15). These reasonable approaches to accountability can provide a strong way forward to protect fundamental rights. Lastly, in industries or organisations where the AI Act is not enforceable, other regulations, such as national and international frameworks, can be applied to protect citizens' fundamental rights (Linden, 2021, pp. 5–6). Thus, the absence of regulation should not be an excuse for those willing actors interested in accountability principles.

4. Conclusion

In this Chapter, we have argued that AI systems, at least for now, cannot emerge without human intervention. Thus, we must focus on regulating humans as developers and deployers of AI systems instead of shifting the discussion onto the responsibility of AI systems as if they were fully autonomous beings or capable of legal personality.

The experiences from the last decade have left us with various lessons, such as evaluating AI's effects (negative and positive) on society. AI can be very useful in providing faster and more efficient services to humans, but it can also cause lethal outcomes. For example, while they can help fight crime, it is also clear that AI systems can threaten fundamental rights when they are wrongly or poorly designed and deployed in our societies. Thus, AI systems can discriminate, target vulnerable people, and even breach our privacy. To solve these dilemmas affecting European citizen's fundamental rights, the EU AI Act promotes a framework where developers and deployers of AI systems are charged with certain obligations to close accountability gaps, such as imposing technical requirements onto deployers of AI systems to consider technical documentation, accuracy and robustness, and cybersecurity obligations. At the human level, the AI Act has also considered including human oversight as part of the framework that allows accountability. Human oversight is covered preliminarily in Arts. 14 and 26. However, it is currently being disputed whether, for instance, Art. 14 (human oversight) only regulates developers and exempts deployers from human oversight obligations. We have argued that it takes two (to

tango) for accountable AI, meaning that Arts. 14 and 26 (human oversight) should be read together when studying and arguing for the responsibility of both "humans in the loop" (developers and deployers). Developers are responsible for enabling human oversight measures to be incorporated into their AI systems, and deployers are responsible for conducting effective human oversight when they or their organisations use an AI system. This approach can enable effective accountability, promoting citizens' trust when interacting with AI systems (Van Kolfschooten and Shachar, 2023, pp. 1–3; Ng et al, 2020, pp. 7–12). It is hoped that such measures as technical and human requirements will foster accountability among developers and deployers of AI systems, requiring them to introduce AI systems into the European market that are not harmful to humans (Cooper et al, 2022). For instance, rather than blaming computers for their outputs, humans in the loop will be required to move towards a more meaningful human oversight to prevent faulty AI systems and offer explanations to citizens.

Accountable AI may translate as developers' and deployers' joint moral and legal responsibility to allow non-harmful AI in the market. Thus, accountable AI will not be achieved only by adding algorithmic design requirements on developers or designers. Accountability also requires skilled AI deployers to oversee AI systems effectively. Whether the EU AI Act would have positive effects or provide real measures to protect fundamental rights remains to be seen.

References

Appelman, N., Ó Fathaigh, R. and van Hoboken, J. (2021) 'Social welfare, risk profiling and fundamental rights: the case of SyRI in the Netherlands'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=3984935 (Accessed: 18 June 2024).

Barzashka, I. (2023) 'Seeking strategic advantage: the potential of combining artificial intelligence and human-centred wargaming', *The RUSI Journal*, 168(7), pp. 26–32.

Bovens, M. (2010) 'Two concepts of accountability: accountability as a virtue and as a mechanism', *West European Politics*, 33(5), pp. 946–967.

Chander, A. (2017) 'The racist algorithm?', *Michigan Law Review*, 115(6), pp. 1023–1045.

Clifford, D. (2017) 'Citizen-consumers in a personalised galaxy: emotion influenced decision-making, a true path to the dark side?' *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.3037425 (Accessed: 3 February 2025).

Constantino, J. (2022) 'Exploring Article 14 of the EU AI Proposal: human in the loop challenges when overseeing high-risk ai systems in public service organisations', *Amsterdam Law Forum*, 14(3), pp. 1-17.

Constantino, J. (2024) 'Article 15 accuracy, robustness and cybersecurity (Forthcoming)', in. *Wolters Kluwer*.

Constantino, J. and van der Linden, T. (2024) 'AI Applications not covered by the AI Act (Forthcoming)', in *Springer*.

Constantino, J. and Wagner, B. (2024) 'Accountability and oversight in the Dutch intelligence and security domains in the digital age', *Frontiers in Political Science*, 6 [Online]. Available at: https://doi.org/10.3389/fpos.2024.1383026 (Accessed: 4 February 2025).

Cooper, A.F., Moss, E., Laufer, B. and Nissenbaum, H. (2022) 'Accountability in an algorithmic society: relationality, responsibility, and robustness in machine learning', in *2022 ACM Conference on Fairness, Accountability, and Transparency*, pp. 864–876.

Demircan, M. (2023) *Deployers of High-Risk AI Systems: What Will Be Your Obligations Under the EU AI Act?* [Online]. Available at: https://competitionlawblog.kluwercompetitionlaw.com/2023/06/02/deployers-of-high-risk-ai-systems-what-will-be-your-obligations-under-the-eu-ai-act/ (Accessed: 3 February 2025).

DK (2023) *Simply artificial intelligence*. DK Publications. Available at: https://www.dk.com/us/book/9780744076820-simply-artificial-intelligence/ (Accessed: 4 February 2025).

Docksey, C. and Propp, K. (2023) 'Government access to personal data and transnational interoperability: an accountability perspective', *Oslo Law Review*, 10(1), pp. 1–34.

Dougherty, C. (2015) *Google Photos mistakenly labels black people 'gorillas'*. Bits Blog [Online]. Available at: https://archive.nytimes.com/bits.blogs.nytimes.com/2015/07/01/google-photos-mistakenly-labels-black-people-gorillas/ (Accessed: 30 September 2024).

Drukarch, H., Calleja, C. and Fosch Villaronga, E. (2023) 'An iterative regulatory process for robot governance', *Data & Policy*, 5 (e8) [Online]. Available at: https://doi.org/10.1017/dap.2023.3 (Accessed: 4 February 2025).

Edwards, L., Schafer, B. and Harbinja, E. (2020) *Future law: emerging technology, regulation and ethics* [Online]. Available at: https://edinburghuniversitypress.com/book-future-law.html (Accessed: 18 June 2024).

Eligon, J. and Williams, T. (2015) 'Police program aims to pinpoint those most likely to commit crimes', *The New York Times*, 25 September [Online]. Available at: https://www.nytimes.com/2015/09/25/us/police-program-aims-to-pinpoint-those-most-likely-to-commit-crimes.html (Accessed: 18 June 2024).

European Commission (2019) *Ethics guidelines for trustworthy AI: High-Level Expert Group on artificial intelligence* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/ethics-guidelines-trustworthy-ai (Accessed: 11 June 2024).

European Data Protection Board (EDPB) (2020) *Guidelines 3/2019 on processing of personal data through video devices*. European Data Protection Board [Online]. Available at: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32019-processing-personal-data-through-video_en (Accessed: 18 June 2024).

Green, B. (2022) 'The flaws of policies requiring human oversight of government algorithms', *Computer Law & Security Review*, 45, 105681 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105681 (Accessed: 4 February 2025).

Hacker, P. (2018) 'Teaching fairness to artificial intelligence: existing and novel strategies against algorithmic discrimination under EU law', *Common Market Law Review*, 55(4) [Online]. Available at: https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\COLA\COLA2018095.pdf (Accessed: 11 June 2024).

Hage, J. (2017) 'Theoretical foundations for the responsibility of autonomous agents', *Artificial Intelligence and Law*, 25(3), pp. 255–271.

Hanif, H. et al. (2023) 'Tough decisions? Supporting system classification according to the AI' in Sileno, G., Spanakis, J. and Van Dijck, G. (eds.) *Frontiers in Artificial Intellignece and Applications. Volume 379: Legal Knowledge and Information Systems -.* , pp. 353–358 [Online]. Available at: https://doi.org/10.3233/FAIA230987 (Accessed: 4 February 2025).

Henao, F. (2021) *Why data handling may put a bump on the road to autonomous driving*. Automotive News Europe [Online]. Available at: https://europe.autonews.com/guest-columnist/why-data-handling-may-put-bump-road-autonomous-driving (Accessed: 18 June 2024).

Hill, R.K. (2016) 'What an algorithm is', *Philosophy & Technology*, 29(1), pp. 35–59.

Holzinger, A. (2016) 'Interactive machine learning for health informatics: when do we need the human-in-the-loop?', *Brain Informatics*, 3(2), pp. 119–131.

Human Rights Law Centre (2021) *The Federal Court approves a $112 million settlement for the failures of the Robodebt system*. Human Rights Law Centre [Online]. Available at: https://www.hrlc.org.au/human-rights-case-summaries/2021/9/30/the-federal-court-approves-a-112-million-settlement-for-the-failures-of-the-robodebt-system (Accessed: 18 June 2024).

Johansson-Pajala, R.-M. and Gustafsson, C. (2020) 'Significant challenges when introducing care robots in Swedish elder care' *Disability and Rehabilitation: Assistive Technology*, 17(2), pp. 166–176.

Kang, H.S., Makimoto, K., Konno, R. and Koh, I. S. (2020) 'Review of outcome measures in PARO robot intervention studies for dementia care', *Geriatric Nursing*, 41(3), pp. 207–214.

Kelly, P.A. et al. (2021) 'The effect of PARO robotic seals for hospitalized patients with dementia: a feasibility study', *Geriatric Nursing*, 42(1), pp. 37–45.

Köchling, A. and Wehner, M.C. (2020) 'Discriminated by an algorithm: a systematic review of discrimination and fairness by algorithmic decision-making in the context of HR recruitment and HR development', *Business Research*, 13(3), pp. 795–848.

Koivisto, I., Koulu, R. and Larsson, S. (2024) 'User accounts: how technological concepts permeate public law through the EU's AI Act', *Maastricht Journal of European and Comparative Law*, 31(3), [Online]. Available at: https://doi.org/10.1177/1023263X241248469 (Accessed: 4 February 2025).

Van Kolfschooten, H. and Shachar, C. (2023) 'The Council of Europe's AI Convention (2023–2024): promises and pitfalls for health protection', *Health Policy*, 138, 104935 [Online]. Available at: https://doi.org/10.1016/j.healthpol.2023.104935 (Accessed: 4 February 2025).

Kowalski, R. (1979) 'Algorithm = logic + control', *Communications of the ACM*, 22(7), pp. 424–436.

Kowert, W. (2017) 'The foreseeability of human–artificial intelligence interactions', *Texas Law Review*, 96, pp. 181-204.

Kuziemski, M. and Misuraca, G. (2020) 'AI governance in the public sector: three tales from the frontiers of automated decision-making in democratic settings', *Telecommunications Policy*, 44(6) [Online]. Available at: https://doi.org/10.1016/j.telpol.2020.101976 (Accessed: 4 February 2025).

Le Sueur, A. (2015) 'Robot government: automated decision-making and its implications for parliament'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=2668201 (Accessed: 18 June 2024).

Leiman, T. (2021) 'Law and tech collide: foreseeability, reasonableness and advanced driver assistance systems', *Policy and Society*, 40(2), pp. 250–271.

Lennox, J. (2020) *2084: artificial intelligence and the future of humanity*. Chicago: Zondervan Reflective [Online]. Available at: https://www.johnlennox.org/shop/24/2084-artificial-intelligence-and-the (Accessed: 6 June 2023).

MacKay, D.J.C. (2003) *Information theory, inference, and learning algorithms*. Cambridge: Cambridge University Press.

Maclure, J. (2020) 'The new AI spring: a deflationary view', *AI & Society*, 35(3), pp. 747–750.

Mahler, T. (2021) 'Between risk management and proportionality: the risk-based approach in the EU's Artificial Intelligence Act Proposal'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=4001444 (Accessed: 18 June 2024).

Muthukrishnan, N. et al. (2020) 'Brief history of artificial intelligence', *Neuroimaging Clinics of North America*, 30(4), pp. 393–399.

Neumann, O., Guirguis, K. and Steiner, R. (2022) 'Exploring artificial intelligence adoption in public organizations: a comparative case study', *Public Management Review*, 26(1), pp. 114–141.

Newberry, S. (2015) 'Public sector accounting: shifting concepts of accountability', *Public Money & Management*, 35(5), pp. 371–376.

Ng, Y.-F., O'Sullivan, M., Paterson, M. and Witzleb, N. (2020) 'Revitalising public law in a technological era: rights, transparency and administrative justice'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=3689497 (Accessed: 18 June 2024).

'NJCM et al v. The Dutch State', ECLI:NL:RBDHA:2020:1878, Rechtbank Den Haag, C-09-550982-HA ZA 18-388 (2020) [Online]. Available at: https://deeplink.rechtspraak.nl/uitspraak?id=ECLI:NL:RBDHA:2020:1878 (Accessed: 18 June 2024).

Novelli, C., Taddeo, M. and Floridi, L. (2022) 'Accountability in artificial intelligence: what it is and how it works'. *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.4180366.

OECD (2024) *Recommendation of the Council on artificial intelligence, OECD/LEGAL/0449* [Online]. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449 (Accessed: 18 June 2024).

Panezi, A. (2021) 'Liability rules for AI-facilitated wrongs: an ecosystem approach to manage risk and uncertainty'. *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.3768779 (Accessed: 4 February 2025).

Pasquale, F. (2015) *The black box society: the secret algorithms that control money and information*. Cambridge, MA: Harvard University Press.

Ray, P. (2016) 'Internet of robotic things: concept, technologies, and challenges', *IEEE Journals & Magazine* [Online]. Available at: https://ieeexplore.ieee.org/abstract/document/7805273 (Accessed: 30 September 2024).

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L, 2024/1689, 12 July [Online]. Available at: http://data.europa.eu/eli/reg/2024/1689/oj (Accessed: 5 February 2025).

Richardson, R., Schultz, J. and Crawford, K. (2019) 'Dirty data, bad predictions: how civil rights violations impact police data, predictive policing systems, and justice', *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=3333423 (Accessed: 18 June 2024).

Rosenblat, A., Kneese, T. and Boyd, D. (2014) 'Workplace surveillance'. *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.2536605 (Accessed: 4 February 2025).

Simmons, A.B. and Chappell, S.G. (1988) 'Artificial intelligence-definition and practice', *IEEE Journal of Oceanic Engineering*, 13(2), pp. 14–42.

Sipola, T., Alatalo, J., Wolfmayr, M. and Kokkonen, T. (eds.) (2024) *Artificial intelligence for security: Enhancing protection in a changing world*. Cham: Springer Nature Switzerland.

Stephenson, J. and Acklam, C. (2019) 'Artificial intelligence in care: where does responsibility lie?', *Nursing and Residential Care*, 21(5), pp. 281–283.

Sykes, C.J. (2000) *Big brother in the workplace*Hoover Institution [Online]. Available at: https://www.hoover.org/research/big-brother-workplace (Accessed: 18 June 2024).

Van der Linden, T. (2021) 'Regulating artificial intelligence: please apply existing regulation', *Amsterdam Law Forum*', 13(3), pp. 3-9. Available at: https://doi.org/10.37974/ALF.432 .

Van de Poel, I.R. et al. (2012) 'The problem of many hands: climate change as an example', *Science and Engineering Ethics*, 18(1), pp. 49–67.

Verdiesen, I., Santoni de Sio, F. and Dignum, V. (2021) 'Accountability and control over autonomous weapon systems: a framework for comprehensive human oversight', *Minds and Machines*, 31(1), pp. 137–163.

Wachter, S. (2024) 'Limitations and loopholes in the EU AI Act and AI Liability Directives: what this means for the European Union, the United States, and beyond', *Yale Journal of Law and Technology*, 26(3), pp. 671–718.

Wagner, B., de Gooyert, V. and Veeneman, W. (2023) 'Sustainable development goals as accountability mechanism? A case study of Dutch infrastructure agencies', *Journal of Responsible Technology*, 14, 100058 [Online]. Available at: https://doi.org/10.1016/j.jrt.2023.100058 (Accessed: 5 February 2025).

Whiteford, P. (2021) 'Debt by design: the anatomy of a social policy fiasco – or was it something worse?', *Australian Journal of Public Administration*, 80(2), pp. 340–360.

Winick, E. (2018) *Amazon ditched AI recruitment software because it was biased against women*. MIT Technology Review [Online]. Available at: https://www.technologyreview.com/2018/10/10/139858/amazon-ditched-ai-recruitment-software-because-it-was-biased-against-women/ (Accessed: 18 June 2024).

Wisman, T. (2020) *The SyRI victory: holding profiling practices to account*. Digital Freedom Fund [Online]. Available at: https://digitalfreedomfund.org/the-syri-victory-holding-government-profiling-to-account/ (Accessed: 18 June 2024).

The Digital Services Act: Online Risks, Transparency and Data Access

Marie-Therese Sekwenz & Rita Gsenger

Abstract

The Digital Services Act (DSA) represents a landmark legislative framework in the European Union, aimed at regulating online platforms, enhancing transparency, and mitigating systemic risks associated with digital services. The Act aligns with broader EU regulatory efforts, including the General Data Protection Regulation (GDPR) and the Artificial Intelligence (AI) Act, positioning it as a cornerstone of digital governance.

A key objective is to create a harmonized internal market that prevents regulatory fragmentation while ensuring consumer protection and fundamental rights. The DSA introduces obligations for intermediary services, including very large online platforms (VLOPs) and very large online search engines (VLOSEs). Moreover, the regulation mandates due diligence measures such as transparency reporting, algorithmic accountability, and user rights protections. Transparency mechanisms include the publication of terms and conditions databases, the Statement of Reasons repository, and advertising libraries. Moreover, the DSA enforces structured risk assessment and mitigation strategies, particularly for systemic risks such as illegal content dissemination, disinformation, and fundamental rights violations.

A core component of the DSA is its approach to content moderation, introducing user empowerment mechanisms such as Trusted Flaggers, internal complaint-handling systems, and out-of-court dispute resolution bodies. Additionally, the Regulation includes crisis response provisions enabling swift intervention by the European Commission in extraordinary circumstances. To ensure compliance, the DSA establishes independent audit requirements and risk-based oversight mechanisms, reinforcing platform accountability. This Chapter aims to give an overview and comprehensive introduction to these provisions.

1. Introducing the DSA: Context and scope

The most important European legislative act currently regulating (large) online platforms and their content moderation systems is the Digital Services Act (DSA). The DSA is the legal update of the E-Commerce Directive (2000/31/EC) of 2000 and expands the original scope by going beyond the regulation only of individual rights (Kaesling, 2023, p. 552). The wording of the Directive did not take into account the importance that social networks and online marketplaces would play in daily life as the digital economy has developed into a platform economy (Rodríguez de las Heras Ballel, 2021, p. 80); furthermore, the scale of the services and the multiplication of various intermediaries needed to be considered. Differing legislative efforts of Member States led to the fragmentation of legal regulations and challenges regarding the enforcement of services that operate across borders (Schwemer, 2023, p. 233). Moreover, the important role of algorithmic decision-making (Castellucia and Le Métayer, 2019; Dogru. Facciorusso and Stark, 2020), disinformation (Bayer et al, 2021; Iosifidis and Nicoli, 2021), and illegal content (De Streel et al, 2020; Kübler et al, 2021) has become more evident.

The general aim of the DSA is a "safe, predictable and trusted online environment" (Art. 1 (1) DSA) through the realisation of an internal European market. Since platforms operate transnationally and Member States may have their own rules, there is a risk that the market might fragment, as occurred with the regulatory attempts of Germany (Network Enforcement Act, 2017) and Austria (Communication Platforms Act, 2020). An internal market would enable companies to benefit from unification and allow them to innovate in a harmonised environment. Moreover, new markets can be accessed and consumers overall would have more choices (Hofmann and Raue, 2023, p. 33).

In December 2020, the DSA was presented in conjunction with the Digital Markets Act (DMA) (Directive (EU) 2019/790), which aims to ensure a fair platform economy with a functioning internal market (Morais Carvalho et al, 2021, p. 74). In the first Chapter, the DSA determines its subject matter (Art. 1) and scope (Art. 2) and provides definitions (Art. 3). Chapter II focuses on the liability of providers and intermediary services, and Chapter III on due diligence and transparency. Chapter III consists of sections listing the specifications concerning the obligations of different intermediary services, such as online platforms or very large online platforms (VLOPs) and search engines (VLOSEs) (as defined by Art. 33(1) DSA).

Chapter IV specifies implementation, cooperation, penalties and enforcement and includes specificities about Digital Service Coordinators (DSCs) and other relevant authorities and competencies, such as the European Board for Digital Services. The Board acts as an independent advisory body for the DSCs (Arts. 61–64 DSA); DSCs are the regulatory body situated in each Member State. Member States choose these "competent authorities" (Art. 49, (2)), and the DSCs are subsequently "responsible for all matters relating to supervision and enforcement" of the DSA in the respective Member State (Art. 49 (2)).

The DSA defines its scope in Art. 2 (1), including intermediary services (Art. 3 (g) DSA), hosting services (Art. 3 (g) (iii) DSA), online platforms (Art. 3 (i) DSA), VLOPs (Art. 33(1) DSA) and VLOSEs (Art. 3 (j) DSA) that offer their services inside the European Union.

Intermediary services refers to three types of "information society services" (lit. g): first, services that are "mere conduit" (i), transmitting information by a recipient of the service. Second, "a 'caching' service" (ii) that includes the transmission and storage of information and third, "a 'hosting' service, consisting of the storage of information provided by, and the request of, a recipient of the service" (iii). An online platform is a hosting service that, "at the request of a recipient of the service, stores and disseminates information to the public" (Art. 3 lit. i). Online search engines are also intermediary services that "allow[s] users to input queries in order to perform searches of, in principle, all websites, or all websites in a particular language, on the basis of a query on any subject in the form of a keyword, voice request, phrase or other input, and returns results in any format in which information related to the requested content can be found" (lit. j).

VLOPs and VLOSEs are defined as services and intermediaries operating in the European Union that are reported to have more than 45 million monthly active users (Art. 33 (1)). The number of users should cover at least 10% of the EU population. The number is reported by the platforms themselves, and they must provide an updated number of monthly active users "at least once every six months" (Art. 24 (2)) or "without undue delay" (Art. 24 (3)) upon receiving a request from the European Commission. The European Commission first designated platforms and search engines considered to be very large in April 2023; now, that list is frequently updated and includes platforms such as AliExpress, Google Search, Facebook, TikTok, Meta and Amazon (European Commission, 2024a). This limit cannot be bypassed by European nation-states and no platforms with fewer

monthly active users can be obliged to adhere to the risk identification and mitigation requirements (Kaesling, 2023, p. 533). The European Commission assumes that intermediaries of this size have significant influence on the internal market and that they have sufficient resources to adhere to the Regulation (Kaesling, 2023, p. 541).

The DSA includes natural or legal persons who have the possibility of using a service (Art. 3 lit. b); such a person is referred to as a "recipient" (Art. 3 lit. b). However, the DSA also refers to persons as "users" throughout the text, and this term is preferred in this chapter as it is more commonly used. The DSA presents a legal definition that describes active users or recipients. This definition, however, is in the main text of the DSA, not in the Recitals, emphasizing the importance of the differentiation. An active user of an online platform can be classified in two ways: they can "request [...] the online platform [...] host information" (Art. 3 lit. p), meaning, for instance, uploading user-generated content to platforms or commenting on other content (Kaesling, 2023, p. 542); or, an active recipient is a person "exposed to information hosted by the online platform and disseminated through its online interface" (Art. 3 lit. p). Therefore, receiving or consuming content on platforms without contributing or uploading content is sufficient to be considered an active user. Participation is confirmed independent of registration and includes the consumption of any content (whether visual or audio) that starts without any user involvement as soon as a website opens (Kaesling, 2023, p. 542). An active recipient of a search engine "has submitted a query to an online search engine and been exposed to information indexed and presented on its online interface" (Art. 3 lit. q DSA). A query includes the input of terms, and if the query is completed automatically and the recipient presses enter, the input counts as active use (Kaesling, 2023, p. 542).

Intermediaries profit from the *Good Samaritan Clause* that limits liability and determines that they are not responsible for any content shared that might be illegal (G'sell, 2023, p. 4). Therefore, they are exempt from liability under certain conditions (Hofmann and Raue, 2023, p. 32f) and, moreover, are not required to participate in any monitoring activities (Art. 8 DSA).

Complementing the DMA[1], the DSA aims to enable citizens to exercise their fundamental rights in a safe online environment (Morais Carvalho et al, 2021, p. 75). The DSA aims to reduce risks of VLOPs and VLOSEs

1 For more information on the DMA, see Chapter 6, 'The Brave Little Tailor v. Digital Giants: A Fairy-Tale Analysis of the Social Character of the DMA' by Liza Herrmann.

by establishing clear rules and transparency. In addition to a trustworthy online environment, the DSA seeks to ensure that fundamental rights are protected and consumer protections strengthened. Lastly, the DSA aims to establish legal certainty (Hofmann and Raue, 2023, p. 33).

Similar to other European Regulations such as the General Data Protection Regulation[2], the AI Act[3] or the NIS 2 Directive[4], the DSA includes risk-based elements in its regulatory structure (Efroni, 2021). Risk detection, analysis and evaluation are thus included in the legislative package, with internal measures, external audits, transparency requirements and access reviewed by the legislature (the European Commission and DSCs) and researchers. The DSA practises "enforced self-regulation" (Kaesling, 2023, p. 532) in parts, such as systemic risk assessments (Art. 34), as the platforms are required to detect, analyse and evaluate systemic risks. That means, they – the platforms – are initially responsible; however, the compliance of platforms is tested and regularly reviewed, and in a last step, regulators intervene and enforce. The European Commission supervises the compliance of VLOPs and VLOSEs and can impose monetary sanctions (ibid.) that are not to exceed 6% of the service providers' annual turnover (Art. 52 (3). Lastly, due to Art. 88 DSA, the Commission has the ability to create Delegated Acts that detail the implementation of the DSA, for instance, on Audits (European Commission, 2023a) or the transparency reporting obligations of intermediary services (European Commission, 2023b).

In this Chapter, we will discuss the most important provisions and their consequences, including the due diligence of VLOPS and VLOSEs, including transparency mechanisms (section 2), user rights and processes (section 3), risk assessment, risk mitigation, and audits (section 4).

2. See-through regulation? Novel transparency mechanisms in the DSA

The DSA creates several new mechanisms that provide novel insights into the day-to-day decisions taken on platforms. Transparency mechanisms

2 For more information on the GDPR, see Chapter 14 'EU Data Protection Law in Action: Introducing the GDPR' by Julia Krämer.

3 For more information on the AI Act, see Chapter 2 'Searching for Harmonised Rules: Understanding the Paradigms, Provisions, and Pressing Issues in the Final EU AI Act' by Hannah Ruschemeier and Jascha Bareis, and Chapter 3 'Accountable AI: It Takes Two to Tango' by Jorge Constantino.

4 For more information on the NIS 2 Directive, see Chapter 17 'Unpacking the NIS 2 Directive: Enhancing EU Cybersecurity for the Digital Age' by Eyup Kun.

centrally include reports and databases to inform stakeholders. This text will therefore highlight the main tools of transparency by focusing on transparency reports (Art. 15, 24 and 42 DSA), the Terms and Conditions database (Art. 14 DSA), the Statement of Reasons (Art. 17 DSA) and the Ad Library, also referred to as the Ad Repository (Art. 39 DSA). Additional means of transparency can be found in the rules regarding recommendation systems (Art. 27 DSA), parameters on targeted advertising (Art. 26 DSA) and in the link between the Code of Practice of Disinformation and the DSA as a Code of Conduct (Art. 45–47 DSA) (Just and Saurwein, 2024).

Flyverbom (2016, p. 110–112) defined transparency as a complex process connected to the development, interpretation and aggregation of publishing information aimed at enhancing accountability, openness and trust within a certain period. The DSA itself does not form its own definition of transparency (Kosters and Gstrein, 2023, p. 117) but rather reflects on it in several passages, including in Recital 49: "To ensure an adequate level of transparency and accountability, providers of intermediary services should make publicly available an annual report in a machine-readable format, in accordance with the harmonised requirements contained in this Regulation". Such a machine-readable form of transparency could also enhance the automatisation of checks and balances in an empirically-based accountability regime (Murray and Flyverbom, 2020). Conversely, Kosters and Gstrein (2023) highlight the importance of the audience within the transparency regime and differentiate transparency into three layers: "The first layer of transparency involves the disclosure of information. The second layer consists of ensuring that the information disclosed is also understandable to the broader public. Lastly, a third layer of transparency includes tailoring the explanation of information to the different types of users of the platform" (Kosters and Gstrein, 2023, p. 130). According to their case study of one VLOP, the DSA contributes to the first two layers through, for example, the provision of information in transparency reports, and to the second layer through the offer of a dashboard for the Statement of Reasons (Digital Services Act, 2024); however, they found that the DSA was still lacking in the third layer of transparency. Ideally, by being able to interlock several different control mechanisms, the forms of transparency that the DSA creates can form a more solid understanding of meaningful, accountable and consistent transparency regimes (Sekwenz and Wagner, 2025, forthcoming).

2.1 A harmonised form of reporting through DSA transparency reports?

The DSA's new rules on transparency reporting can be seen as a predecessor to the provisions that frame reporting under the German NetzDG or the Austrian KoPlG (Heldt, 2019; Werthner et al, 2024, p. 627). According to the DSA, platforms have different reporting obligations to be disclosed in an annual report – or for VLOPs and VLOSEs, in biennial reporting intervals – and such reports must be machine-readable (Art. 15(1) DSA). According to Art. 9 and 10 DSA, transparency reports must include information about orders from public authorities (for example, the police in a Member State), numbers about illegal content or median-time spans of action in response to such notices (Art. 15(1) (a) DSA).

Details provided in transparency reports include data concerning flags received from user-reporting (Art. 16 DSA) describing details of violation reasons, reports from Trusted Flaggers (who report to platforms about illegal content with increased flagging priority, see Art. 22 DSA), the moderation action set (for example, deletion or deplatforming), the automated means included in the moderation process (for instance, the use of Artificial Intelligence (AI) for detecting illegal content) and aspects of reaction time (Art. 15 (1) (b) DSA). Furthermore, details must be included on the specific purpose of the automated means used in the process, their accuracy and the possible error rate of tools like AI (Art. 15(1) (c) DSA). Article 15(1) (d) DSA specifies reporting details on the internal complaint-handling system according to Art. 20 DSA. This mechanism should enable users to question content moderation actions on platforms. The provisions of Art. 24 DSA (see Recital 65 DSA) only apply to online platforms, VLOPs and VLOSEs; these include paragraphs on the out-of-court dispute settlements (Art. 21 DSA), including the number of disputes received, the median time needed to form a decision or the decisions taken in such cases (Art. 24 (1) (a) DSA). In addition, information about malicious user behaviour, such as deplatforming (Kettemann et al, 2022), must be provided according to Art. 23 DSA, for example, details about the reason for suspension (Art. 24 (1) (b) DSA).

Recital 100 opens the scope for Art. 42 DSA, under which "additional transparency requirements should apply specifically to [VLOPs and VLOSEs]" such as biannual reporting obligations. Such platforms must report on the human resources used in the process of content moderation, including details about language skills, educational measures, training or support (Art. 42 (2) (a–b) DSA). Furthermore, Art. 42 DSA requires the inclusion

of qualitative information – broken down to Member State levels (Art. 42 (2) (c) DSA – about the means of content moderation, such as details about the training of content moderators or the educational measures provided to them.

2.2 A place for all platform contracts – The terms and conditions database

According to the DSA, contractual rules governing online behaviour – found in the Community Standards of a platform – are to be provided within the terms and conditions, which are defined in Art. 3 (u) DSA as "all clauses, irrespective of their name or form, which govern the contractual relationship between the provider of intermediary services [the platform] and the recipients of the service [the user]". These and other contractual rules for VLOPs and VLOSEs should be provided in the official languages of all Member State platforms that provide their services and include opt-out details addressed in the generalised contract according to Recital 48 DSA and Art. 14 (6) DSA.

Terms and conditions not only include norms and procedures but also the "measures, and tools" used in content moderation (Art. 14,19 DSA). Since terms and conditions describe how to behave on platforms, these contractual amendments, also referred to as community standards or *netiquette* are a flexible way to adapt frameworks to new challenges, such as the COVID-19 pandemic or wars and conflicts (European Commission, 2022; Kettemann and Sekwenz, 2022). Article 14 DSA requires that users be informed about significant changes (2) and that information is to be provided in a machine-readable format (5). Furthermore, information for children is explicitly mentioned (3), and enforcement has to be in line with fundamental rights (4). Since February 2024, platforms have uploaded their terms and conditions and changes to a website that informs users about the current version that platforms use for content moderation (Terms and Conditions Database, 2024). For the first time, this organised database of contractual rules provides the reader with updates on new clauses, actions or exemptions.

2.3 Quick insights in content moderation decisions through the statement of reason database

The Statement of Reason database is a new measure of transparency in the DSA regulated under Art. 17 DSA. According to Recital 66, "to ensure transparency and to enable scrutiny over the content moderation decisions of the providers of online platforms and monitoring the spread of illegal content online, the Commission should maintain and publish a database which contains the decisions and statements of reasons of the providers of online platforms when they remove or otherwise restrict availability of and access to information". This database therefore captures content moderation decisions in cases of a violation of the terms and conditions (Art. 14 DSA) or the law of a Member State (Art. 3 (h) DSA), similar to the Lumen Database, which was created at Harvard University to capture insight into the moderation process (Lumen Database, 2024). These captured content moderation actions either affect the visibility of content (Art. 17(1) (a) DSA), monetary elements (Art. 17(1) (b) DSA), suspension of the service (Art. 17(1) (c) DSA) or the suspension of an account (Art. 17(1) (d) DSA). Information in the so-called transparency database also includes content moderation decisions such as the facts upon which a decision is based, the circumstances of a case, the source of information (e.g. flagging) or the identity of the notifier (e.g. a Trusted Flagger). Additionally, information about the automated means in the process should be provided as a reference to legal or contractual grounds, as well as information about user rights (e.g. the internal complaint-handling system according to Art. 20 DSA or out-of-court dispute settlements according to Art. 21 DSA). Since the general aim of increasing transparency is welcomed by the community, the accuracy, depth of information and completeness have been critiqued by researchers evaluating the meaningfulness of platforms' reporting practices (Drolsbach and Pröllochs, 2023; Kaushal et al, 2024; Trujillo, Fagni and Cresci, 2024). Such a database is a novum to the world of online governance and opens a path for increased research on platforms to be conducted. The database includes an individual ID for each decision that can be linked to thorough investigations in conjunction with researcher data access or independent audits, and it can also link to the transparency reports of a platform to control for cross-transparency mechanisms (Sekwenz and Wagner, 2025, forthcoming).

2.4 Ad library

Another key database the DSA creates is the advertising repository, the use of which, according to Art. 39 DSA, is mandatory for VLOPs and VLOSEs (Duivenvoorde and Goanta, 2023; Izyumenko et al, 2024). This database provides users with a publicly available search function and API. According to Art. 39(2) (a) DSA, the database should include information about the advertisement (name of the product/service/brand and the subject of the ad, e.g. political advertising). Furthermore, the person on whose behalf the ad is presented has to be disclosed (b–c), in addition to information about the duration of the ad presentation and display (d), targeted and unincluded groups (e–f) and the number of users for whom the ad has been displayed (g). Such information, however, should not be included in the database if the content was classified as illegal under the law of a Member State (Art. 39(3) DSA). Additionally, for the DSA, the upcoming Directive on Transparency and Targeting of Political Advertising will create a new centralised database for this specific type of online advertising at the European level (see Art. 13, Regulation 2024/900).

2.5 Data access for researchers

Article 40 DSA holds specific interest for researchers investigating platforms due to its provision of data access to the DSC or the Commission (Art. 40 (1)). The first part of the Article (1–3) regulates access by public authorities, whereas the second part (4–6 and 8–11) focuses on researcher access. The following section will focus on the second part of Art. 40 due to its relevance for researchers. Research access is provided for the purpose of investigating systematic online risks in order to reduce information asymmetries and support risk mitigation (Kaesling, 2023, p. 639). Therefore, access should be constrained to data concerning the provisions of the DSA, especially understanding and identifying systemic risks according to Art. 35 (Art. 40 (4)).

The DSC can request that VLOPs and VLOSEs "explain the design, the logic, the functioning and the testing of their algorithmic systems" (Art. 40 (3)). Platform providers need to adhere to these requests "within a reasonable period" (Art. 40 (4)); however, platforms can request an amendment to the data access request within 15 days if they do not have access to that data or if the security of their service and trade secrets are endangered

(Art. 40 (5) lit. a–b). The DSC will grant researchers requesting data access the "status of 'vetted researchers' for the specific research" (Art. 40 (8)). These researchers need to fulfil certain requirements as specified in Art. 40 (8) (lit. a-g): researchers must be part of a research organisation (lit. a), which is defined as "a university, including its libraries, a research institute or any other entity, the primary goal of which is to conduct scientific research or to carry out educational activities involving also the conduct of scientific research" (Copyright Directive Art. 2 (1)). The organisation must be non-profit (lit. a) and operate in the public interest (lit. b). Additionally, researchers must work independently and not for commercial interests (lit. b), disclose their research funding (lit. c), protect personal data and implement measures to guarantee data security (lit. d). Furthermore, they must prove that data access is necessary for their research, that it is proportionate and will contribute to the understanding of risk mechanisms (lit. e, f). Finally, researchers must make their results publicly available (lit. g).

Research needs to "contribute to the detection, identification and understanding of systematic risks" (Art. 40(12)). According to Husovec (2023), Art. 40(12) provides two functions: it protects providers against unjust access and minimises technical restrictions of data access for researchers. He argues that scraping should remain central for research aside from API access.

3. On user rights, processes and institutionalised flagging entities

Transparency mechanisms in the DSA combine a variety of different facets of transparency, including transparency reports, the three databases or repositories (terms and conditions, statement of reason and advertising) and the provision of a reporting mechanism for users, as described earlier. On the other hand, the DSA also provides new roles and rights for accredited entities like trusted flaggers, out-of-court dispute settlement bodies and the new legal position of the recipient of a service (see Art. 3 (b) DSA) through the internal complaint-handling system, creating the novel possibility of user empowerment. These mechanisms unfold after the initial content moderation process has ended and open new legal pathways for user empowerment, a more structured response to moderation dissent and the inclusion of experts and civil society on a regular and institutionalised basis (Douek, 2022, pp. 37–51).

3.1 Drop-down of user empowerment? Notice and action mechanisms

Users have been included in the process of content moderation for years and can be described as a central component in the curation of content on platforms such as Reddit or Mastodon (Jhaver et al, 2019; Roth and Lai, 2024). The tool that facilitates user engagement in content moderation is referred to as flagging (Kou and Gui, 2021). The DSA specifies rules on how platforms should design flagging mechanisms in Art. 16 DSA (Sekwenz et al, 2025). A notice action mechanism must empower users to notify the platform about illegal content or contractual violations in a user-friendly design that is easy to access (Art. 16(1) DSA). The design has to indicate the reason why the content has been deemed illegal, a link to the content in question (e.g. URL), the name and email address of the flagging individual and the claim to act in *bona fide* (Art. 16(2) (a-d) DSA). When a user has flagged a piece of content, the intermediary must notify the user (reporting user) about the received notice (Art. 16(4) DSA) as well as the user whose content was reported (Art. 16(5) DSA). Furthermore, Article 16(6) DSA specifies the procedure for platforms to "process any notices that they receive […] and take their decisions in respect of the information to which the notices relate, in a timely, diligent, non-arbitrary and objective manner". Together with the transparency reports of other higher-level means of DSA transparency, the reporting or flagging mechanisms provide a crucial function since they serve as the data collection processes that feed the transparency reports and the statement of reason database. As research on the NetzDG has shown, reporting mechanisms can be used to nudge the user towards reporting loops that favour terms and conditions. As a result, there is more detailed reporting on contractual violations than with the use of the more cumbersome (for the user) illegal content reporting, e.g. through implementing the need to click substantively more often to flag illegal content, leading to low numbers of illegal content flags in transparency reports (Wagner et al, 2020). In 2019, this dark pattern (Brignull, 2019; Gray et al, 2024) of user flagging received a 2 million euros under the German national law in a case brought by national authorities against Facebook (Escritt, 2019).

3.2 Trust me, I am a trusted flagger

Another factor concerning notice action mechanisms in the DSA is the 'fast-lane option' for Trusted Flaggers of illegal content, as specified in

Art. 22 DSA (see Recital 61 DSA; Appelman and Leerssen, 2022). These flaggers have the needed expertise to file flags through the complaint mechanism and, importantly, relevant legal experience that a standard user might not be expected to have.

Trusted Flaggers operate in their "designated area of expertise" when awarded their status after filing an application to the DSC of their Member State (Art. 22(2) DSA; Schwemer, 2019); their status can also be revoked according to Art. 22 (7) DSA). An applicant to the DSC has to fulfil the following conditions: have the expertise and competence to "detect, identify and notify" platforms about illegal content on their service (a), show independence from the platforms (b) and flag "diligently, accurately, and objectively" (c). Flaggers must publish annual reports providing information on their flagging in the relevant time period (Art. 22 (3), Recital 62 DSA); these reports have to be sent to the DSC and made publicly available in a database (Art. 22(5) DSA). The reports should be structured in a way that provides details on the platform the flagging has been applied to (a), the type of illegal content (b) and the platform's moderation action (c). Information and explanation about how the Trusted Flaggers maintain their independence must also be included. Independence mechanisms might include the platforms automatically providing flagging tools for Trusted Flaggers that help to 'book-keep' reported flags from flagging entities. The identity of the Trusted Flaggers is disclosed as well. If a platform observes misbehaviour from Trusted Flaggers, either in submitting "insufficiently precise, inaccurate or inadequately substantiated notices" (Art. 16 DSA) or complaints in the mechanisms provided through the internal complaint-handling system (Art. 20 DSA), the DSC should be informed and after considering evidence and information may suspend the Trusted Flagger (Art. 22(6) DSA). If the investigation into a Trusted Flagger appears to be substantiated (either through the information from a platform or their own initiative), their status can be revoked (Art. 22(7) DSA). In addition, information about notices received by Trusted Flaggers has to be indicated in transparency reports (Art. 15(1) (b) DSA) and can be indicated in the SOR (Art. 17 (3) (b) DSA).

3.3 The wronged user? Internal complaint-handling systems in the DSA

Online platforms, VLOPs and VLOSEs are also obligated to provide an internal complaint-handling system that can be seen as a second step in a platform's reporting or moderation process. Here, a user has the opportunity to use the internal complaint-handling system to lodge complaints about content or accounts for platform decisions within a period of six months (Art. 20 (1) DSA). If a notice received by a platform is not substantiated, the platform can act against the complaint (Art. 20 (3) DSA). Furthermore, this process cannot be fully automated and must have "qualified staff in the loop" of the complaint-handling system (Art. 20 (5) DSA). The question of effective implementation of a complaint-handling system was already questioned in the case of Alibaba in 2024 ('DSA: Commission Opens Formal Proceedings against AliExpress' (European Commission, 2024a).

3.4 The right of a judge or the DSA's answer to it: Out-of-court dispute settlements

After a user has gone through the internal complaint-handling system of a platform, the user still has the right to challenge the content moderation decision: the out-of-court dispute settlement. If a conflict can't be resolved under Art. 20 DSA, the user has the right to "select any out-of-court dispute settlement body that has been certified" according to Art. 21 (1) DSA (Barata, 2023; Coimisiún na Meán, 2024). Such a certification requires mandatory reports; the certified status can also be revoked. According to Art. 21 (3) DSA, redress mechanisms should be easy for users to access to enable them to open a settlement process with an authority in an electronic format. If a case has already been decided, it is not possible for it to be raised again with the dispute settlement body (Art. 21 (2) DSA). Additionally, such a decision does not create binding case law for a platform, as the platform has the freedom to decide similar cases differently. A dispute settlement body must be "impartial and independent, including financially independent" of platforms, have the needed expertise, have a form of remuneration that does not bias the participant in a way that would affect their judgment, be "capable of settling disputes in a swift, efficient and cost-effective manner and in at least one of the official languages", electronically approachable, compliant with the law, apply the rules fairly and have publicly accessible procedures (Art. 21 (3) (a–f) DSA). There currently exist four certified out-

of-court dispute settlement bodies (*ADROIT*, 2024; Europe, 2024; *OPVT*, 2024; *RTR*, 2024; *User Rights*, 2024)

4. In crisis – Please follow the Commission

According to the DSA, a crisis is a situation in which "extraordinary circumstances occur that can lead to a serious threat to public security or public health in the Union or significant parts thereof" (Recital 91 DSA). This rule may have been influenced by the events of the Covid-19 pandemic and was added in quickly following the Russian invasion of Ukraine in February 2022 (Buijs and Buri, 2023; Kettemann and Sekwenz, 2022). Civil society has criticised the subjectivity of the term crisis, the time frames for when a crisis might start or end, the definition of reliable information and the role of human rights in the decision-making process (Access Now, 2022; Coimisiún na Meán, 2024; European Digital Rights, 2024).

When a crisis occurs, the Board adopts a decision to act and the Commission is granted the power to assess the functioning of services, use measures "to prevent, eliminate or limit any such contribution to the serious threat[s]" and be informed about the content in question, the implementation and the impact of the measures demanded (Art. 36 (1) DSA) (Ferreau, 2024). Additionally, the board can issue crisis protocols that provide detailed measures, such as the obligation to display crisis information on platforms (Art. 48 DSA). Crisis protocols can be mandatory or an ex-ante solution for potential crisis situations (Recital 108 DSA).

Any measures implemented by the Commission are bound to certain rules according to Art. 36 (3) DSA, where measures may not exceed a period of three months. Actions need to be "strictly necessary, justified and proportionate" and in line with the Charter of Fundamental Rights; furthermore, clear time frames for measures under the crisis response mechanism must be defined. The DSA requires that decisions to act on a crisis by the Commission be made publicly available, the Board granted the right to access information and provide its views and platforms be immediately informed (Art. 36 (4) DSA). If there is a variety of specific measures, then platforms choose which measure(s) to implement (Art. 36 (5) DSA). Furthermore, the Commission and the platforms should be in dialogue about the implementation, the evaluation of their effectiveness and the goals they seek to achieve (Art. 36 (6) DSA). The Commission must

also report to the EU Parliament and the Council about crisis-response decisions on an annual basis (Art. 36 (11) DSA).

5. Identifying and mitigating systemic risks for intermediaries

The DSA is considered a risk-based Regulation in several aspects of compliance, similar to other EU Regulations such as the GDPR or the AI Act (De Gregorio and Dunn, 2022). The DSA recognises that increased individual and societal risk originates from intermediary services, as many people use these services on a daily basis (Recital 1 DSA). In the DSA, systemic risks are considered in regard to platform functionalities and user behaviour (Brougton Micova and Calef, 2023, p. 6), mixing a top-down and bottom-up approach to risk. Depending on the risks, platforms are required to fulfil a set of obligations (De Gregorio and Dunn, 2022). Search engines were included in the Regulation due to their importance in finding information and maintaining a functioning internet (Kaesling, 2023, p. 533). VLOPs and VLOSEs are required to follow stricter rules due to the increased level of risk associated with such platforms. They are considered to be infrastructures and "de facto public spaces" (Kaesling, 2023, p. 531 transl. by the authors). They need to provide a point of contact for users (Art. 12 DSA), access to the data for the European Commission and for research (Art. 40 DSA) and more transparency (Art. 38, 39, 42). Moreover, external audits are also required (Art. 37). The additional rules that identify more internal processes and measures are defined in Art. 34 and Art. 35 DSA, which will be explained in more detail in the next subsection. Subsequently, the process of external auditing to review the conducted risk assessments will be elaborated.

5.1 That seems pretty risky: Risk assessment under the DSA

According to Art. 34 (1) DSA, VLOPs and VLOSEs need to "identify, analyse and assess" systematic risks once a year (Art. 34(1) S. 2). Systemic risks are not legally defined in the DSA and are only elaborated according to their potential societal impact (Kaesling, 2023, p. 560).

In the following, the Article elaborates on the systemic risks considered in the DSA (Art. 34). First, illegal content (lit. a) is considered to be a high

risk,[5] and the probability of illegal content being distributed on VLOPs and VLOSEs is also considered high (Kaesling, 2023, p. 562).

Subsequently, the legislation mentions "negative effects for the exercise of fundamental rights" (lit. b); these fundamental rights include human dignity, private and family life, the protection of personal data, freedom of expression and information, freedom and pluralism of the media, non-discrimination and the protection of children and consumers (ibid.). One problem concerning fundamental rights – specifically freedom of expression and deliberative democracy – is disinformation (Del Moral Sánchez, 2024, p. 7). Generally, VLOPs and VLOSEs are not obliged to adhere to fundamental rights; however, their position is akin to a public space so their obligation to the public increases (Kaesling, 2023, p. 562f.). The protection of fundamental rights should not lie in the hands of private corporations, and aside from the protection of privacy, fundamental rights were previously not as protected in online spaces compared to the enhanced protection and recognition the DSA provides (Ponce Del Castillo, 2020, p. 3). According to Art. 1 European Charter of Fundamental Rights, the protection of human dignity is critical for the interpretation and application of all other fundamental rights. The protection of human dignity includes the protection against the severe discrimination of vulnerable groups (e.g. due to their sexual orientation) (Borowsky 2019, p. 121), online mobbing and terrorism. In addition, the depiction of child sexual abuse material violates the dignity of children (Kaesling, 2023, p. 563), and denying the Shoah is considered a violation of the dignity of the deceased (Borowsky, 2019, p. 121). Other fundamental rights that are mentioned in Art. 34 lit. b include "respect for private and family life […], the protection of personal data […], freedom of expression and information, including the freedom and pluralism of the media, […] nondiscrimination […], respect for the rights of the child […], and […] a high-level of consumer protection […]".

Furthermore, "negative effects on civic discourse and electoral processes, and public security" (Art. 34 (1)(c), Recital 82) are another risk category. As they are mentioned conjointly, the connection between public debate and electoral processes is emphasised, as these issues may create opportunities that result in danger to public security. Here, information that is not illegal is concerned (Kübler et al., 2023). Social media platforms that are VLOPs

5 For more detailed information on illegal content in the DSA, see Chapter 5 'The Digital Services Act – An Appropriate Response to Online Hate Speech?' by Pascal Schneiders and Lena Auler.

have a responsibility to investigate information interaction that might be part of disinformation campaigns (Kaesling, 2023, p. 567).

Finally, "serious negative effects in relation to gender-based violence, the protection of public health and minors and serious negative consequences to the person's physical and mental well-being" (Art. 34 (1)(d)) are considered to be a particularly high risk. For such cases, the Commission introduced a threshold wherein the negative effects are required to be *serious*. The seriousness of the consequences is not only considered on a societal level but also regarding the individual persons concerned, including, for instance, the psychological damage to individuals moderating content (Pinchevski, 2023).

Codes of conduct provide guidance for the implementation of risk assessment and mitigation. While the Codes are voluntary, they play a crucial role in risk mitigation and auditing and are therefore considered an "inescapable as part of DSA compliance" (Griffin and Vander Maelen, 2023, p. 4). Examples of Codes of Conduct are the Code on Hate Speech (2016) and the Code of Practice on Disinformation (2018, 2022). The Codes of Conduct apply to consequences of systemic risks such as "disinformation or manipulative and abusive activities" (Recital 103 DSA), including deliberative coordinated efforts to manipulate and mislead, which may be particularly harmful to vulnerable recipients of information. In this regard, following a Code of Conduct is considered risk mitigation measure under Art. 35 DSA (Recital 103 DSA). In 2018, the Code of Practice on Disinformation was developed to encourage self-regulatory behaviours to combat disinformation. However, an assessment of the Code concluded that it was unsuccessful due to a lack of commitment, objectives and tools to measure compliance (Sounding Board, 2018). Therefore, the Strengthened Code of Practice (2022) was developed and is a Code of Conduct under Art. 45 DSA; however, it is still voluntary, complementing the DSA and making it a model of co-regulation. In such a model, the interaction between the intermediary and the regulator is key to its success (Del Moral Sánchez, 2024, p. 17).

5.2 Better to avoid it – Risk mitigation under the DSA

Article 35 DSA proposes risk mitigation measures that intermediaries can employ in case of risk detection. These risk mitigation measures should be "reasonable, proportionate and effective" (Art. 35 (1)). Accordingly, in-

termediaries should be "adapting the design, features or functioning of their services, including their online interfaces" (lit. a) and "adapting their terms and conditions and their enforcement" (lit. b). Furthermore, intermediaries should "test(...) and adapt(...) their algorithmic systems, including their recommender systems (lit. d). According to Art. 8 DSA, there is no proposed general monitoring obligation for platforms and their user-generated content; however, the DSA creates new regulatory rules and practices around content moderation systems. According to the Regulation, content moderation can be understood as:

> [...] the activities, whether automated or not, undertaken by providers of intermediary services, that are aimed, in particular, at detecting, identifying and addressing illegal content or information incompatible with their terms and conditions (see Art. 14 DSA), provided by recipients of the service, including measures taken that affect the availability, visibility, and accessibility of that illegal content or that information, such as demotion, demonetization, disabling of access to, or removal thereof, or that affect the ability of the recipients of the service to provide that information, such as the termination or suspension of a recipient's account. (Art. 3 lit. t DSA)

According to the DSA, content moderation is crucial as a remedy against identified systemic risks on VLOPs and VLOSEs (Art. 35 lit. c); however, if content moderation goes wrong, there can also be negative effects on communities (Feuston et al, 2020).

5.3 Audits

Annual systemic risk assessments are required to be structured in audits that follow the guidelines laid out in the Delegated Regulation (DR) to Art. 27 DSA. These assessments should "diligently identify, analyse and assess any systemic risks in the Union". First, an audit can be conducted on the design or functioning of the service or system, the algorithmic system (see Art. 27 DSA) or the use of the service or system. Second, within these three levels, audits should assess the following factors in their risk assessment (Art. 34 (2) (a-e) DSA):

- the design of their recommender systems and any other relevant algorithmic system,
- the content moderation systems,
- the applicable terms and conditions and their enforcement,

- the systems for selecting and presenting advertisements,
- the data-related practices of the provider.

Within these levels and factors, four categories of risks can be differentiated according to the risks outlined in Art. 34 DSA.

Audits are included in the risk assessment reports (Art. 12(1) DR) and have to follow the inner logic and methodology outlined in the DR (Recital 16, Art. 13(2) (b), Art. 2 (6), Art. 10(4) DR). Audits are not only conducted internally by the platforms according to Art 34 DSA, there is also an external component according to Art. 37 DSA – the independent audit – which is conducted by third parties (e.g. consulting firms) to test the systemic risk assessments of platforms according to Art. 37. External audits also must follow a methodology according to Art. 37 (4) DSA in conjunction with Art. 10 DR and must be filed in a report according to Art. 37(4) DSA. If the audit report does not find the platform's initiatives to act against any risks to have been identified or reported sufficiently, the VLOP or VLOSE in question has to address the auditors' concerns and describe the changes made in an audit implementation report according to Art. 37 (6) DSA.

5.4 The deluge of delegated regulations

Delegated Regulations (DRs) further clarify the DSA. For example, Art. 33 on the definition and calculation of average monthly user numbers to designate VLOPs and VLOSEs is defined in the DR (European Commission, 2023b). Additionally, in Art. 34 and 37, audits are more concisely described and define risk classes for auditing, give guidelines on how to use methodologies and tests to evaluate compliance under the DSA, or give further information on what could be understood under "reasonable level of assurance" DR (European Commission, 2023a). Furthermore, according to Art. 40, the DR on researcher data access outlines how such access should be established, how such accreditation processes should look and how the rights and responsibilities for data access can be distributed. In addition, transparency reports include a DR in their outline to further support coherent reporting process structures and create a guideline to standardise the complex reporting duties in Art. 15, 24 and 42 DSA (European Commission, 2022). Another interesting detail about the DRs in question is that the regulator actively included the feedback of stakeholders and research reports (Wagner et al., 2023) during the process of creating these DRs (*European Commission – Have Your Say*, 2023).

6. Conclusion

To conclude, the DSA introduces a groundbreaking regulatory framework that aims to enhance transparency, accountability and user protection across online platforms, with specific attention focused on VLOPs and VLOSEs. This Chapter has provided an overview of the DSA, one of the first efforts to regulate harmful online content and protect users' fundamental rights online. As discussed in section 2, the DSA's emphasis on transparency is pivotal. The Regulation establishes multiple tools to ensure that platforms are open about their operations, including transparency reports (Art. 15, 24, 42), the Terms and Conditions database (Art. 14), the Statement of Reasons database (Art. 17) and the Ad Library (Art. 39). The novel transparency mechanisms for intermediary services include reports, online repositories (such as the Ad Library according to Art. 39) and Statements of Reason (Art. 17). Furthermore, the DSA provides rules for researchers to access platform data to research systemic risks (Art. 40). The DSA's aims to empower users through new roles and rights, including the Trusted Flaggers mechanism (Art. 22) and the internal complaint-handling system (Art. 20), which reflect the DSA's aim to involve users more actively in content moderation processes by giving them the tools to flag illegal content and challenge platform decisions. Furthermore, the introduction of out-of-court dispute settlements (Art. 21) provides users with a structured and accessible way to seek redress when their rights have been infringed upon. The DSA's includes a crisis response mechanism (Art. 36), which allow the European Commission to rapidly implement measures in extraordinary circumstances such as public health emergencies or threats to public security. These mechanisms, which were influenced by events such as the Covid-19 pandemic and the Russian invasion of Ukraine, provide regulators with the flexibility to act swiftly in times of crisis.

Finally, the DSA adopts a risk-based approach to regulating platforms, particularly VLOPs and VLOSEs, which have a significant societal impact due to their size and reach. The DSA requires these platforms to conduct annual systemic risk assessments (Art. 34) focusing on key areas such as illegal content, infringement of fundamental rights and the protection of minors. Risk mitigation measures (Art. 35) are also mandated, obliging platforms to adapt their systems – recommender algorithms and content moderation processes – to minimise risks to users. Additionally, external audits (Art. 37) are required to ensure that platforms' risk assessments are thorough and that they effectively implement mitigation measures.

In summary, the DSA is a transformative regulation that not only aligns with other EU legislative initiatives, such as the GDPR and AI Act, but also pioneers a new era of platform governance. Its holistic approach, integrating transparency, user empowerment, risk management and crisis response, sets a strong foundation for future digital regulation, aiming to create a safer, fairer and more accountable online ecosystem for all users. As the digital landscape continues to evolve, the DSA's provisions will play a crucial role in ensuring that platforms operate in a manner that respects individual rights and societal values.

References

Access Now (2022) 'Civil Society to EU: Don't Threaten Rights with Last-Minute "Crisis Response Mechanism" in DSA' [Online]. Available at: https://www.accessnow.org/press-release/crisis-response-mechanism-dsa/ (Accessed: 19 July 2024).

Appelman, N. and Leerssen, P. (2022) 'On "Trusted" Flaggers', *Yale Journal of Law & Technology,* 24, pp. 452-475.

Barata J. (2023) 'The Out-of-Court Settlement Mechanism under the DSA: Questions and Doubts', *DSA Observatory* [Online]. Available at: https://dsa-observatory.eu/2023/10/26/the-out-of-court-settlement-mechanism-under-the-dsa-questions-and-doubts/ (Accessed: 19 July 2024).

Bayer, J., Holznagel, B., Lubianiec, K., Pintea, A., Schmitt, J. B., Szakács, J. and Uszkiewicz. E. (2021) 'Disinformation and Propaganda: Impact on the Functioning of the Rule of Law and Democratic Processes in the EU and Its Member States - 2021 Update', PE 653.633. Brussels: European Union.

Borowsky, M. (2019) 'GRCh Art. 1 Würde des Menschen' in Meyer, J. and Hölscheidt, S. (eds.) *Charta der Grundrechte der Europäischen Union,* Baden-Baden: Nomos Verlagsgesellschaft, pp. 81–147.

Broughton Micova, S. and Calef, A. (2023) 'Elements for Effective Systemic Risk Assessment Under the DSA', *SSRN* [Online]. Available at: https://doi.org/10.2139/ssrn.4512640 (Accessed: 9 February 2025).

Bujs, D. and Buri, I. (2023) 'The DSA's Crisis Approach: Crisis Response Mechanism and Crisis Protocols', *DSA Observatory* [Online]. Available at: https://dsa-observatory.eu/2023/02/21/the-dsas-crisis-approach-crisis-response-mechanism-and-crisis-protocols/ (Accessed: 19 July 2024).

Bundesnetzagentur (n.d.) *Digital Services Coordinator* [Online]. Available at: https://www.bundesnetzagentur.de/DSC/DE/_Home/stArt.html (Accessed: 24 May 2024).

Carvalho, J. M., Arga e Lima, F. and Farinha, M. (2021) 'Introduction to the Digital Services Act, Content Moderation and Consumer Protection', *Revista de Direito e Tecnologia,* 3(1), pp. 71–104.

Coimisiún na Meán (2024) 'Article 21 Out-of-Court Dispute Settlement. Guidance and Application Form' [Online]. Available at: https://www.cnam.ie/wp-content/uploads/2024/02/20240216_Article21_GuidanceForm_Branded_vF_KW.pdf (Accessed: 19 July 2024).

Comisiún na Méan (n.d.) 'Online Safety' [Online]. Available at: https://www.cnam.ie/online-safety/ (Accessed: 24 May 2024).

De Gregorio, G. and Dunn, P. (2022) 'The European Risk-Based Approaches: Connecting Constitutional Dots in the Digital Age', *Common Market Law Review,* 59(2), pp. 313–26.

De Streel, A., Defreyne, E., Jacquemin, H., Ledger, M. and Michel, A. (2020) *Online Platforms' Moderation of Illegal Content Online. Law, Practices and Options for Reform*, Luxembourg: European Parliament [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf (Accessed: 9 February 2025).

Del Moral Sanchez, M. (2024) 'The DSA and the Fight against Online Disinformation in the Context of EU Law: Avenues for Internal Dialogue and External Territorial Extension', *SSRN Electronic Journal* [Online]. Available at: https://doi.org/10.2139/ssrn.4847475 (Accessed: 26 July 2024).

'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce' (2000) *Official Journal of the European Union,* L178, 17 July, pp. 1–16 [Online]. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed; 9 February 2025).

'Directive (EU) 2019/790 of 17 April 2019 on Copyright and Related Rights in the Digital Single Market and Amending Directives 96 9/ EC and 2001/29/EC' (2019) *Official Journal of the European Union,* L130, May 17, pp. 92–125 [Online]. Available at: http://data.europa.eu/eli/dir/2019/790/oj (Accessed: 9 February 2025).

Dogruel, L., Facciorusso, D. and Stark, B. (2020) '"I'm Still the Master of the Machine." Internet Users' Awareness of Algorithmic Decision-Making and Their Perception of Its Effect on Their Autonomy', *Information, Communication & Society*, 25(9), pp. 1–22.

Drolsbach, C. and Pröllochs, N. (2023) 'Content Moderation on Social Media in the EU: Insights From the DSA Transparency Database', *arXiv*, 7 December [Online]. Available at: http://arxiv.org/abs/2312.04431 (Accessed: 4 February 2024).

Duivenvoorde, B. and Goanta, C. (2023) 'The Regulation of Digital Advertising under the DSA: A Critical Assessment', *Computer Law & Security Review,* 51, 105870 [Online]. Available at: https://doi.org/10.1016/j.clsr.2023.105870 (Accessed: 9 February 2025).

Efroni, Z. (2021) 'The Digital Services Act: risk-based regulation of online platforms', *Internet Policy Review* [Online]. Available at: https://policyreview.info/Articles/news/digital-services-act-risk-based-regulation-online-platforms/1606 (Accessed: 26 July 2024).

Escritt, T. (2019) 'Germany Fines Facebook for Under-Reporting Complaints', *Reuters*, 2 July [Online]. Available at: https://www.reuters.com/Article/us-facebook-germany-fine-idUSKCN1TX1IC (Accessed: 19 August 2023).

European Commission (2016) *Code of conduct on countering illegal hate speech online* [Online]. Available at: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (Accessed: 26 July 2024).

European Commission (2018) *Code of Practice Against Disinformation* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/2018-code-practice-disinformation (Accessed: 26 July 2024).

European Commission (2022) *Strengthened Code of Practice on Disinformation* [Online]. Available at https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation (Accessed: 26 July 2024).

European Commission (2023a) *COMMISSION DELEGATED REGULATION (EU) …/… of XXX supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=PI_COM:Ares(2023)8428591 (Accessed: 9 February 2025).

European Commission (2023b) *COMMISSION IMPLEMENTING REGULATION (EU) …/… of XXX laying down templates concerning the transparency reporting obligations of providers of intermediary services and of providers of online platforms under Regulation (EU) 2022/2065 of the European Parliament and of the Council* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/delegated-regulation-independent-audits-under-digital-services-act (Accessed: 9 February 2025).

European Commission (2024a) *Commission opens formal proceedings against AliExpress under the Digital Services Act*, Press Release [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/IP_24_1485 (Accessed: 19 July 2024).

European Commission (2024b) *Supervision of the designated very large online platforms and search engines under DSA* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (Accessed: 26 July 2024).

European Digital Rights (2022) *A New Crisis Response Mechanism for the DSA* [Online]. Available at https://edri.org/our-work/public-statement-on-new-crisis-response-mechanism-and-other-last-minute-additions-to-the-dsa/ (Accessed: 19 July 2024).

Ferreau, J. F. (2024) 'Crisis? What Crisis? The Risk of Fighting Disinformation with the DSA's Crisis Response Mechanism', *Journal of Media Law,* 16(1), pp. 57-64.

Griffin, R. and Vander Maelen, C. (2023) 'Codes of Conduct in the Digital Services Act: Exploring the Opportunities and Challenges', *SSRN Electronic Journal* [Online]. https://doi.org/10.2139/ssrn.4463874 (Accessed: 9 February 2025).

Heldt, A. (2019) 'Reading between the Lines and the Numbers: An Analysis of the First NetzDG Reports', *Internet Policy Review*, 8(2) [Online]. Available at: http://policyreview.info/node/1398 (Accessed: 12 July 2019).

Hoboken, J., Buri, I., Quintais, J., Fahy R., Appelman N. and Straub, M. (2023) 'Putting the DSA into Practice: Enforcement, Access to Justice, and Global Implications' [Online]. Available at: https://doi.org/10.17176/20230208-093135-0 (Accessed: 9 February 2025).

Hofmann, F. and Raue, B. (2023) 'Einleitung' in Hofmann, F. und Raue, B. (Hrsg.), *Digital Services Act. Gesetz über Digitale Dienste*. Baden-Baden: Nomos, pp. 32–48.

Husovec, M. (2023) 'How to Facilitate Data Access under the Digital Services Act', *SSRN* [Online]. Available at: https://ssrn.com/abstract=4452940 (Accessed: 26 July 2024).

Iosifidis, P. and Nicoli, N. (2021) *Digital Democracy, Social Media and Disinformation*. London: Routledge.

Izyumenko, E., Senftleben, M., Schutte, N., Smit, E. G., van Noort, G. and van Velzen, L. (2024) 'Online Behavioural Advertising, Consumer Empowerment and Fair Competition: Are the DSA Transparency Obligations the Right Answer?', *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=4729118 (Accessed: 21 May 2024).

Jhaver, S., Birman, I., Gilbert, E. and Bruckman, A. (2019) 'Human-Machine Collaboration for Content Regulation: The Case of Reddit Automoderator', *ACM Transactions on Computer-Human Interaction*, 26(31), pp. 1–35.

Just, N. and Saurwein, F. (2024) 'Enhancing Social-Media Regulation through Transparency? Examining the New Transparency Regime in the EU', *TechREG Chronicle,* 2 [Online]. Available at: https://www.zora.uzh.ch/id/eprint/257668 (Accessed: 21 May 2024).

Kaesling, K. (2023) 'Zusätzliche Verpflichtungen in Bezug auf den Umgang mit systemischen Risiken für Anbieter von sehr großen Online-Plattformen und sehr großen Online-Suchmaschinen', in Hofmann, F. und Raue, B. (eds.), *Digital Services Act. Gesetz über Digitale Dienste*. Baden-Baden: Nomos. DSA Kommentar, pp. 631–684.

Kapantai, E., Christopoulou, A., Berberidis, C. and Peristeras, V. (2021) 'A Systematic Literature Review on Disinformation: Toward a Unified Taxonomical Framework', *New Media & Society*, 23(5), pp. 1301–26.

Kaushal, R., van de Kerkhof, J., Goanta, C., Spanakis, G. and Iamnitchi, A. (2024) 'Automated Transparency: A Legal and Empirical Analysis of the Digital Services Act Transparency Database', *Arxiv,* 3 May 2024 [Online]. Available at: http://arxiv.org/abs/2404.02894 (Accessed: 9 April 2024).

Kettemann, M.C. and Sekwenz, M.T. (2024) 'Pandemics and Platforms: Private Governance of (Dis)Information in Crisis Situations', in Kettemann, M.C., Lachmayer, K. (ed.). *Pandemocracy in Europe.* Oxford: Hart Publishing, pp. 263–282.

Kou, Y. and Gui, X. (2021) 'Flag and Flaggability in Automated Moderation; The Case of Reporting Toxic Behavior in an Online Game Community', *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems,* Article 437, pp. 1–12. Association for Computing Machinery [Online]. Available at: https://doi.org/10.1145/3411764.3445279 (Accessed: 24 June 2024).

Kübler, J., Sekwenz, M. T., Rachinger, F., König, A., Gsenger, R., Pirkova, E., Kettemann, M.C., Wagner, B., Krennerich, M. and Ferro, C. (2023) 'The 2021 German Federal Election on Social Media: Analysing Electoral Risks Created by Twitter and Facebook', *Proceedings of the 56th Hawaii International Conference on System Sciences,* 56, pp. 4036–4045.

Murray, J. and Flyverbom, M. (2020) 'Datafied Corporate Political Activity: Updating Corporate Advocacy for a Digital Era', *Organization,* 28(4), pp. 621–640.

Pinchevski, A. (2023) 'Social Media's Canaries: Content Moderators between Digital Labor and Mediated Trauma', *Media, Culture & Society,* 45(1), pp. 212–21.

Ponce Del Castillo, A. (2020) 'The Digital Services Act Package: Reflections on the EU Commission's Policy Options', *ETUI Policy Brief. European Economic, Employment and Social Policy,* 12 [Online]. Available at: https://www.etui.org/sites/default/files/2020-09/The%20digital%20services%20act%20package.%20Reflections%20on%20the%20EU%20Commission%27s%20policy%20options-2-2020.pdf (Accessed: 9 February 2025).

'Regulation (EU) 2022/2065 of 19 October 2022 on a Single Market For Digital Services and Amending Directive 2000/31/EC (Digital Services Act)', *Official Journal of the European Union*, 65 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:2022:277:FULL&from=EN (Accessed: 26 July 2024).

Rodríguez De Las Heras Ballell, T. (2021) 'The Background of the Digital Services Act: Looking towards a Platform Economy', *ERA Forum,* 22(1), pp. 75–86.

Roth, Y. and Lai, S. (2024) 'Securing Federated Platforms: Collective Risks and Responses', *Journal of Online Trust and Safety,* 2(2) [Online]. Available at: https://tsjournal.org/index.php/jots/Article/view/171 (Accessed: 4 March 2024).

Schwemer, S. F. (2019) 'Trusted Notifiers and the Privatization of Online Enforcement', *Computer Law & Security Review,* 35(6), 105339 [Online]. Available at: https://doi.org/10.1016/j.clsr.2019.105339 (Accessed: 9 February 2025).

Schwemer, S. F. (2023) 'Digital Services Act: a reform of the e-Commerce Directive and much more', in Savin, A. and Trzaskowski, J. (eds.) *Research Handbook on EU Internet Law*. Cheltenham: Elgar, pp. 232–253.

Sounding Board (2018) 'The Sounding Board's Unanimous Final Opinion on the So-Called Code of Practice', 24 September 2018 [Online]. Available at: https://www.ebu.ch/files/live/sites/ebu/files/News/2018/09/Opinion%20of%20the%20Sounding%20Board.pdf (Accessed: 26 July 2024).

Trujillo, A., Fagni, T. and Cresci, S. (2024) 'The DSA Transparency Database: Auditing Self-Reported Moderation Actions by Social Media', *arXiv*, 20 January 2024 [Online]. Available at: http://arxiv.org/abs/2312.10269 (Accessed: 9 February 2024).

Wagner, B., Rozgonyi, K., Sekzwenz, M. T., Cobbe, J. and Singh, J. (2020) 'Regulating Transparency? Facebook, Twitter and the German Network Enforcement Act', *Association for Computing Machinery, Proceedings of the 2020 Conference on Fairness, Accountability, and Transparency* [Online]. Available at: https://doi.org/10.1145/3351095.3372856 (Accessed: 22 August 2021).

Werthner, H., Ghezzi, C., Kramer, J. et al (eds) (2024) *Introduction to Digital Humanism: A Textbook*. Berlin: Springer Nature Switzerland.

The Digital Services Act – An Appropriate Response to Online Hate Speech?

Pascal Schneiders & Lena Auler

Abstract

Online hate speech seems to permeate Facebook, X, Telegram, and the like, prompting increased national and supranational pushes for regulation of digital platforms. One of the most recent high-profile legislative frameworks is the Digital Services Act, which includes cross-sectoral and EU-wide moderation, transparency, and other due diligence obligations that are tiered according to the role, size, and impact of the online services. This chapter presents and critically analyses the measures raised in the Digital Services Act that are relevant to curbing hate speech. It concludes with recommendations for the future academic and regulatory approach to online hate speech.

1. Introduction

Social media platforms, such as Facebook, Instagram, and Reddit, have long since become central venues not only for maintaining relationships and seeking entertainment, but also for consuming and commenting on content (Newman, 2023). However, hopes that social media would evolve into arenas of deliberate discourse – if they ever existed beyond the small circle of a tech-savvy avant-garde – can rightly be described as dashed. Instead, there is now a widespread impression that a heated public sphere (Wagner, 2019), an outrage industry (Berry and Sobieraj, 2016), or even digital fascism (Fielitz and Marcks, 2019; Fuchs, 2022) prevails in the posts and comment sections of Facebook and Co. Hate speech, which is not a standardised legal term (Koreng, 2017; Valerius, 2020), but in social science usually refers to the "bias-motivated, hostile, and malicious speech aimed at a person or group of people because of some of their actual or perceived innate characteristics" (Cohen-Almagor, 2011, p. 1; see also Erjavec and Kovačič, 2012; Sponholz, 2023), seems to poison interactions on platforms and beyond (Bayer and Bárd, 2020; Udupa et al, 2021).

Indeed, content analyses have demonstrated hate speech's presence on social media despite the existence of content-moderation measures (Hestermann et al, 2021). Such speech represents only a minority of social media content (Siegel, 2020), and exists mostly in the form of stereotyping rather than the most drastic forms, such as incitements to violence (Paasch-Colberg et al, 2022). Nevertheless, many users are exposed to hate speech. An annual survey of internet users aged 14 and over in Germany shows that the proportion of respondents who had encountered hate speech online has remained consistently high for years (around 75%). Especially adolescents and young adults are exposed to hate speech (Landesanstalt für Medien NRW, 2023; see also Keipi et al, 2017). For those affected, especially younger people, hate speech has primarily psychological consequences, ranging from emotional stress and anxiety to depression (Keipi et al, 2017; Lee-Won et al, 2020). Furthermore, hate speech can silence vulnerable groups and demobilise them from participating in public life. By spreading hate speech and suggesting a or intimidating the majority opinion, highly active predominantly right-wing, networks can discourage people who are not themselves under attack from entering into the discourse and normalise negative stereotypes and radical views in wider circles (Das NETTZ et al, 2024; Gelber and McNamara, 2016). Not last, hate speech can incite others to make extremely uncivil statements or even to commit acts of violence (Müller and Schwarz, 2021; Williams et al, 2020).

It seems plausible that it is the specific platform logics that facilitate the emergence, dissemination, reception, and impact of hate speech (see also Recuero, 2024). That is, the affordances, rules, and algorithmic values of social media encourage low-threshold communication and networking, and incentivise exaggerated and emotional content – all of which serves to create a fertile environment for hate speech. In any case, "proprietors of spaces are responsible for the features of their spaces that present hazards by posing risks of harm if not managed" (Price, 2021, p. 260).

While hate speech has long been an issue that has received little political attention (Banks, 2010), politicians now never tire of insisting that the internet is "no lawless space" (see, for example, EPP Group, 2021; The Economist 2018; Cooper 2018). Against this backdrop, content moderation, understood as "the screening, evaluation, categorization, approval or removal/hiding of online content according to relevant communications and publishing policies" (Flew et al, 2019, p. 40; see also Art. 3 lit. t DSA), is becoming increasingly important. Soft law measures, which at the EU level

are essentially the "Code of conduct on countering illegal hate speech online" implemented in 2016 together with Facebook, Microsoft, Twitter (later, X), and YouTube (European Commission, 2016), and the Commission Recommendation (EU) 2018/334 of 2018 on measures to effectively tackle illegal content online, were clearly insufficient in the Commission's view for curbing hate speech. The European Commission (EC) saw a need for improvement in terms of transparency and feedback to users on the decisions about their notices. The Audiovisual Media Services Directive (AVMSD) (Directive 2010/13/EU), which prohibits the distribution of content that incites violence or promotes hatred, only applies on a sector-specific basis, e.g., to providers of video-sharing platforms, but not to text-based media or platforms. Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online, which entered into application in June 2022, is limited to illegal terrorist content.[1]

Accordingly, the EC presented the proposal for a Digital Services Act (DSA) (European Commission, 2020b) in December 2020 together with the proposal for a Digital Markets Act (DMA) (European Commission, 2020a).[2] The final version of the DSA (Regulation 2022/2065), which came into full force in February 2024, serves to update the 2000 Directive on electronic commerce (e-Commerce Directive) (Directive 2000/31) and significantly extends binding platform regulation. Some of the recitals, definitions, and procedures of the above-mentioned Code of Conduct and Commission Recommendations have been recognisably incorporated into the DSA (Cole et al, 2020). While the main features of the existing liability regime enshrined in the e-Commerce Directive remain "essentially the same" (Jaursch, 2021, N. 16; see also Cauffman and Goanta, 2021; Hofmann, 2023, p. 113), the DSA introduces detailed new transparency, moderation, and other due diligence rules, including risk assessments, au-

1 The regulation provides for hosting service providers to be obliged to apply measures to remove terrorist content from their services without delay. Authorities to be designated by the Member States (whether administrative, law enforcement, or judicial) are authorised to order hosting service providers to remove or disable access to terrorist content found to be illegal in a court or administrative decision within one hour throughout the EU (Art. 3 para. 1 Regulation [EU] 2021/784). In addition, service providers may be required to take further measures to prevent the public dissemination of terrorist content, such as the establishment of reporting mechanisms for users (Art. 5 para. 2b Regulation [EU] 2021/784).

2 For more information on the Digital Markets Act, see Chapter 6 'The Brave Little Tailor v. Digital Giants: A Fairy-Tale Analysis of the Social Character of the DMA' by Liza Herrmann.

dits, and research data access rules. In so doing, the DSA aims to ensure a harmonised, safe, predictable, and trustworthy online environment in which the fundamental rights enshrined in the EU Charter of Fundamental Rights (CFR) are "effectively protected" (Art. 1 para. 1 DSA) – this also includes the protection of the personal rights of those affected by hate speech (Kalbhenn and Hemmert-Halswick, 2021; Kapusta, 2024). Consequently, significant hopes are placed on the DSA to help curb hate speech. As early as October 2023, the EC sent X (formerly, Twitter) its first formal request for information under the DSA due to the spread of violent content and hate speech after the Hamas-led attack on Israel (European Commission, 2023a). In January 2025, a revised version of the Code of conduct on countering illegal hate speech online (the 'Code of conduct+') was integrated into the regulatory framework of the DSA. To date, the Code of conduct+ was signed and submitted for integration under the DSA by services such as Facebook, Instagram, LinkedIn, Snapchat, TikTok, Twitch, X and YouTube (European Commission, 2025b).The DSA may also have been motivated by the fact that, in recent years, some Member States have already made national progress in terms of new requirements for content moderation on digital platforms. For instance, Germany introduced the "Netzwerkdurchsetzungsgesetz" (NetzDG, Network Enforcement Act) (BGBl. I 2017, p. 3351), which came into force in January 2019, France implemented the "loi visant à lutter contre les contenus haineux sur internet" (loi Avia, "law aiming to fight against heinous content on the internet") (LOI n° 2020-766),[3] and Austria advanced the now-repealed "Kommunikationsplattformen-Gesetz" (Communication Platforms Act) (BGBl. I Nr. 151/2020), which came into force at the beginning of 2021. The NetzDG in particular, which may well have been the first law of its kind, has attracted global attention, been subject of controversial debate (Schulz, 2019, pp. 13–14), and has served as a source of inspiration for the DSA (Holznagel, 2021, p.123).

The DSA has been described as a "legislative mega-project" (Holznagel, 2021, p. 123) and a "constitution for the internet" (Geese, 2022). It is said to "represent the furthest reaching expansion of platform regulation in the OECD nations to date" (Cioffi et al, 2022, p. 828), potentially affecting the

3 In June 2020, the Conseil Constitutionel declared the law passed by the National Assembly in May of the same year to be unconstitutional, particularly because the one-hour deletion period imposed on the platforms for obviously illegal content constituted an unreasonable, unnecessary, and disproportionate interference with freedom of expression (Décision n° 2020-801 DC du 18 juin 2020, para. 8). The law was subsequently adapted to the court's requirements and published.

freedom of expression of millions of EU citizens and having a regulatory impact far beyond the Union's borders. Therefore, its measures against hate speech and suitability should be analysed all the more intensively (Latzer et al, 2019). In particular, experience with the NetzDG can help to understand the opportunities and risks of the content moderation measures against illegal content provided for in the DSA. The remainder of this chapter discusses the ways in which hate speech is dealt with within the DSA. First, the general regulatory approach of the DSA is discussed. Next, relevant provisions for platforms (in particular, the notice and action procedure), additional due diligence obligations for very large online platforms (VLOPs), and the transparency obligations contained in the DSA are presented. Subsequently, selected aspects of the regulation, including the privatisation of law enforcement and the effectiveness of content moderation in dealing with hate speech, are critically discussed. The chapter concludes with recommendations for the future regulatory treatment of hate speech.

2. Regulation of online hate speech in the DSA

2.1 Regulatory approach of the DSA for content moderation

In the context of platform regulation, particularly when it comes to the design of provisions for content moderation and dealing with hate speech, EU legislators face the challenge of harmonising the interests of the various stakeholders involved in digital communication. This proves to be a difficult balancing act, especially as there are multiple different interests in this context (Berberich, 2023, p. 130).

The fundamental rights of communication require the guarantee of open discourse as a basic prerequisite for a democratic society. On the one hand, the fundamental rights of users, who can invoke their freedom of expression and information when posting and consuming content (Art. 11 CFR), must be taken into account. At the same time, it must be ensured that users are adequately protected from the negative consequences of the dissemination of unlawful content, such as discrimination (Art. 21 CFR). Moreover, users must be guaranteed that, in case of an infringement, they can also take action in the digital communication space. On the other hand, due diligence obligations affect the services' freedom to conduct business (Art. 16 CFR). For their part, the services can also invoke the right to

freedom of expression. When drafting their terms of use, the providers can decide within the limits of their private autonomy which requirements they wish to set for the use of their services, and can thus also moderate unwanted (but not illegal) content on their platforms (Adelberg, 2022; Berberich, 2023, pp. 144–155).

The DSA attempts to address these complex interests by opting for a regulatory concept based on state–private co-regulation (Hofmann and Raue, 2023, p. 37). The legislator delegates the moderation of the content published on their platforms to the service providers, which seems to be without alternative considering the large amounts involved (Brauneck, 2024, p. 379). Indeed, questionable content can hardly be viewed and classified manually. The DSA also imposes a variety of due diligence obligations on platforms, which act as counterweights to the services' privileged liability and which the DSA can monitor and enforce by establishing a European supervisory structure. For example, providers of intermediary services are obliged to conduct content moderation "in a diligent, objective and proportionate manner" and to take the fundamental rights of the services' users into account (Art. 14 DSA). By limiting itself to procedural, content-independent requirements, the Regulation guarantees the protection of fundamental rights through procedures and a principle for procedural fairness (Berberich, 2023, p. 130).

2.2 Illegal content and hate speech

The DSA mainly targets *illegal* hate speech (Recitals 12, 62, 80, 87, 106 DSA), but does not define *what* content is illegal, just as the EC Directive does not define illegal activities. What is defined as illegal remains (for the time being) a matter for the Member States' or other EU legislation (Art. 3 lit. h DSA). However, there are (as yet) no legal definitions of hate speech as a legal concept in the EU Member States (European Commission, 2021). This means that hate speech – that is, the combination of a (supposed) group reference and the public, inflammatory defamation of this group or its (supposed) members (see Section 1) – does not necessarily have to be unlawful; it can also be contained in permissible expressions of opinion (Brugger, 2003). A binding framework for the definition and prosecution of serious forms of racist and xenophobic hate speech and crimes was established by the Council of the European Union in Framework Decision 2008/913/JHA of 28 November, 2008. In the report on the implementation

of the Council Framework Decision, the Commission clarifies that "publicly inciting to violence or hatred directed against a group of persons or a member of such a group defined by reference to race, colour, religion, descent or national or ethnic origin", as well as "publicly condoning, denying or grossly trivialising crimes of genocide, crimes against humanity and war crimes" (Art. 1a, 1c Framework Decision 2008/913/JI) is to be treated as a (racist or xenophobic) criminal offence or *hate speech* in the Member States (European Commission, 2014). The conduct must be intentional and have a certain potential impact, i.e., be carried out "in a manner likely to incite violence or hatred against such a group or a member of such a group" (Art. 1c Framework Decision 2008/913/JI). At the end of 2021, the EC asked the Council to introduce an EU-wide definition of hate speech and include it in the list of so-called EU crimes. The latter are crimes of a particularly serious nature with a cross-border dimension, as set out in Art. 83 para. 1 of the Treaty on the Functioning of the European Union (TFEU) (European Commission, 2021). This would be accompanied by EU-wide minimum rules on the definition of criminal offences and penalties. However, the process has been stalled in the Council since 2022 (European Parliament, 2024).

2.3 Provisions for hosting services, online platforms, and VLOPs

The DSA does not impose completely new measures on digital platforms. They have been active in self-regulation for many years, and automatically and proactively moderate large-scale, third-party content (Gorwa et al, 2020; Klonick, 2018.). Thus, the DSA formalises practices and standards for curbing hate speech. The horizontal obligations for all online intermediaries listed in the DSA are graded according to the scope of the digital services, which are divided into: 1) intermediary services, 2) hosting services, 3) online platforms, and 4) VLOPs and very large search engines (VLOSEs) ("pyramid-model"; Hofmann and Raue, 2023, p. 33). While intermediary services merely pass on information provided by users or store it temporarily for the sole purpose of (efficient) transmission, hosting services store the information provided on behalf of their users (Art. 3(g) DSA). Hosting service providers that store information and make it available to the public on behalf of a user (e.g., app stores and social media platforms) are considered online platforms (Art. 3(i) DSA). VLOPs have a significant reach in the EU (by definition, at least 45 million monthly active users or, in

case of a decreasing or increasing population, 10% of the EU population) (Art. 33 para. 1 and 2 DSA) and have a particular social and economic impact (Justification and Recital 79 DSA). Accordingly, they must fulfil the most comprehensive catalogue of obligations, including internal risk assessments, external audits, and data exchanges with authorities and researchers. To date, the Commission has designated two VLOSEs (Bing and Google Search) and 25 VLOPs, including Instagram, YouTube, TikTok, Facebook, X, and LinkedIn (European Commission, 2025b).

The content moderation measures formulated in the DSA include mechanisms for notifying illegal content as well as, in a broader sense, complaint procedures, out-of-court dispute settlement bodies and, last but not least, service providers' obligation to report suspected serious offences to the competent authorities. These decisions by the platforms should be swift, transparent, and contestable for all parties involved (de Streel et al, 2020, p. 79). In the following, the measures contained in the DSA – from liability obligations for user-generated content to due diligence obligations concerning the design and operations of services – are considered in greater detail. First, it is important to discuss when platform providers are responsible for the user-generated content disseminated on the platforms.

2.3.1 Notice and action procedure

At the heart of the DSA's content moderation measures is Art. 16, which requires hosting services and (VL)OPs to establish procedures for individuals or institutions to provide notices for content they consider to be illegal. The notice and action mechanism provided for in Art. 16, especially the presumption of knowledge in para. 3, is closely linked to the liability regime in Chapter II of the Regulation (Gerdemann and Spindler, 2023, p. 8; Raue 2023, p. 290). The liability privileges established in Chapter II exempt providers from responsibility for third-party content (Hofmann, 2023, pp. 129–131). Art. 8 DSA clarifies – in line with the liability concept of the e-Commerce Directive – that the providers of intermediary services are not subject to any proactive precautionary and investigation obligations regarding illegal content. This privilege is based on the notion that, due to the large amount of content that is distributed on platforms, providers are unable to check every single piece of content individually. Without the privilege, business models of online platforms could be jeopardised (Hofmann, 2023, p. 184). They can only be obliged to block or remove content as soon as they become aware of illegal activity or content. Knowl-

edge may be obtained, for example, through a notification by users or other organisations in the sense of Art. 16 (para. 3). The notice and action mechanism thus compensates for a weakness in liability by implementing a procedural reporting obligation and counterbalancing the exemptions from liability (Legner, 2024, p. 106; Raue, 2023, p. 289). Service providers are obliged to process all notices and decide on them "in a timely manner" (Recital 52 DSA). If they use automated means for processing or decision-making, the person or organisation that has submitted the notice must be informed of this (Art. 16 para. 6). In contrast to Regulation (EU) 2021/784 or the NetzDG, the DSA does not set any time limits for the processing period. The NetzDG required social network providers to remove or block access to "manifestly unlawful" content reported by users or complaints bodies within 24 hours. However, the signatories of the Code of conduct+ committed to review the majority (at least 50%) of hate speech notices from so-called (trusted flagger-like) Monitoring Reporters within 24 hours (European Commission, 2025a).

According to the DSA, service providers must inform users and give reasons when users are affected by the following restrictive moderation decisions that are imposed on the ground that the user-generated or -distributed information is illegal or incompatible with the terms and conditions: a) any restrictions of the visibility of specific information items, such as the removal, demoting, or blocking of content; b) restriction of monetary payments; c) suspension or termination of the provision of the service in whole or in part; and d) suspension or termination of the user's account. The statement of reasons shall be provided at the time of the removal or blocking at the latest (Art. 17 para. 2 DSA). If individuals or entities abuse the notice and action mechanisms by frequently submitting obviously unfounded notices – i.e., for the purpose of silencing marginalised groups (Duffy and Meisner, 2023) – the platform providers shall suspend the processing of the notices and complaints (Art. 23 para. 2 DSA).

Likewise related to content moderation, Art. 7 of the DSA introduces the so-called "good Samaritan privilege". It means that providers benefit from the liability privileges of the DSA if they conduct voluntary investigations on their own initiative or take other measures to detect, identify, remove, or disable access to illegal content. The provision clarifies that voluntary investigations do not automatically establish an active role that would remove the liability privileges. It is intended to prevent platforms that want to proactively prevent infringements with good intentions from being penalised (Koehler, 2024, p. 118; Kuczerawy, 2021). Providers should

not be deterred from taking voluntary measures. However, they must ensure that an objective, non-discriminatory, and proportionate procedure is in place that takes into account the rights and interests of all parties involved (Hofmann, 2023, p. 128). In this context, according to Recital 26, providers should take protective measures against the unjustified removal of lawful content. To that aim, providers should, for example, take reasonable measures to ensure that, where automated tools are used to conduct such activities, the relevant technology is sufficiently reliable to limit to the maximum extent possible the rate of errors.

In addition, the DSA encourages cooperation between platforms and third parties – so called trusted flaggers – in detecting and notifying – and only of – illegal or unlawful content. Trusted flaggers receive notices of illegal content from users, but can also search online platforms for illegal content themselves. They are awarded by the Digital Services Coordinators (DSCs)[4] upon request and have to be independent from online platforms, but not necessarily from state authorities (Art. 22 para. 2 DSA). Accordingly, trusted flaggers can include industry organisations, authorities as Europol, or the criminal content units of national law enforcement agencies, including the National Internet Referral Unit at the Federal Criminal Police Office (Bundeskriminalamt, BKA) in Germany[5] (Recital 61 DSA).[6] Trusted flaggers are required, among other things, to have expertise in dealing with illegal content, to represent collective interests, and to carry out their activities diligently, accurately, and objectively. Notices submitted by trusted flaggers should be given priority in the platforms' content mod-

4 The DSCs are appointed by Member States and are responsible for various issues relating to the application and enforcement of the Act (Art. 49(2) DSA). Together with the Commission, coordinators and – depending on specific Member State provisions – additional competent national authorities form the DSA's oversight structure. The DSCs should fulfil their tasks impartially and independently, i.e., they must not take instructions from other authorities (Art. 50 para. 2 DSA). In extreme cases, they are authorised to take interim measures to prevent the risk of serious harm (Art. 51 para. 2e DSA). In addition, a European Board for Digital Services, which advises the coordinators and the Commission, will help ensure the uniform application of the act (Art. 61 para. 2a DSA).

5 Internet Referral Units (IRUs) actively search the internet for criminal or extremist content. On the potential for abuse of the EU-wide IRUs, see Chang (2018), who expressed the concern that "IRUs are setting a dangerous precedent of state-initiated, privately-enforced, and extra-legal censorship that could be abused to limit speech that is neither genuine incitement to violence nor terrorism" (p. 124).

6 As part of the efforts to combat terrorist content, such service providers as Google and YouTube have already awarded IRUs' Trusted Flagger status (Chang, 2018).

eration decision (Art. 22 para. 1 DSA). That is, the decision on the content of illegal content remains with the platforms (Ruschemeier, 2024). If an investigation by the DSC reveals that a trusted flagger no longer fulfils its requirements, the DSC can revoke that status. This is the case if, for example, the trusted flagger demonstrates a lack of expertise, diligence, and objectivity, or frequently submits inaccurate or unsubstantiated notices. Investigations can be made ex officio – that is, a regulatory authority may initiate an investigation on its own without a complaint having been filed – or in response to information from third parties regarding the behaviour of trusted flaggers (Art. 22 para. 6–7 DSA). As such, the DSA does not provide for the permanent and regular watching of the watchmen; instead, the monitoring of trusted flaggers is largely based on the observation of their work by third parties.

It should be noted that digital platforms have been working with trusted flaggers for years, among other reasons, because of the Code of Conduct on countering illegal hate speech online (see Section 1). In Germany, trained organisations participating in YouTube's Priority Flagger programme include, for example, the BKA, several state criminal investigation offices, jugendschutz.net, the German Association for Voluntary Self-Regulation of Digital Media Service Providers (Freiwillige Selbstkontrolle Multimedia-Diensteanbieter, FSM), media state authorities, and non-profit associations. Their notices of content that violates YouTube's community guidelines are given priority (Google and Youtube, 2019).

2.3.2 Complaint and redress mechanisms

According to Art. 20 para. 1 of the DSA, users can dispute: 1) the removal, blocking, or demoting of content deemed illegal or incompatible with the general terms and conditions; 2) the suspension or termination of the service; 3) the suspension or termination of the user account; and 4) the suspension or restriction of monetisation options by the service provider. This should be possible via an internal complaint-handling system for a period of at least six months after the moderation decision. It should be possible to lodge a complaint regardless of whether the moderation decision was made proactively by the platform or in response to a notice from a user or trusted flagger. Online platforms must process complaints promptly. Furthermore, users should be able to appeal to an independent out-of-court dispute settlement body certified by the Member State's DSC (Art. 21 DSA). If the dispute settlement body decides in favour of the user, the online

platform will bear all fees and costs. If the decision is unfavourable to the user, the user shall bear only his own fees and costs (Art. 21 para. 5). Users are still free to seek legal protection in court against the online platform's decision to restrict an information piece, payments, account, or its service.

2.3.3 Cooperation with authorities

Moreover, the DSA requires service providers to cooperate with the authorities. This includes reporting obligations and complying with official orders. For example, the DSA obliges providers of hosting services to contact the respective Member State's law enforcement or judicial authorities if they have reasonable grounds to suspect that a serious criminal offence "has taken place, is taking place or is likely to take place". In this context, the provider shall make all relevant information available to the authorities (Art. 18 para. 1), including, *where relevant*, information required to locate and identify the respective user of the service (Recital 56).

Further to reporting, the DSA gives national judicial or administrative authorities the option of issuing reasoned orders to providers of intermediary services, including foreign providers, to provide information about individual users (Art. 10) or to take action against certain content found to be illegal (including cross-border content) (Art. 9). The EU Regulation on addressing the dissemination of terrorist content online (Regulation 2021/784)[7], which entered into force in June 2022, contains a similar mechanism for taking action against certain types of illegal content. The orders addressed to providers might also be aimed at preventing the reappearance of illegal content, but without imposing a general monitoring obligation (Recital 30). When determining the territorial scope of the order, the authorities are required to weigh up the interests at stake and, in particular, to consider the rights enshrined in the EU Charter of Fundamental Rights, such as the freedoms of expression and information (Recital 36 DSA). The official information and moderation orders must be documented in the transparency reports (Art. 15 para. 1a DSA). In case providers do not comply with the orders, the DSA itself does not lay down any consequences, with enforcement instead being a matter of national law. This stands in contrast with the information obligations under Art. 9 para. 1 and Art. 10

7 For more information on this Regulation, see Chapter 7, 'Eyes shut, fingers crossed: the EU's governance of terrorist content online under Regulation 2021/784' by Valerie Albus.

para. 1 DSA, which can be enforced by means of the regulation, such as through fines (Recital 32 DSA; see also Hofmann, 2023, p. 196, 201). Providers merely have to state that they have received the order and how they have complied with it (Art. 9 para 1, Art. 10 para. 1).

2.4 Additional due diligence obligations for providers of VLOPs and VLOSEs

VLOPs and VLOSEs must fulfil special due diligence obligations, including risk assessments, risk mitigation, audits and data access. The supervision and enforcement of these obligations is the sole responsibility of the EC (Art. 56 and Art. 2 DSA).

2.4.1 Risk assessment and mitigation

Risk assessments relate to systemic risks arising from the design, functioning, use or misuse of the services (in accordance with Art. 34 para. 1 DSA). Systemic risks include: a) the dissemination of illegal content (Recital 80 gives the example of "illegal hate speech"); b) adverse effects of the service on fundamental rights (including the fundamental rights to human dignity and to freedom of expression and information); c) negative effects on democratic and electoral processes, social debate, and public safety; and d) negative effects in relation to gender-based violence, the protection of public health and minors, and serious negative consequences to a person's physical and mental well-being. Risk analyses must be conducted by the platforms themselves ("first party audit"; Meßmer and Degeling, 2023), proactively and on an annual basis, and before the introduction of new, critical functionalities (Art. 34 para. 1 DSA). Determining the extent to which hate speech constitutes a systemic risk arising from the design, operation, or use of VLOP/VLOSE services is thus initially the responsibility of the platforms. In doing so, they must pay particular attention to: 1) the terms and conditions, 2) the content moderation systems, and 3) the design of the algorithmic recommender systems. The procedure and criteria of the analysis are not predetermined in more detail. With the "risk management framework" (European Commission, 2023a), the EC proposed a methodology for risk assessment and mitigation (however, in the context of Russian disinformation campaigns and not in relation to hate speech). Accordingly, a distinction can be made between qualitative and

quantitative risk indicators. The quality of a risk posed by a particular type of content is assumed to be a function of a speech's context, the speaker's position or intent, the content or form of the speech, the reach, size, and characteristics of the audience, and the likelihood of harm. Quantitative measures comprise the audience's size and exposure to and engagement with the content, the content's prevalence, and the influence of algorithmic promotion (European Commission, 2023a).

If the VLOPs identify internal systemic risks, they must take reasonable, proportionate, and effective measures to mitigate them. The DSA lists a number of non-exhaustive measures in this regard, including the adaption of the terms and conditions, internal decision-making processes, the design, features, or functioning of their services, the advertising systems, the algorithmic recommender systems, and the content moderation processes (Art. 35 para. 1 DSA). In particular, platforms could adapt the responsiveness to user notices, the speed and consistency of removal and labelling, and the de-amplification of illegal or otherwise harmful content (algorithmic down-ranking, the removal of recommendation, searchability, and/or monetisation) (European Commission, 2023a). Moreover, VLOPs can cooperate with trusted flaggers to reduce systemic risks (Art. 35 para. 1g). The DSA does not concretely specify how platforms should proceed, thereby enabling VLOPs to try out different risk mitigation practices. However, the EC may furthermore require the application of preventive and remedial crisis response measures to assess threats and related measures (Art. 36), and request (VL)OPs to participate in the development of codes of conduct for risk reduction (Art. 45 DSA). Correspondingly, the EC announced that adherence to the Code of conduct+ may be considered as an appropriate risk mitigation measure for VLOPs and VLOSEs (European Commission, 2025c).

The internal risk analyses and mitigation plans must be assessed for compliance by independent organisations ("second-party audit"; Meßmer and Degeling, 2023) at least once a year (Art. 37 DSA). The audit organisations are commissioned by the service provider. The EC has issued a Delegated Act (2024/436) with rules on independent audits to assess VLOPs' and VLOSEs' compliance with the DSA. According to Art. 290 TFEU, the Commission can use delegated acts to supplement or amend existing legislative acts. The aforementioned Delegated Act provides auditors with fairly comprehensive access to information on procedures and processes, decision-making structures, IT systems, data sources, algorithmic systems, information technology systems, testing environments, personnel, and in-

ternal compliance procedures (Art. 5 Delegated Act). It specifies audit procedures, defines minimum standards, and seeks to allow a certain degree of comparability of the reports. However, it does not specify any methods or quality criteria according to which the audits are to be conducted. The services were to be audited for the first time at the end of August 2024.

2.4.2 Data access

Access to platform data by independent research institutions is essential for assessing the extent and impact of hate speech (King and Persily, 2019; Rieder and Hofmann, 2020; Stark et al, 2020). Art. 40 para. 4 of the DSA – which was extensively amended during the legislative process – provides for private non-public access for "vetted researchers". This makes the DSA the first EU law to enable mandatory data access (Jaursch and Lorenz-Spreen, 2024). The possibility of data access is linked to the condition that the research contributes to: 1) the detection, identification, and understanding of systemic risks (Art. 34 para. 1) and to 2) the assessment of the adequacy, efficiency, and impact of risk mitigation measures (Art. 35). The draft Delegated Act (DDA) laying down the technical conditions and procedures under which VLOPs and VLOSEs are to share data mentions a variety of data that allow to study systemic risks. Among these are user-related data such as profile information, relationship networks, individual-level content exposure and engagement histories; interaction data such as comments or other engagements; data related to content (personalised) recommendations, and data related to content moderation and governance (Recital 12 DDA). This should also allow for studies on the role of platform logic and algorithmic recommendations in the dissemination of hate speech. Platforms shall make available an overview of the data inventory of their services easily accessible online, including examples of available datasets and suggested modalities to access them (Art. 6.4 DDA). Such modalities may be, among others, data transfer to the vetted researchers, and a transmission of the data to and storage in a secure processing environment which are to be operated by data providers themselves or by a third party (Recital 16 DDA). How data access is organised in detail is, to some extent, up to the platforms. This includes how the application programming interface (API) should be designed or in which format data should be made accessible (Van Drunen and Noroozian, 2024). As a first step, (groups of) researchers have to submit an application for vetted researcher status to the DSC where the platform(s) of interest is/are based or to the DSC of

the research organisation's Member State. In the course of this process, the researchers submitting the application must address the specific research for which they consider data access to be necessary (Art. 40 para. 8). One of the admission requirements is that the researchers must be affiliated to scientific (not exclusively academic) research organisations and do not pursue commercial interests. This may also include civil society organisations. Researchers can also be non-EU based (Albert, 2024). Within 21 days from the receipt of a data access application that fulfills all prerequisites (such as information about funding, and a description of the research project and planned methodology; Art. 8 DDA), the DSC where the main establishment of a provider is located will decide whether to transmit a reasoned request to the relevant VLOP or VLOSE and inform the researcher of its decision (Art. 7 DDA). The DSC also determines the modalities according to which access to the data is to be granted by the platform. A key factor here is how sensitive the data is (Art. 9 DDA). The platform then has 15 days to ask the DSC for amendments to the request. This is only possible if the service provider considers that it cannot comply with the request due to a lack of access to the data or due to concerns about the security of the service or the protection of confidential information (Art. 40 para. 5). However, the platform provider must offer alternatives on how access to the requested (or other) data can be granted (Art. 40 para. 6). This makes it more difficult to evade data access by invoking business secrets. The DSC decides on the request for amendment within a further 15 days. DCSs may consult independent experts before formulating a reasoned request or taking a decision on an amendment request (Art. 14 DDA).

In addition to the data access, platforms should provide vetted researchers with the relevant metadata and data documentation (such as codebooks) so that they can cope with the data (Recital 26 DDA). In future, a data access portal hosted by the EC will provide a public overview of all reasoned requests sent by the DCSs (including not successful ones). VLOPs and VLOSEs are also obliged to provide immediate access (e.g., without having to contact a supervisory authority) to (real-time) data that are *publicly* accessible in their online interface by researchers and used to investigate systemic risks (Art. 40 para. 12). This can be interpreted as a "right to scrape" (Klinger and Ohme, 2023). Said publicly available data may, for example, include data "on aggregated interactions with content from public pages, public groups, or public figures, including impression and engagement data such as the number of reactions, shares, comments from recipients of the service" (Recital 97). As it is not limited to researchers who

are affiliated to a research organization, NGOs and journalists could also make use of this right.

2.5 Transparency obligations

Art. 15 DSA stipulates that providers of intermediary services and of (VL)OPs must disclose the measures they have taken regarding notices submitted in accordance with Art. 16 or on their own initiative in a transparency report published at least once a year. Shorter reporting cycles of six months apply to VLOPs (Art. 42 para. 1). In the transparency reports, the service providers must indicate whether the moderation decisions were made on a legal basis or according to their own general terms and conditions (Art. 15 para. 1b). Online platforms must also state, among other things, the extent to which automated means are used for content moderation, as well as their precision (Art. 15 para. 1c, 1e). As the DSA thus formulates transparency obligations regarding both illegal content and content that does not comply with the general terms and conditions, platforms cannot escape regulation by (increasingly) moderating according to their own standards. Such an effect was observed after the introduction of the NetzDG in Germany (Kalbhenn and Hemmert-Halswick, 2021).

Further to the reporting obligations relating to the user notices procedures, VLOPs and VLOSEs must file publicly available reports outlining the results of the first-party audits on risk analysis, but only after they have been audited by independent organisations (Art. 42 para. 4a). They also have to report on the risk mitigation measures they have been recommended by audit organisations and on those they have implemented (Art. 42 para. 4b, 4d). The second-party audit reports (on the service providers' compliance with the DSA regulations on risk assessment and mitigation) must be published within three months of receipt from the auditing organisation (Art. 42 para. 4c). Last but not least, vetted researchers who have been granted access to data are obliged to make their research results available free of charge "within a reasonable period after the completion of the research" (Art. 40 para. 8g).

In light of the above, it remains to be seen how effective and appropriate the DSA's measures are for combatting hate speech. Certainly, this question can only be answered after a longer period of time, when provisions have been fully implemented and empirical legal studies have been conducted.

However, some evaluation criteria and critical aspects can already be discussed.

3. Evaluation of the Regulatory Measures

3.1 Legitimacy and accuracy of content moderation

In terms of evaluation criteria, regulatory measures should first and foremost be legitimate (i.e., in line with fundamental rights). Furthermore, they should be suitable for solving the identified problem – that is, the low-threshold, significant generation and dissemination of hate speech, in particular on social media platforms. This solution should be appropriate, i.e. it should consider and balance different fundamental rights.

In the run-up to the implementation of the NetzDG in Germany, there was fierce criticism of an alleged privatisation of law enforcement (Pohlmann et al, 2023). This accusation can also be applied to the DSA (Cauffman and Goanta, 2021). In the first instance, it is the service providers who interpret the law and decide which reported content is litigable and should thus be removed or blocked (however, without the service providers taking over the prosecution and the final decision still being made by the courts; Hong, 2022). Other concerns that have been raised in connection with the NetzDG relate to the restriction of freedom of expression through over-removal by service providers (Mchangama and Fiss, 2019). After all, the NetzDG would create economic and regulatory incentives for service providers to remove content in cases of doubt in order to avoid reputational damage or fines (Buiten et al, 2020). With regard to the DSA, it's "good Samaritan" clause increases the risk of overblocking, as it encourages platform providers to engage in proactive content moderation – with the latter being challenging for external observers to comprehend (Kuczerawy, 2021).

Furthermore, the formalisation of digital platforms' content moderation obligations is linked to an increase in their opinion power (Helberger, 2020; Senftleben, 2024). However, the relatively low proportion of removed or blocked content in all NetzDG complaints supports the assumption that, to date, the extent of overblocking has tended to be overestimated (Kohl, 2022). Solid proof of over- or underblocking would require an in-depth and systematic legal review of notified content, including supposedly obviously illegal content, which is not practically feasible. Due to its systemic regula-

tory approach, there are no *direct* sanctions against under- or overblocking in the DSA itself. However, that said, the complaint and review procedures set out in the DSA could reduce the risks of the latter (Buiten et al, 2020; Cornils, 2020).

Apart from this, the independent audits to be conducted by VLOPs to ensure compliance with their obligations (Art. 37 DSA) should reduce the risk of over- or underblocking. In this context, it should also be examined whether the platform providers have carefully and objectively processed the notices received via the internal complaint-handling mechanisms. Furthermore, VLOPs must also explicitly consider the possible (negative) effects of content moderation on, among other things, freedom of expression and information when assessing systemic risks (Art. 34). However, it is up to the platforms themselves to define, assess, and address systemic risks (Griffin, 2023). Another critical point is that there are no minimum standards for conducting audits.

3.2 Involvement of state authorities

As far as the information provision obligations of platforms towards law enforcement or judicial authorities are concerned, consistent prosecution of illegal offences online is generally desirable. Otherwise, perpetrators are unlikely to change their minds (Kettemann, 2019). Failure to do so may give the impression of a lack of interest in enforcing norms, which in turn may lower the inhibition threshold for further hate speech (Rüdiger, 2019). Enforcement of legislation could and should also be enhanced by the establishment of additional prosecutors specialising in hate speech and related phenomena.

The authorisation of national authorities to order (EU-wide) action against allegedly illegal content, as provided for in the DSA, has the potential for instrumentalisation or abuse by state actors. For example, there could be boundary shifts regarding politically unpopular content and what can or cannot ultimately be removed by order. Limiting this risk of abuse, it should be noted that what is defined as illegal must accord with EU law (Art. 9 para. 1). More concerning is the risk that authoritarian governments outside the EU will use the measure in question to legitimise their own laws in the supposed fight against terrorism, extremism, fake news, or hate speech (Chang, 2018). For instance, Turkey, Russia, Belarus, and Malaysia have introduced legislation similar to the NetzDG, but with the aim of cen-

soring content critical of their regimes rather than protecting freedom of expression (Mchangama and Fiss, 2019; Reporters without Borders, 2017).

3.3 Effectiveness of content moderation

Regarding the suitability or effectiveness of co-regulatory content moderation measures in curbing hate speech, only little evidence has thus far been produced (Courchesne et al, 2021). Most studies relate to the NetzDG in Germany or "deplatforming", that is, the removal of one's account on social media for breaking platform rules. For example, Hestermann et al (2021) found a decline in hate comments between the study periods of January 2018 and July to November 2020, although this observation cannot be clearly attributed to the introduction of the NetzDG. Andres and Slivko (2021) conducted a quasi-experimental study on the effect of content moderation. They analysed Twitter posts published by followers of the populist and far-right parties AfD in Germany and FPÖ in Austria on the topics of religion and migration between July 2016 and June 2019. Their analysis of the automatically determined, multidimensional hate speech intensity of the tweets showed that the amount and intensity of hate speech decreased moderately among AfD followers after the NetzDG came into force in January 2018, but not among FPÖ supporters. This speaks in favour of the effectiveness of the NetzDG. Moreover, case studies on deplatforming show that blocking access to accounts, and thus to their content, can prevent the dissemination of hate speech (Ali et al, 2021; Bodden et al, 2023; Fielitz and Schwarz, 2020; Hammer et al, 2021). In this way, hate groups are deprived of the infrastructure to recruit and mobilise members, organise internally, disseminate their content, finance their activities, and harass minorities or dissenters (Rogers, 2020).

3.4 Data access

Access to data is fundamentally relevant to policy and research, not least to provide regulators with a broader, previously fragmented evidence base on the spread, impact, and containment of hate speech and other phenomena on social media, and the role of platform logics in this context. Previously, all major platforms have attempted to restrict or prevent data donation and

scraping. For example, in summer 2023, X sued the non-profit organisation Center for Countering Digital Hate, which had conducted research on the dissemination of hateful content on social media, accusing them of having "unlawfully" scraped data from X (X Corp. v. Center for Countering Digital Hate Inc., 2023). In autumn 2023, X ended free access to its API for researchers (Kupferschmidt, 2023). In August 2024, the CrowdTangle analytics tool was discontinued (Meta, 2024a). It allowed trending content to be detected, as well as how often a link was shared and who shared it. Meta's Content Library (Meta, 2024b) neither provides access to news media nor offers the same research functionalities as CrowdTangle (Coalition for Independent Technology Research, 2024). Other collaborations initiated by the platforms, such as Facebook's Social Science One Project or its Ad Library, have also been heavily criticised by researchers due to very limited access and incomplete data. As Meta's depreciation of CrowdTangle deprives researchers and journalists of real-time election monitoring tools, which could impair the ability to track misinformation and disinformation, the EC launched formal infringement proceedings against Meta in April 2024 (European Commission, 2024b).[8] The EC has also already opened formal investigative proceedings against X and TikTok due to shortcomings in giving researchers access to publicly accessible data. It is to be welcomed that the EC seems willing to enforce the DSA's data access regimes.[9]

However, there are still some open questions and points of criticism regarding the procedures and access modalities (for a more detailed analysis, see Seiling et al, 2024). For example, whether the application for vetted researcher status, once successful, must be resubmitted for each research project is still unclear. Likewise, the procedure for cross-platform analyses –

8 After initiating formal proceedings, the Commission carries out an in-depth investigation and gathers evidence, for example by sending additional requests for information, conducting monitoring actions, interviews, inspections and requesting access to algorithms. In addition, the Commission may take further enforcement steps. The DSA does not set a legal deadline for concluding formal proceedings, which depends on various factors, including the case's complexity and the company's cooperation.

9 In this context, however, the fact that the EU Commission is in charge of supervising VLOPs and VLOSEs poses a risk – in addition to the lack of state neutrality: As the executive body of the EU, it can be put under political pressure, meaning that platform regulation can become a geopolitical bargaining chip. This is already becoming apparent in the trade dispute between the EU and the US. During the election campaign, US Vice President J. D. Vance threatened the EU with making further support for Ukraine in the Russian war of aggression dependent on whether the Commission would discontinue the ongoing proceedings against X (Scheer et al,. 2025).

whether several separate applications for data access are to be submitted to the relevant DSC – has yet to be specified. Last but not least, the delegated act does not provide researchers with any clear remedy if the data received does not conform to quality standards.

4. Conclusion

4.1 Starting point and the DSA's approach

Online hate speech is a problem that affects millions of EU citizens and has negative consequences not only for individuals online and offline, but also for society as a whole. It does not only constitute an insult or group-related devaluation of people, but also suppresses their freedom of expression and can incite others to violence. Online hate speech on social media has reached problematic levels of visibility *despite* the moderation efforts of platform providers according to community standards (which sometimes go beyond legal definitions of criminal offences; Liesching, 2021, pp. 106–107), social media editorial teams, and existing national regulations (e.g., Germany's NetzDG). This suggests that platforms are not consistently tackling hate speech, implying that (further) external or co-regulatory measures are needed (Buiten et al, 2020) – or that a significant proportion of hate speech is not considered unlawful or perceived as violating the platforms' community standards. The extent of (at least not illegal) hate speech is likely to increase in the future now that Facebook has ended its cooperation with fact checkers and reduced community standards (Stippler et al., 2025). This has already been demonstrated on X (Hickey et al., 2023; Arun et al., 2024).

Against this background, the DSA is an important legislative project in the EU to strengthen incentives to curb hate speech and impose standardised and binding complaint, deletion, objection, reporting, and data access obligations on digital platforms. As described earlier, the EC has already launched several formal investigative proceedings against VLOPs. For example, in December 2023, it announced formal infringement proceedings against X on the basis of suspected breaches in its data access obligations, failure to counter the dissemination of illegal content, and deceptive design practices (European Commission, 2023b). In January 2024, the EC sent formal requests to 17 VLOPs and VLOSEs to provide more information on the measures they have taken to comply with the obligation

to provide researcher access to publicly available data (European Commission, 2024c). In February, two days after full DSA implementation, the EC announced similar proceedings against TikTok for potential breaches in protecting minors against the platform's potentially "addictive design", advertising transparency, and data access for researchers (European Commission, 2024d). However, the DSA is no *constitution for the internet* (see above), as its amendments are too incremental. The DSA establishes no specific standards for dealing with hate speech (or disinformation or illegal content). Rather, the aim is to formalise and standardise previously self-regulatory content moderation processes and the associated legitimate interests and considerations. It helps to increase the accountability of platforms and empower a critical public through regular transparency reports, risk and countermeasure assessments, independent audits and reports on moderation decisions, obligations to provide reasons, and opportunities for objection (Buchheim, 2022).

In order to defend the freedom of expression that hate speech threatens, the DSA relies on cooperation between users, notice centres, and other trusted flaggers, authorities, and platforms. These actors are involved in different phases of hate-speech management, from identifying and moderating hate speech to sanctioning hate speech disseminators and structurally adapting platforms. This distributes the responsibility for a discourse arena free from hate speech across several shoulders instead of shifting it unilaterally (e.g., in the form of general monitoring) to individual actors while simultaneously exempting others (Bryson, 2023; Buiten et al, 2020; Griffin, 2023). The DSA is concerned with procedural improvements (of reporting and objection options, transparency, and compliance) and leaves the definition of illegal content to Member States themselves. To this end, the DSA performs a balancing act between effective (rigorous deletion by platforms) and legitimate (involvement of users) content moderation. For example, the DSA includes complaint mechanisms and a certified out-of-court dispute settlement body that allow users to challenge the content moderation decisions of digital platforms. In this context, it is irrelevant whether the moderation decision was taken proactively by the platform or was triggered by a user's notice. It would be useful to extend these mechanisms to cover not only the decision by a platform to *remove*, but also the decision to *retain* notified content. Moreover, the DSA also contains comprehensive reporting obligations. For example, intermediary services and online platforms must document whether they have made moderation decisions on a legal basis or

as per their own terms and conditions. Moreover, VLOPs have to disclose the results of first- and second-party audits.

4.2 Risks and opportunities in relation to the DSA

Of course, the implementation of the DSA is not without risk: the Act formalises the fact that it is the hosting service providers and online platforms that decide in the *first instance* what content is illegal. While independent state courts will, naturally, continue to make final decisions on the legality of content, taking legal action is unlikely to be attractive for the majority of users, meaning that they will often accept the provider's decision, and thus the initial decision will effectively be the final decision (Raue, 2023, p. 345). This leads to the criticism that due diligence obligations would turn platforms into "quasi-judges" (Spindler, 2017, p. 481; Berberich, 2023, p. 173). This does not mean that private companies are not allowed to do so. Rather, it is the lack of transparency in content moderation that is problematic (Heldt, 2019). The inability of independent third parties to scrutinise the moderation decisions of platforms means that the possibility of overblocking cannot be excluded. Already marginalised groups (e.g., sex workers and abortion rights activists) are particularly vulnerable to overblocking (Appelman, 2023; Haimson et al, 2021). At this point, insight into the specific community standards and access to data for independent research institutions is crucial for identifying and evaluating any systematic over- or underblocking. To date, the content moderation measures of social media platforms according to their own community standards have not been transparent. However, it is important to determine where, and on what basis, the red line for hate speech is drawn, as the accuracy and precision of content moderation measures have implications for effective freedom of expression. Encouragingly, the research data access regime prescribed by the DSA (Art. 40) should allow for analyses on the precision of (automated) content moderation measures taken by, and other systemic risks associated with, platforms.

4.3 Implications

In this context, data access should be free of charge and the data should be easily accessible and findable, machine-readable, able to be structured

(e.g., by outlet), interoperable, and replicable. Metrics should be easy to understand (Democracy Reporting International, 2024; Ranaivoson and Domazetovikj, 2023; Specht-Riemenschneider, 2021). Data preparation should meet uniform, comparable standards, and data pools should be accessible in their entirety (Klinger and Ohme, 2023).

Moreover, data access regimes should be adapted to the (dynamic) needs of researchers (Van Drunen and Noroozian, 2024). On this basis, there is a need for cross-platform, continuous studies focusing on: 1) the reach and frequency of exposure to different degrees of hate speech, as well as their origins and evolution; 2) the differentiated effects of different degrees of hate speech at the individual and societal levels; 3) algorithmically induced radicalisation effects; and 4) the principles and accuracy of content moderation measures to curb hate speech. This requires a standardised conceptualisation of hate speech to ensure comparability of the study results. More fundamentally, social science is faced with the question of how to deal with the temptations of data access. Is it part of its role and mission to take on service tasks in return for data access and to carry out a kind of "third-party audit" (Meßmer and Degeling, 2023)? The attractiveness of data access for researchers could lead to research activities concentrating on the conclusively defined systemic risks arising from the design, functioning, use, or misuse of VLOPs and VLOSEs, with the result that other issues may be neglected.

Although Recital 5 of the DSA addresses the problem of the "intermediation and spread of unlawful or otherwise *harmful* information and activities", it is important to emphasise that legal regulation is limited to *illegal* content and should therefore not (and this cannot be ruled out) target legal hate speech, incivility, or a negative quality of discourse (Cornils, 2020). This means that hate speech must be countered in a differentiated way, depending on its intensity. Clearly illegal hate speech that is directly and immediately harmful (e.g., by inciting violence) should be removed by the platforms as quickly as possible in order to avoid contagion effects on third parties. Civil society actors or platform providers are called upon to address issues of discourse quality. Non-profit initiatives (e.g., having funding stabilised) should be strengthened in their commitment to more discursive diversity or the protection of the personal rights of those affected by hate speech (de Streel et al, 2020).

Platform providers, in turn, could label problematic, but not illegal, hate speech (e.g., negative stereotyping) as such, as they often already do in connection with disinformation. On the one hand, labelling hate speech can

make those affected feel less isolated and that the views expressed form a minority position. On the other, it can strengthen the enforcement of social norms and more civil communication behaviour among observers of hate speech (Blackwell et al, 2017; Katsaros et al, 2021). Moreover, warnings or other interventions can (quite successfully) encourage users to think twice before sharing problematic content (Katsaros et al, 2021), thus mitigating impulsive reactions encouraged by platform logics. In addition, platforms could be required (at least by opt-in) not to measure the relevance of user-generated content based on affective interactions (Tucker et al, 2018). Instead, algorithmic logics could be guided by such values as rationality, civility, and diversity (Friess and Eilders, 2015). The DSA already stipulates that VLOPs and VLOSEs must provide their users with a recommender system which is not based on profiling (Art. 38). However, the definition and operationalisation of such values is challenging, volatile, and has already been criticised for being paternalistic. Similarly, it is challenging to distinguish between occasionally subtle illegal hate speech and legally permissible but harmful speech when dealing with large amounts of content. The context, tone, and intent of speech are all significant here. At the same time, it must be made clear that content moderation only takes effect after hate speech has already been produced. It does not address the underlying causes of hate speech, such as radicalisation, which often stems from perceived injustice, the formation of an outwardly delineated group identity, or the propagation of ideologies in closed groups and offline networks. Such a sense of injustice can be reinforced by one-sided information (van den Bos, 2020). It is also unlikely that removing or blocking illegal hate speech will change the attitudes of those who create and disseminate it in the first place. As the EC itself stated in the context of the Code of Conduct on countering illegal hate speech online, notice and action procedures and the removal of content can only help address the symptoms (European Commission, 2020c).

Last but not least, it is not possible to draw direct conclusions about the individual impact of hate speech from its prevalence in social networks. In between are the individual visibility of hate speech in social network feeds, the prerequisite of having to recognise hate speech, different attitudes, experiences, processing strategies, and other intervening variables. The same is true for the effectiveness of removing or countering hate speech. Researchers and policy-makers should also consider the extent to which the development of perceived and content-analytically measured hate speech and the registered offences in this context can be explained by the fact that:

a) hate speech is an inconsistently defined and operationalised term; b) the intensity of use of digital platforms is increasing; c) the use of certain terms and public discourses are becoming more or less taboo, and levels of awareness and understanding of hate speech are changing; d) criminal law enforcement is intensifying; and e) measurement methods are becoming more accurate. This article provides some food for thought on how some of these issues could be effectively handled. In order to provide reliable answers to questions such as these, legal and communication sciences should more closely combine their different strengths and collaborate more intensively in future.

Acknowledgements

The authors would like to thank two anonymous reviewers, Rita Gsenger and Marie-Therese Sekwenz for their valuable feedback throughout the revision and publication process.

References

Adelberg, P. (2022) 'Hassrede in sozialen Netzwerken – Reichweite und Grenzen der Pflichten und Rechte der Netzwerkbetreiber', *Kommunikation & Recht*, 25(1), pp. 19–25.

Albert, J. (2024). *Researcher access to platform data: Experts weigh in on the Delegated Act* [Online]. DSA Observatory. Available at: https://dsa-observatory.eu/2024/11/29/researcher-access-to-platform-data-experts-weigh-in-on-the-delegated-act/ (Accessed: 2 January 2025).

Ali, S., Saeed, M.H., Aldreabi, E., Blackburn, J., De Cristofaro, E., Zannettou, S. and Stringhini, G. (2021) 'Understanding the effect of deplatforming on social networks', *13th ACM Web Science Conference 2021*, pp. 187–195.

Andres, R. and Slivko, O. (2021) *Combating online hate speech: the impact of legislation on Twitter* [Discussion Paper]. Leibniz-Zentrum für Europäische Wirtschaftsforschung. [Online]. Available at: https://ftp.zew.de/pub/zew-docs/dp/dp21103.pdf (Accessed: 21 January 2025).

Appelman, N. (2023) *Disparate content moderation: mapping social justice organisations perspectives on unequal content moderation harms and the EU platform policy*. Institute for Information Law, University of Amsterdam [Online]. Available at: https://dsa-observatory.eu/2023/10/31/research-report-on-disparate-content-moderation/ (Accessed: 30 December 2024).

Arun, A., Chhatani, S., An, J., & Kumaraguru, P. (2024). X-posing Free Speech: Examining the Impact of Moderation Relaxation on Online Social Networks. *Proceedings of the 8th Workshop on Online Abuse and Harms (WOAH 2024)*, 201–211. https://doi.org/10.18653/v1/2024.woah-1.15

Banks, J. (2010) 'Regulating hate speech online', *International Review of Law, Computers & Technology*, 24(3), pp. 233–239.

Bayer, J. and Bárd, P. (2020) *Hate speech and hate crime in the EU and the evaluation of online content regulation approaches* [Online]. Policy Department for Citizens' Rights and Constitutional Affairs. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/655135/IPOL_STU(2020)655135_EN.pdf (Accessed: 21 January 2025).

Berberich, M. (2023) '§ 5 Sorgfaltspflichten, Moderationsverfahren und prozedurale Fairness' in Steinrötter, B. (ed.) *Europäische Plattformregulierung*. Nomos, pp. 126–174.

Berry, J.M. and Sobieraj, S. (2016) *The outrage industry: political opinion media and the new incivility*. Reprint ed. New York: Oxford University Press.

Blackwell, L., Dimond, J., Schoenebeck, S. and Lampe, C. (2017) 'Classification and its consequences for online harassment: design insights from HeartMob', *Proceedings of the ACM on Human-Computer Interaction*, *1*(CSCW), pp. 1–19.

Bodden, N., Holec, H.A., Hoß, B., Ziegele, M. and Wilms, L. K. (2023) 'Vom Netz genommen. Die Auswirkungen von Deplatforming auf die Online-Kommunikation der extremen Rechten auf Telegram am Beispiel der Identitären Bewegung', *Medien & Kommunikationswissenschaft*, 71(3–4), pp. 266–284. Available at: https://doi.org/10.5771/1615-634X-2023-3-4-266.

Brauneck, J. (2024) 'Das Verantwortungsbewusstsein der Plattformbetreiber im Digital Services Act', *Neue Zeitschrift für Verwaltungsrecht*, 43(6), pp. 377–384.

Brugger, W. (2003) 'The treatment of hate speech in German constitutional law (Part I)', *German Law Journal*, 4(1), pp. 1–22.

Bryson, J.J. (2023) 'Human experience and AI regulation: what European Union law brings to digital technology ethics', *Weizenbaum Journal of the Digital Society*, 3(3). Available at: https://doi.org/10.34669/WI.WJDS/3.3.8.

Buchheim, J. (2022) 'Der Kommissionsentwurf eines Digital Services Act – Regelungsinhalte, Regelungsansatz, Leerstellen und Konfliktpotential' in Spiecker, I.,

Buiten, M., Streel, A. and Peitz, M. (2020) 'Rethinking liability rules for online hosting platforms', *International Journal of Law and Information Technology*, 28, pp.139–166.

Cauffman, C. and Goanta, C. (2021) 'A new order: the Digital Services Act and consumer protection', *European Journal of Risk Regulation*, 12(4), pp. 758–774.

Chang, B. (2018) 'From Internet Referral Units to international agreements: censorship of the internet by the UK and EU', *Columbia Human Rights Law Review*, 49(2), pp. 114–212.

Cioffi, J.W., Kenney, M.F. and Zysman, J. (2022) 'Platform Power and Regulatory Politics: Polanyi for the Twenty-First Century' *New Political Economy*, 27(5), pp. 820–36.

'Charter of the Fundamental Rights of the Euroepan Union (2000/C 364/01)' (2000) *Official Journal of the European Communities* C 364/1, 18 December [Online]. Available at: https://www.europarl.europa.eu/charter/pdf/text_en.pdf (Accessed: 20 January 2025).

Coalition for Independent Technology Research (2024) *Blocking our right to know: surveying the impact of Meta's CrowdTangle shutdown* [Online]. Available at: https://independenttechresearch.org/wp-content/uploads/2024/07/CrowdTangle-Survey-Report-Final.pdf (Accessed: 20 January 2025).

Cohen-Almagor, R. (2011) 'Fighting hate and bigotry on the internet', *Policy & Internet*, 3(3), pp. 1–26.

Cole, M. D., Ukrow, J. and Etteldorf, C. (2020) *Zur Kompetenzverteilung zwischen der Europäischen Union und den Mitgliedstaaten im Mediensektor Eine Untersuchung unter besonderer Berücksichtigung medienvielfaltsbezogener Maßnahmen* [Online]. Institut für Europäisches Medienrecht. Available at: https://www.rlp.de/fileadmin/rlp-stk/pdf-Dateien/Medienpolitik/EMR_Gutachten_Zur_Kompetenzverteilung_im_Mediensektor.pdf (Accessed: 20 January 2025).

'COMMISSION RECOMMENDATION (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online', *Official Journal* L 63, 6 April. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018H0334 (Accessed 19 January 2025).

Cooper, H. (2018). 'Angela Merkel signals potential changes to online hate speech law', *Politico* 03 February [online]. Available at: https://www.politico.eu/article/angela-merkel-signals-potential-changes-to-germany-online-hate-speech-law/ (Accessed: 19 January 2025).

Cornils, M. (2020) *Designing platform governance: A normative perspective on needs, strategies, and tools to regulate intermediaries* [Online]. AlgorithmWatch. Available at: https://algorithmwatch.org/de/wp-content/uploads/2020/05/Governing-Platforms-legal-study-Cornils-May-2020-AlgorithmWatch.pdf (Accessed: 20 January 2025).

Courchesne, L., Ilhardt, J. and Shapiro, J. N. (2021) 'Review of social science research on the impact of countermeasures against influence operations', *Harvard Kennedy School Misinformation Review*, 13 September [Online]. Available at: https://doi.org/10.37016/mr-2020-79 (Accessed: 20 January 2025).

Das NETTZ, Gesellschaft für Medienpädagogik und Kommunikationskultur, HateAid and Neue deutsche Medienmacher*innen (eds.) (2024) *Lauter Hass - leiser Rückzug: Wie Hass im Netz den demokratischen Diskurs bedroht* [Online]. Kompetenznetzwerk Hass im Netz. Available at: https://kompetenznetzwerk-hass-im-netz.de/wp-content/uploads/2024/02/Studie_Lauter-Hass-leiser-Rueckzug.pdf (Accessed: 20 January 2025).

'Delegated Regulation (EU) 2024/436 of 20 October 2023 supplementing Regulation (EU) 2022/2065 of the European Parliament and of the Council, by laying down rules on the performance of audits for very large online platforms and very large online search engines' (2024), *Official Journal* L [Online]. Available at: http://data.europa.eu/eli/reg_del/2024/436/oj (Accessed: 21 January 2025).

Democracy Reporting International (2024) *Access granted: why the European Commission should issue guidance on access to publicly available data now* [Online]. 9 September. Available at: http://democracy-reporting.org/en/office/global/publications/access-granted-why-the-european-commission-should-issue-guidance-on-access-to-publicly-available-data-now (Accessed: 30 December 2024).

De Streel, A., Defreyne, E., Jacquemin, H., Ledger, M., Michel, A., Innesti, A., Goubet, M. and Ustowski, D. (2020) *Online platforms' moderation of illegal content online. Law, practices and options for reform* [Online, study requested by the IMCO committee]. Policy Department for Economic, Scientific and Quality of Life Policies. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2020/652718/IPOL_STU(2020)652718_EN.pdf (Accessed: 20 January 2025).

'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')' (2000) *Official Journal* L 178, 17 July, pp. 1–16. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed: 19 January 2025).

'Directive (EU) 2010/13/EU of the European Parliament and of the Council of 10 March 2010 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive)' (2010) *Official Journal* L 303, 15 April, p. 69-92. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32010L0013.

Döhmann, G., Westland, M. and Campos, R. (eds.) *Demokratie und Öffentlichkeit im 21. Jahrhundert – zur Macht des Digitalen*. Baden-Baden: Nomos Verlagsgesellschaft mbH & Co. KG, pp. 249–272.

Duffy, B. E. and Meisner, C. (2023) 'Platform governance at the margins: Social media creators' experiences with algorithmic (in)visibility', *Media, Culture & Society*, 45(2), pp. 285–304.

EPP Group. (2021) *Social media cannot be a lawless place* [Online]. Available at: https://www.eppgroup.eu/newsroom/social-media-cannot-be-a-lawless-place (Accessed: 17 January 2025).

Erjavec, K. and Kovačič, M. P. (2012) '"You don't understand, this is a new war!" Analysis of hate speech in news web sites' comments', *Mass Communication and Society*, 15(6), pp. 899–920 [Online]. Available at: https://doi.org/10.1080/15205436.2011.619679 (Accessed 19 January 2025).

European Commission (2014a) REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL on the implementation of Council Framework Decision 2008/913/JHA on combating certain forms and expressions of racism and xenophobia by means of criminal law /* COM/2014/027 final */ [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52014DC0027 (Accessed: 19 January 2025).

European Commission (2016) Code of Conduct on Countering illegal hate speech online [Online]. Available at: https://commission.europa.eu/strategy-and-policy/policies/justice-and-fundamental-rights/combatting-discrimination/racism-and-xenophobia/eu-code-conduct-countering-illegal-hate-speech-online_en (Accessed: 19 January 2025).

European Commission (2020a) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on contestable and fair markets in the digital sector (Digital Markets Act) COM/2020/842 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A842%3AFIN (Accessed: 19 January 2025).

European Commission (2020b) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on a Single Market For Digital Services (Digital Services Act) and amending Directive 2000/31/EC COM/2020/825 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=COM%3A2020%3A825%3AFIN (Accessed: 20 January 2025).

European Commission (2020c) The Code of conduct on countering illegal hate speech online [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/qanda_20_1135 / (Accessed: 19 January 2025).

European Commission (2021) C*ommunication from the Commission to the European Parliament and the Council. A more inclusive and protective Europe: Extending the list of EU crimes to hate speech and hate crime* [Online]. Available at: https://commission.europa.eu/document/download/926b3cb2-f027-40b6-ac7b-2c198a164c94_en?filename=COM_2024_146_1_EN.pdf (Accessed: 20 January 2025).

European Commission (2023a) *Application of the risk management framework to Russian disinformation campaigns* [Online]. Publications Office of the European Union. Available at: https://data.europa.eu/doi/10.2759/764631 (Accessed: 20 January 2025).

European Commission (2023b) *Commission opens formal proceedings against X under the Digital Services Act* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_6709 (Accessed: 21 January 2025).

European Commission (2024b) *Commission opens formal proceedings against Facebook and Instagram under the Digital Services Act* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_2373 (Accessed: 21 January 2025).

European Commission (2024c) *Commission sends requests for information to 17 Very Large Online Platforms and Search Engines under the Digital Services Act* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/news/commission-sends-requests-information-17-very-large-online-platforms-and-search-engines-under (Accessed: 21 January 2025).

European Commission (2024d) *Commission opens formal proceedings against TikTok under the Digital Services Act* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926 (Accessed: 21 January 2025).

European Commission (2025a) *CODE OF CONDUCT ON COUNTERING ILLEGAL HATE SPEECH ONLINE +* [Online]. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/111777 (Accessed: 18 March 2025).

European Commission (2025b) *Supervision of the designated very large online platforms and search engines under DSA* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (Accessed: 18 March 2025).

European Commission (2025c) *The Code of conduct on countering illegal hate speech online +* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/code-conduct-countering-illegal-hate-speech-online (Accessed: 18 March 2025).

European Parliament (2024) *Briefing. Hate speech and hate crime must become crimes under EU law* [Online]. Available at: https://www.europarl.europa.eu/news/en/agenda/briefing/2024-01-15/11/hate-speech-and-hate-crime-must-become-crimes-under-eu-law (Accessed: 21 January 2023).

Fielitz, M. and Marcks, H. (2019) *Digital fascism: challenges for the open society in times of social media* [Online]. Berkeley Center for Right-Wing Studies Working Paper Series. Berkeley. Available at: https://escholarship.org/uc/item/87w5c5gp (Accessed: 20 January 2025).

Fielitz, M. and Schwarz, K. (2020) *Hate not found?! Das Deplatforming der extremen Rechten und seine Folgen* [Online]. Institut für Demokratie und Zivilgesellschaft. Available at: https://www.idz-jena.de/fileadmin//user_upload/Hate_not_found/WEB_IDZ_FB_Hate_not_Found.pdf (Accessed: 20 January 2025).

Flew, T., Martin, F. and Suzor, N. (2019) 'Internet regulation as media policy: rethinking the question of digital communication platform governance', *Journal of Digital Media & Policy*, 10(1), pp. 33–50.

'Framework Decision 2008/913/JHA of 28 November 2008 on combating certain forms and expressions of racism and xenophobia by means of criminal law' (2008) *Official Journal* L 328/55, 6 December [Online]. Available at: https://db.eurocrim.org/db/en/doc/1044.pdf (Accessed: 19 January 2025).

Friess, D. and Eilders, C. (2015) 'A Systematic Review of Online Deliberation Research' *Policy & Internet*, 7, pp. 319-339.

Fuchs, C. (2022) *Digital fascism*. Abingdon: Routledge.

Geese, A. (2022) *Europe Calling "DSA Deal: A constitution for the internet!"* [Online video]. 29 April. Available at: https://en.alexandrageese.eu/video/europe-calling-dsa-deal/ (Accessed: 19 January 2025).

Gelber, K. and McNamara, L. (2016) 'Evidencing the harms of hate speech', *Social Identities*, 22(3), pp. 324–341.

Gerdemann, S. and Spindler, G. (2023) 'Das Gesetz über digitale Dienste (Digital Services Act) (Teil 1)', *Gewerblicher Rechtsschutz und Urheberrecht*, 125(1–2), pp. 3–11.

'Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)' *BGBl.* I 2017, p. 3351 [Online]. Available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html (Accessed on: 20 January 2025).

Google and Youtube (2019) *Stellungnahme im Rahmen der öffentlichen Anhörung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestages 15. Mai 2019* [Online]. Available at: https://kripoz.de/wp-content/uploads/2019/05/stellungnahme-frank-netzdg.pdf (Accessed on: 21 January 2025).

Gorwa, R., Binns, R. and Katzenbach, C. (2020) 'Algorithmic content moderation: technical and political challenges in the automation of platform governance', *Big Data & Society*, 7(1) [Online]. Available at: https://doi.org/10.1177/2053951719897945 (Accessed: 20 January 2025).

Griffin, R. (2023) 'The law and political economy of online visibility. Technology and regulation', *Technology and Regulation*, pp. 69–79.

Haimson, O. L., Delmonaco, D., Nie, P. and Wegner, A. (2021) 'Disproportionate removals and differing content moderation experiences for conservative, transgender, and black social media users: marginalization and moderation gray areas', *Proceedings of the ACM on Human-Computer Interaction*, 5(CSCW2), 466, pp. 1–35.

Hammer, D., Matlach, P., Gerster, L. and Baaken, T. (2021) *Fluchtwege. Wie das Netzwerkdurchsetzungsgesetz auf etablierten sozialen Medien durch die Verlinkung zu alternativen Plattformen umgangen wird* [Online]. Institute for Strategic Dialogue. Available at: https://www.isdglobal.org/wp-content/uploads/2021/08/Fluchtwege_050821_V4.pdf (Accessed: 20 January 2025).

Helberger, N. (2020) 'The political power of platforms: how current attempts to regulate misinformation amplify opinion power', *Digital Journalism*, 8(6), pp. 842–854.

Heldt, A. (2019) 'Let's meet halfway: sharing new responsibilities in a digital age,' *Journal of Information Policy*, 9, pp. 336–369.

Hestermann, T., Hoven, E. and Autenrieth, M. (2021) '"Eine Bombe, und alles ist wieder in Ordnung": Eine Analyse von Hasskommentaren auf den Facebook-Seiten reichweitenstarker deutscher Medien', *Kriminalpolitische Zeitschrift*, 4, pp. 204–214.

Hickey, D., Schmitz, M., Fessler, D., Smaldino, P. E., Muric, G., & Burghardt, K. (2023). Auditing Elon Musk's Impact on Hate Speech and Bots. *Proceedings of the International AAAI Conference on Web and Social Media*, *17*, 1133–1137. https://doi.org/10.1609/icwsm.v17i1.22222

Hofmann, F. (2023a) 'Vor Art. 4 ff' in Hofmann, F. and Raue, B. (eds.) *Digital Services Act*. Baden-Baden: Nomos, pp. 111–139.

Hofmann, F. (2023b) 'Art. 7 Freiwillige Untersuchungen auf Eigeninitiative und Einhaltung der Rechtsvorschriften' in Hofmann, F. and Raue, B. (eds.) *Digital Services Act*. Baden-Baden: Nomos, pp. 175–183.

Hofmann, F. (2023c) 'Art. 8 Keine allgemeine Verpflichtung zur Überwachung oder aktiven Nachforschung' in. Hofmann, F. and Raue, B. (eds.) *Digital Services Act*. Baden-Baden: Nomos, pp. 183–191.

Hofmann, F. (2023d) 'Art. 9 Anordnungen zum Vorgehen gegen rechtswidrige Inhalte' in Hofmann, F. and Raue, B. (eds.) *Digital Services Act*. Baden-Baden: Nomos, pp. 191–206.

Hofmann, F. and Raue, B. (2023) 'Einleitung' in Hofmann, F. and Raue, B. (eds.) *Digital Services Act*. Baden-Baden: Nomos, pp. 31–48.

Holznagel, D. (2021) 'Chapter II des Vorschlags der EU-Kommission für einen Digital Services Act—Versteckte Weichenstellungen und ausstehende Reparaturen bei den Regelungen zu Privilegierung, Haftung & Herkunftslandprinzip für Provider und Online-Plattformen', *Computer und Recht*, 37(2), pp. 123–132.

Hong, M. (2022) 'Regulating hate speech and disinformation online while protecting freedom of speech as an equal and positive right – comparing Germany, Europe and the United States', *Journal of Media Law*, 14(1), pp. 76–96.

Jaursch, J. (2021) *Der DSA-Entwurf: Ehrgeizige Regeln, schwache Durchsetzungsmechanismen. Warum eine europäische Plattformaufsicht sinnvoll ist* [Online]. Stiftung Neue Verantwortung. Available at: https://www.stiftung-nv.de/sites/default/files/snv_dsa-aufsicht.pdf (Accessed: 20 January 2025).

Jaursch, J. and Lorenz-Spreen, P. (2024) *Researcher access to platform data under the DSA: questions and answers* [Online]. Available at: https://reclaimingautonomyonline.notion.site/Researcher-access-to-platform-data-under-the-DSA-Questions-and-answers-8f7390f3ae6b4aa7ad53d53158ed257c (Accessed: 30 December 2024).

Kalbhenn, J. C. and Hemmert-Halswick, M. (2021) 'EU-weite Vorgaben für die Content-Moderation in sozialen Netzwerken Kommentar zu dem Entwurf der Europäischen Kommission zu einem Digital Services Act', *Zeitschrift für Urheber- und Medienrecht*, 3, pp. 184–194.

Kapusta, I. (2024) 'Plattformregulierung 2.0: Die (un-)mittelbare Grundrechtsbindung Privater im Digital Services Act', in Laimer, S., Mittwoch, A.-C., Müller, T. and Staffler, L. (eds.) *Daten, Plattfomen, Smart Contracts*. Baden-Baden: Nomos, pp. 271–327.

Katsaros, M., Kim, J. and Tyler, T. (2024) 'Online Content Moderation: Does Justice Need a Human Face?' *International Journal of Human–Computer Interaction*, 40 (1), pp. 66–77.

Keipi, T., Näsi, M., Oksanen, A. and Räsänen, P. (2017*) Online hate and harmful content: cross-national perspectives*. Abingdon: Routledge.

Kettemann, M. C. (2019) *Stellungnahme als Sachverständiger für die öffentliche Anhörung zum Netzwerkdurchsetzungsgesetz auf Einladung des Ausschusses für Recht und Verbraucherschutz des Deutschen Bundestags* [Online]. Leibniz-Institut für Medienforschung| Hans-Bredow-Institut. Available at: https://kripoz.de/wp-content/uploads/2019/05/stellungnahme-kettemann-netzdg.pdf (Accessed: 19 January 2025).

King, G. and Persily, N. (2019) A new model for industry-academic partnerships. *PS: Political Science and Politics*, 53(4), pp. 703–709.

Klinger, U. and Ohme, J. (2023) *What the scientific community needs from data access under Art. 40 DSA: 20 points on infrastructures, participation, transparency, and funding* [Online]. Available at: https://doi.org/10.34669/WI.WPP/8.2 (Accessed: 19 January 2025).

Klonick, K. (2018) The new governors: the people, rules, and processes governing online speech. *Harvard Law Review*, 131, pp. 1598–1670.

Koehler, M. (2024) 'Artikel 7 Freiwillige Untersuchungen' in Mueller-Terpitz, R. and Koehler, M. (eds.) *Digital Services Act*. München: C.H. Beck, pp. 106–118.

Kommunikationsplattformen-Gesetz, BGBl. I Nr. 151/2020 [Online]. Available at: https://www.ris.bka.gv.at/eli/bgbl/I/2020/151/20201223 (Accessed: 19 January 2025).

Kohl, U. (2022) 'Platform regulation of hate speech – a transatlantic speech compromise?' *Journal of Media Law*, 14(1), pp. 25-49.

Koreng, A. (2017) 'Hate-Speech im Internet: Eine rechtliche Annäherung', *Kriminalpolitische Zeitschrift*, 3, pp. 151–159.

Kuczerawy, A. (2021) 'The good Samaritan that wasn't: voluntary monitoring under the (draft) Digital Services Act', *Verfassungsblog*, 12 January [Online]. Available at: https://verfassungsblog.de/good-samaritan-dsa/ (Accessed: 30 December 2024).

Kupferschmidt, K. (2023) 'Twitter's plan to cut off free data access evokes 'fair amount of panic' among scientists', *Science*, 8 February [Online]. Available at: https://www.science.org/content/article/twitters-plan-cut-free-data-access-evokes-fair-amount-panic-among-scientists (Accessed: 19 January 2025).

Landesanstalt für Medien NRW (2023) *Hate Speech. Forsa-Studie 2023. Zentrale Untersuchungsergebnisse* [Online]. Available at: https://www.medienanstalt-nrw.de/fileadmin/user_upload/NeueWebsite_0120/Themen/Hass/forsa_LFMNRW_Hassrede2023_Praesentation.pdf (Accessed: 20 January 2025).

Latzer, M., Saurwein, F. and Just, N. (2019) ‚Assessing Policy II: Governance-Choice Method' in Van Den Bulck, H., Puppis, M., Donders, K. and Van Audenhove, L. (eds.) *The Palgrave Handbook of Methods for Media Policy Research*. Cham: Springer International Publishing, pp. 557-574.

Legner, S. (2024) 'Der Digital Services Act - Ein neuer Grundstein der Digitalregulierung', *Zeitschrift für Urheber- und Medienrecht*, 68(2), pp. 99–111.

Lee-Won, R.J., White, T.N., Song, H., Lee, J.Y. and Smith, M.R. (2020) 'Source magnification of cyberhate: affective and cognitive effects of multiple-source hate messages on target group members', *Media Psychology*, 23(5), pp. 603–624.

Liesching, M. (2021) *Das NetzDG in der praktischen Anwendung: Eine Teilevaluation des Netzwerkdurchsetzungsgesetzes*. Carl Grossmann [Online]. Available at: https://doi.org/10.24921/2021.94115953 (Accessed: 20 January 2025).

LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (1). Journal Officiel de la République Française n°0156, p.11, 25 June [Online]. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970 (Accessed: 19 January 2025).

Mchangama, J. and Fiss, J. (2019) *The digital Berlin Wall: how Germany (accidentally) created a prototype for global online censorship* [Online]. Justitia. Available at: http://justitia-int.org/wp-content/uploads/2019/11/Analyse_The-Digital-Berlin-Wall-How-Germany-Accidentally-Created-a-Prototype-for-Global-Online-Censorship.pdf (Accessed: 20 January 2025).

Meßmer, A.-K. and Degeling, M. (2023) *Auditing recommender systems* [Online]. Stiftung Neue Verantwortung. Available at: https://www.stiftung-nv.de/de/publication/auditing-recommender-systems (Accessed: 30 December 2024).

Meta (2024a) *CrowdTangle*. [Online]. Available at: https://transparency.meta.com/de-de/researchtools/other-datasets/crowdtangle/ (Accessed: 30 December 2024).

Meta (2024b) *Meta Content Library and API* [Online]. Available at: https://transparency.meta.com/en-gb/researchtools/meta-content-library/ (Accessed: 21 January 2025).

Müller, K. and Schwarz, C. (2021) 'Fanning the flames of hate: social media and hate crime', *Journal of the European Economic Association*, 19(4), pp. 2131–2167.

Newman, N. (2023) 'Executive summary and key findings' in Newman, N., Fletcher, R., Eddy, K., Robertson, C.T. and Nielsen, R.K. (eds.) *Reuters Institute Digital News Report 2023*. Oxford: Reuters Institute for the Study of Journalism, pp. 9–29.

Paasch-Colberg, S., Trebbe, J., Strippel, C. and Emmer, M. (2022) 'Insults, criminalisation, and calls for violence: forms of hate speech and offensive language in German user comments on immigration', in Monnier, A., Boursier, A. and Seoane, A. (eds.) *Cyberhate in the Context of Migrations*. Cham: Springer International Publishing, pp. 137–163.

Pohlmann, J., Barbaresi, A. and Leinen, P. (2023) 'Platform regulation and "overblocking" – the NetzDG discourse in Germany', *Communications*, 48(3), pp. 395–419.

Price, L. (2021) 'Platform responsibility for online harms: towards a duty of care for online hazards', *Journal of Media Law*, 13(2), pp. 238–261.

Ranaivoson, H. and Domazetovikj, N. (2023) 'Platforms and exposure diversity: towards a framework to assess policies to promote exposure diversity', *Media and Communication*, 11(2), pp. 379-391.

Raue, B. (2023a) 'Art. 16 Melde- und Abhilfeverfahren' in Hofmann, F. and Raue, B. (eds.) *Digital Services Act*. Baden-Baden: Nomos, pp. 285–313.

Raue, B. (2023b) 'Art. 20 Internes Beschwerdemanangementsystem' in Hofmann, F. and Raue, B. (eds.) *Digital Services Act*. Baden-Baden: Nomos, pp. 341–360.

Recuero, R. (2024) 'The platformization of violence: toward a concept of discursive toxicity on social media', *Social Media + Society*, 10(1), [Online]. Available at: https://doi.org/10.1177/20563051231224264 (Accessed: 20 January 2025).

'Regulation (EU) 2021/784 of the European Parliament and of the Council of 29 April 2021 on addressing the dissemination of terrorist content online' (2021) Official Journal L172/79, 17 May, [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX%3A32021R0784 (Accessed: 21 January 2025).

'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)' (2022) *Official Journal* L 265, 12 October, pp. 1-66 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R1925 (Accessed: 19 January 2025).

'Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act)' (2022) *Official Journal* L 277, 27 October, pp. 1-102. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32022R2065 (Accessed: 19 January 2025).

Rieder, B. and Hofmann, J. (2020) 'Towards platform observability', *Internet Policy Review*, 9(4), pp. 1–28.

Rogers, R. (2020) 'Deplatforming: following extreme internet celebrities to Telegram and alternative social media', *European Journal of Communication*, 35(3), pp. 213–229.

Rüdiger, T.-G. (2019) 'Polizei im digitalen Raum', *Aus Politik und Zeitgeschichte*, 69(21–23), pp. 18–23.

Reporters Without Borders (2017) *Russian bill is copy-and-paste of Germany's hate speech law* [Online]. 19 July. Available at: https://rsf.org/en/news/russian-bill-copy-and-paste-germanys-hate-speech-law (Accessed: 30 December 2024).

Ruschemeier, H. (2024). Flagging trusted flaggers. *Verfassungsblog*, 4 November [Online]. Available at: https://doi.org/10.59704/6c2c9f4cc624f31a (Accessed: 30 December 2024).

Scheer, O., Vela, J. H., & Jahn, T. (2025, January 24). EU-Kommission: Untersuchung zu X abgeschlossen – Musk droht Millionenstrafe. *Handelsblatt*. https://www.handelsblatt.com/politik/international/eu-kommission-untersuchung-zu-x-abgeschlossen-musk-droht-millionenstrafe/100102819.html

Schulz, W. (2019) 'Regulating intermediaries to protect privacy online – the case of the German NetzDG' in Schulz, W., Kettemann, M.C., and Heldt., A.P. (eds.) *Probleme und Potenziale des NetzDG ein Reader mit fünf HBI-Expertisen* [*Problems and potentials of the NetzDG*]. Hamburg: Verlag Hans-Bredow-Institut, pp. 7–19.

Seiling, L., Ohme, J., & Klinger, U. (2024). *Response to the consultation on the delegated regulation on data access provided for in the Digital Services Act*. Weizenbaum Institute [Online]. Available at: https://www.weizenbaum-institut.de/media/Publikationen/Weizenbaum_Policy_Paper/Weizenbaum_Policy_Paper_11.pdf (Accessed: 20 January 2025).

Senftleben, M. (2024) 'Human rights outsourcing and reliance on user activism in the DSA', *Verfassungsblog*, 21 February [Online]. Available at: https://verfassungsblog.de/human-rights-outsourcing-and-reliance-on-user-activism-in-the-dsa/ (Accessed: 30 December 2024).

Siegel, A. A. (2020) 'Online hate speech', in Persily, N. and Tucker, J.A. (eds.) *Social media and democracy: the state of the field, prospects for reform*. Cambridge: Cambridge University Press, pp. 56–88.

Specht-Riemenschneider, L. (2021) *Studie zur Regulierung eines privilegierten Zugangs zu Daten für Wissenschaft und Forschung durch die regulatorische Verankerung von Forschungsklauseln in den Sektoren Gesundheit, Online-Wirtschaft, Energie und Mobilität (Studie im Auftrag des Bundesministeriums für Bildung und Forschung)*. Fachbereich Rechtswissenschaft der Universität Bonn [Online]. Available at: https://www.jura.uni-bonn.de/fileadmin/Fachbereich_Rechtswissenschaft/Einrichtungen/Lehrstuehle/Specht/Dateien/2021-08-25-LSR.pdf (Accessed: 20 January 2025).

Spindler, G. (2017) 'Der Regierungsentwurf zum Netzwerkdurchsetzungsgesetz - europarechtswidrig?' *Zeitschrift für Urheber- und Medienrecht*, 61(6), pp. 473–487.

Sponholz, L. (2023) ‚Hate speech' in Strippel, C., Paasch-Colberg, S., Emmer, M. and Trebbe, J. (eds.) *Challenges and Perspectives of Hate Speech Research*. Digital Communication Research Vol. 12. Berlin: Böhland & Schremmer, pp. 143-163.

Stark, B., Stegmann, D. and Jürgens, P. (2020) *Are algorithms a threat to democracy? The rise of intermediaries: a challenge for public discourse*. Algorithm Watch [Online]. Available at: https://algorithmwatch.org/en/wp-content/uploads/2020/05/Governing-Platforms-communications-study-Stark-May-2020-AlgorithmWatch.pdf (Accessed: 20 January 2025).

Stippler, F., Scheuer, S., Kort, K., Holtermann, F., & Soares, P. A. de S. (2025, January 8). Tech-Konzern: Meta beendet Faktenchecks auf Facebook und Instagram. *Handelsblatt*. https://www.handelsblatt.com/technik/it-internet/tech-konzern-meta-beendet-faktenchecks-auf-facebook-und-instagram/100099044.html

The Economist. (2018) 'In Germany, online hate speech has real-world consequences', *The Economist* 12 January [Online]. Available at: https://www.economist.com/graphic-detail/2018/01/12/in-germany-online-hate-speech-has-real-world-consequences (Accessed: 19 January 2025).

'Treaty on the Functioning of the European Union' (2012) *Official Journal* C 326, 26 October, pp. 47-390 [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF (Accessed: 21 January 2025).

Tucker, J. et al (2018) 'Social Media, Political Polarization, and Political Disinformation: A Review of the Scientific Literature.' *SSRN Electronic Journal* [Online] Available at: https://doi.org/10.2139/ssrn.3144139 (Accessed: 21 January 2025).

Udupa, S., Gagliardone, I. and Hervik, P. (eds.) (2021) *Digital hate: the global conjuncture of extreme speech*. Bloomington: Indiana University Press.

Valerius, B. (2020) 'Hasskriminalität – Vergleichende Analyse unter Einschluss der deutschen Rechtslage', *Zeitschrift für die gesamte Strafrechtswissenschaft*, 132(3), pp. 666–689.

Van den Bos, K. (2020) 'Unfairness and radicalization', *Annual Review of Psychology*, 71(1), pp. 563–588.

Van Drunen, M. Z. and Noroozian, A. (2024) 'How to design data access for researchers: a legal and software development perspective', *Computer Law & Security Review*, 52 [Online].. Available at: https://doi.org/10.1016/j.clsr.2024.105946 (Accessed: 19 January 2025).

Wagner, E. (2019) *Intimisierte Öffentlichkeiten: Pöbeleien, Shitstorms und Emotionen auf Facebook*. Bielefeld: Transcript.

Williams, M. L., Burnap, P., Javed, A., Liu, H. and Ozalp, S. (2020) 'Hate in the machine: anti-black and anti-muslim social media posts as predictors of offline racially and religiously aggravated crime', *The British Journal of Criminology*, 60(1), pp. 93–117.

'X Corp v. Center for countering digital hate Inc.' (2023) Case 3:23-cv-03836 [Online]. Available at: https://s3.documentcloud.org/documents/23892523/x-corp-v-center-for-countering-digital-hate.pdf (Accessed: 21 January 2025).

The Brave Little Tailor v. Digital Giants: A Fairy-Tale Analysis of the Social Character of the DMA

Liza Herrmann

Abstract[1]

This Chapter examines the Digital Markets Act (DMA) from an interdisciplinary perspective, considering both legal and social science perspectives and using the Brothers Grimm's fairy tale of "The Brave Little Tailor" as a connecting narrative element. The DMA is a key piece of legislation in the legal jigsaw of the EU's digital strategy. It aims to contribute to contestable and fair markets in the digital sector across the EU, where a small number of large undertakings, called "gatekeepers", are present and provide core platform services, such as Facebook, YouTube, Google Shopping, and WhatsApp. This Chapter focuses on whether the DMA has a social character and seeks to answer this question in two main sections. The first reflects on the complicated relationship between law and social science and develops a so-called practical approach to try to overcome this never-unanimous discussion. This approach focuses on the benefits of learning from one another by sharing knowledge in an interdisciplinary context rather than taking one side. Subsequently, reflections on the social character of law in general are made. As such, the overriding good of society – derived from the principle of proportionality – serves as a benchmark for further consideration. The second section provides a legal overview of the DMA. It focuses on key aspects of the EU Regulation, such as background considerations on its development, objectives, and material and geographical scope. Building on this and using the aforementioned benchmark, the Chapter assesses several social aspects of the DMA. This mapping exercise shows that, while the DMA is not explicitly intended

1 This Chapter solely reflects the personal opinion of the author. The author would like to thank Dr Lucie Antoine for her initial support and Marie-Therese Sekwenz, Rita Gsenger as well as Lukas Kestler for their valuable comments during the writing process. The author also thanks all participants of the Digital Decade Workshop at the Weizenbaum Institute, Berlin, in September 2024 for their supportive feedback, which was tremendously helpful to the process of completing this paper.

to be a social Regulation, it contains several implicit social aspects that indicate a social character. Finally, and importantly, given the practical approach, the Chapter aims to stimulate further social science research on this topic. Accordingly, the Chapter ends by proposing possible further interdisciplinary research questions.

1. A fairy-tale introduction

Once upon a time, a few large digital giants—called gatekeepers—were able to use their great economic power to set the rules of the game on the internet, much to the detriment of their users and the platform economy. The economic power of these undertakings stems from the creation of "core platform services" (Art. 1(2), 2(2) DMA) (CPSs), which include, for example, online search engines, online social network services, or web browsers such as Facebook, Instagram, YouTube, Google Shopping, Google Maps, Amazon and WhatsApp. Among other things, these services connected many business users with many end users. This multi-sidedness allowed the digital giants to leverage their acquired advantages, such as access to large volumes of data, in other areas of their activities, potentially leading to network effects. Problematically, some of these undertakings could control entire platform ecosystems in the digital economy, even if they were not necessarily dominant under European competition law. That dominant position made it extremely difficult for existing or new market players to compete with them, as entry and exit barriers were (perilously) high. Consequently, a high risk existed that relevant digital markets would become dysfunctional. Stricter rules were requested to combat the digital giants and contain these potential threats. Therefore, the brave little tailor—called the European Commission (EC)—came up with a bold idea: the online and offline worlds are ultimately the same, so what is considered illegal offline must also be illegal online (Vestager, 2020). It is important to ensure everyone—whether they offer or use digital platforms in the EU—benefits from security, trust, innovation, and business opportunities (Breton, 2020). The EC has thus been working for several years on a new regulatory cutting pattern called the Digital Markets Act (DMA; Regulation (EU) 2022/1925). Although this Regulation was not entirely perfect from the outset, the brave little tailor never wavered in its efforts to complete its work and proposed it to the European legislator in 2020. Fortunately, the fight against the digital giants soon began to bear fruit. In less than two years,

the EC designated seven gatekeepers, namely Alphabet, Amazon, Apple, ByteDance, Meta, Microsoft, and Booking, and a total of 24 CPSs provided by these gatekeepers. In addition, the first judgment of the General Court at the Court of Justice of the European Union (CJEU) has been decided (ByteDance Ltd v. EU Commission, 2024a). The decision is currently the subject of an appeal (ByteDance Ltd v. EU Commission, 2024b).

This Chapter examines the DMA from an interdisciplinary perspective, taking into account both jurisprudence and social science. The focus is on whether the DMA is a Regulation with a social character—a question that has yet to be addressed in research. It aims to contribute to a better understanding of the relationship between jurisprudence and social sciences in terms of platform undertakings. The genre of the fairy tale functions as a connecting narrative element. As a subject of research, they are overlapping phenomena incorporating influences from a wide range of disciplines, including those relevant to this Chapter (cf. Bluhm, 2023, p. 3; Frey, Berthold and Bürgle, 2023, p. 541; Pöge-Alder, 2023a, p. 531). Fairy tales have, for centuries, been passed down and adapted from generation to generation (Pöge-Alder, 2023b, p. 447). They reflect the cultural backgrounds and moral concepts of earlier generations and deal with issues that remain relevant today and affect many people (Siegel and McDaniel, 1991, p. 558). Different phenomena of human existence and behaviour appear in fairy tales, such as emotions, moral judgements, communication, and social roles, making them a research subject in the social sciences (Frey, Berthold and Bürgle, 2023, p. 541). In addition, motifs and actions of jurisprudence are often found in fairy tales. The legal influence of the most famous fairy tale collectors and lawyers, the brothers Jacob (1785–1863) and Wilhelm Grimm (1786–1859), known as the "Brothers Grimm", plays a significant role (cf. Diederichsen, 2008, p. 13). The question of law and justice in fairy tales has therefore always been of interest to legal scholars (cf. Carpi and Leiboff, 2016; Lox, Lutkat and Kluge, 2007).[2] In the present analysis, the connecting, narrative fairy tale is that of *The Brave Little Tailor* (in German: Von einem tapfern Schneider), first published in 1812 by the Brothers Grimm in their *Children's and Household Tales* (in German:

2 See also "Once upon a law – the Grimm Brothers' stories, language and legal culture", a joint research project by the Faculty of Arts and Social Sciences, the Faculty of Law, and the University Library of Maastricht University. This project explores the relationship between the Brothers Grimm's collection of fairy tales, their work on language, and the law. See, Once upon a law, 2022.

Kinder- und Hausmärchen (KHM); cf. Grimm and Grimm, 1812, p. 77).[3] The protagonist of the fairy tale, the brave little tailor, goes out into the world and experiences various (un-)real adventures and challenges before finally marrying the king's daughter and ascending to the throne as a reward for his courage. One of the ways he proves his bravery is by killing seven flies (not people, as the other fairy tale characters mistakenly believe) with one blow, which he prominently writes on his belt. Notwithstanding the coincidence, the EC has already named seven gatekeepers—but not (yet) killed them!—shows the brave little tailor's aptness as a narrative element. He is a symbol of how to deal meaningfully with the forces and powers of life and develop moral autonomy in the process (Müller, 1985, p. 24). As shown below, the EC had a similar vision in mind when developing the DMA.

In order to answer the research question, this Chapter proceeds as follows: first, it reflects on the controversial relationship between law and social science and advances a proposal for dealing with this controversy by adopting a so-called *practical approach*. With this in mind, the social character of law in general is considered. The second step involves providing a legal overview of the DMA. Afterwards, the Chapter assesses the Regulation in terms of its social aspects. The previous considerations serve as a benchmark for this mapping exercise. The final step is to draw conclusions in relation to the research question and to develop research questions for further interdisciplinary research on the topic.

3 The KHM is a collection of fairy tales first published in 1812 by Jacob and Wilhelm Grimm. A second volume followed in 1814 (though this was dated 1815), and a revised edition appeared in 1819. The final German edition to be published during the lifetime of the Grimm brothers was the seventh (1857). Although the most accurate translation of the Grimms' title would be Children's and Household Tales, most English readers are familiar with these stories as Grimms' Fairy Tales, or, more commonly, grammatically incorrect, Grimm's Fairy Tales. The fairy tale of The Brave Little Tailor can be found in no. 20 of the KHM.

2. Foundational reflections on law and social science

2.1 The (complicated) relationship between law and social science: a practical approach

By its nature, law and social science are interdisciplinary (Bornstein, 2016, p. 113). According to common understanding, social science is the scientific discipline that deals with the order and organisation of human coexistence (Lehner, 2011, p. 13 f.). The research object of social science is society, i.e., a large and heterogeneous group of people whose coexistence and interaction are ordered and organised (Lehner, 2011, pp. 24, 80; Luhmann, 1995, p. 7). The word social, in simple terms, has three meanings: (1) socially oriented; (2) facing society (negative: antisocial); and (3) aiming at a certain state of society, especially in the sense of negating hardship and approaching equality (Zacher, 1981, p. 726).[4] Social science primarily uses empirical research methods, which continue to be somewhat novel in legal research. Regarding the common understanding of law, it can become a suitable sparring partner for social science. The law is the sum of the rules, regulations, principles, norms, ethics and standards that govern human behaviour in society (Parajuli and Lamicchane, 2019, p. 140). Consequently, the law, in its diversity, has a social connection. The legal system is a differentiated functional system in society; therefore, it always carries out the self-reproduction (autopoiesis) of the social system with its own operations (Luhmann, 1999, p. 3). In other words: From a legal perspective, the legal world is not detached but rather part of our everyday world; we live in the law of this society, even if we do not follow its dictates —whether we want to or not (Kißler, 1984, p. 91). Accordingly, various social functions have emerged in the law to consolidate the cohesion of the legal community. Examples include the settlement of conflicts (reaction function), the control of behaviour (regulatory function), the legitimacy and organisation of social rules (constitutional function), the shaping of

4 These meanings are also reflected in the origin of the word *social*. The word was etymologically borrowed in the 18th century from the French word *social*, which comes from the Latin word *sociālis* (concerning society, communal, sociable), derived from the Latin *socius* (common). The French word *social*, meaning sociable at the beginning of the 17th century, was understood by 18th-century encyclopaedists, who stood in the tradition of natural lawyers, in the sense of directed towards the relationships of living together, connected to the community and serving it as an expression of natural and rational morality that characterises human coexistence (Pfeifer et al, 1993).

living conditions (planning function), and the administration of justice (supervisory function) (Rehbinder, 1973, p. 366).[5]

Nevertheless, the relationship between jurisprudence and the social sciences has consistently been difficult to tackle. A unanimous view on this topic may well be an impossible goal to achieve. Crucial questions arise, such as "Is law a science and if law is a [real] science, what is it really? Law as a social science?" (Rottleuthner, 2021, pp. 264 ff.; Transl. by the author), "What particular characteristics must a social order have in order to be called law?" (Geiger, 1987, p. 5; Transl. by the author), or *What can the lawyer learn from the social sciences?* (Derber, 1963, p. 145). The controversy is often understood as an evaluation of the individual view of the questioner, taking into account their different personal views of society and the law (Hopt, 1975, p. 341). Consequently, the "defensive ignoramus", "progressive author", and "critical jurist" (Hopt, 1975, p. 341; Transl. by the author) involved in this discussion will never agree on one view. Furthermore, although society links the two disciplines, it is perhaps surprising to note that the relationship between the law and social science has tended to be examined in a generally one-sided manner (Kähler, 2018, p. 107). On the one hand, jurisprudence has traditionally drawn comparatively strong links to other disciplines, such as economics, history, and philosophy, thereby leading to it being termed as the "science of sciences" in the 17th century (cf. Doddridge, 1631, p. 35). Of course, this does not grant jurisprudence the right to assume a position of supremacy in scientific discourse. On the other hand, the social sciences have a contrary understanding of this relationship, as the study of law plays only a subordinate role (Rosenstock, Singelnstein and Boulanger, 2019, p. 3). One reason could be that social science research on law in the German-speaking world, unlike in the Anglosphere, remains relatively confined within the respective disciplinary boundaries. Moreover, social science research on law also lacks an institutionally secured bundling as well as a place of firm anchoring (Rosenstock, Singelnstein and Boulanger, 2019, p. 28; Shapiro and Pearse, 2012, p. 1504). Admittedly, this Chapter also analyses whether the DMA contains social aspects, mainly from a legal perspective, due to relevant background knowledge. Thus, the social is explored within the legal.

5 This list is not exhaustive. In the relevant literature, a large number of different functions have emerged, which can vary depending on the perspective of the respective observer. According to Pötzsch (2009, pp. 131 ff.), law has not only a social and societal function but also ensures peace, guarantees the freedom of the individual, and regulates private legal relationships, for example.

Does this complicated relationship mean that a fruitful exchange between the two disciplines is doomed to failure? That cannot be the case. Although the concrete value of interdisciplinary research can never be quantified, the solution cannot be to refrain from any form of exchange. In fact, the beauty of interdisciplinary research is the shared desire to investigate problems and questions that affect several disciplines. At best, the combined expertise of the interdisciplinary team should lead to more innovative and impactful science (cf. Wuchty, Jones and Uzzi, 2007, p. 1036). The exact nature of the relationship between the disciplines is less important for the research question at hand. Rather, the benefits of interdisciplinary research lead this Chapter to a so-called *practical approach* inspired by the brave little tailor. In order to comprehend this approach, it is necessary to examine one key scene within the fairy tale: In a trial of strength with a giant, the brave little tailor crushes a piece of cheese (believed by the giant to be a stone) until its juice runs out, thereby demonstrating his strength through this seemingly impossible task (Ashliman, 2005). He took something similar to what the giant used but something he could manage within the limits of his strength. Therefore, the proposed *practical approach* focuses on the benefits of learning from one another by sharing knowledge in an interdisciplinary context. It does not try to settle the heated debate outlined above, nor does it pass any judgment on understanding the right or wrong relationship between the two disciplines.

2.2 What constitutes the social character of law?

Given the complicated relationship between law and social science, general considerations of the social character of law are challenging. Spoiler: There is no single definition or list of criteria. Accordingly, one might ask why this question is worth asking. The aim is not to find a specific answer. Instead, it deals with the complexity of the question, and maps out cases and criteria that might serve as a starting point for further (interdisciplinary) research. To simplify complex issues, lawyers—quite understandably—tend to press laws into fixed patterns. In order to think outside of these patterns and dare to try something new, it is worth also tackling ambiguous questions. That is a suitable way to develop interdisciplinary research and to benefit from the above. Similarly, the little tailor rarely had a single solution to his challenges

on his journey. Instead, he had to come up with creative solutions to get ahead.

When considering the social character of law, the first thing that comes to mind is whether it is directly aimed at serving society. This is undoubtedly the case when the legislator explicitly defines serving society as the aim or objective of the relevant legal text, such as in the German Social Codes (SGB; *Sozialgesetzbuch*).[6] Others may go even further and understand the law in general as a social system endowed with sanctioning power, whose claim to validity, unlike other systems (e.g., customs or morality), is justified by a higher degree of social communication (Habermas, 1992, p. 44; Kißler, 1984, pp. 92, 95; Luhmann, 1995, p. 35). The premise of the law as a social system is consistent with the assumption that the law, in its diversity, has a social connection. Do these considerations mean that no law is *antisocial* or, conversely, that every law has a social character per se? Is it not the case that any law that has been the subject of a legislative process and thus has the legitimacy of its society (at least in a democratic state) automatically serves its society? Ideally, such a law should not be directed against its society but rather strengthened, as the consideration of the functions of law has already shown.

Nevertheless, the *principle of proportionality* may help make this idea more tangible and find points of reference in the law, given that a democratically legitimate law is inherently social. This principle of the rule of law plays an important role in protecting fundamental rights and assessing legislation in the EU and its Member States. At the European level, very early on, the CJEU took up proportionality in its case law (see Fédération Charbonnière de Belgique v. High Authority of the European Coal and Steel Community, 1956) before establishing it as a general principle (Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel, 1970). With the Maastricht Treaty, the principle of proportionality was "constitutionalised" (Lenaerts, 2021, p. 1), and is now reflected in Art. 5(4) of the Treaty on European Union (TEU) and in the EU Protocol (No 2) on the Application of the Principles of Subsidiarity and Proportionality, and functions as a general principle of EU law. According to Art. 5(4) TEU, the content and form of EU action shall not exceed what

6 For instance, as mentioned in Section 1(1) of the SGB First Book (I) – General Part, according to which the law of the Social Code is intended to shape social benefits, including social and educational assistance, in order to realise social justice and social security.

is necessary to achieve the objectives of the Treaties; the institutions of the EU shall apply the principle. Furthermore, as a general principle of EU law, proportionality also applies to the Member States when they implement EU measures or when their actions restrict fundamental freedoms (Lenaerts, 2021, p. 2; see also Art. 4(3) TEU). Inversely, the principle is reflected at the national level. In Germany, for instance, the principle of proportionality has constitutional status despite not being explicitly mentioned. It derives from the principle of the rule of law (see Art. 20(3) of the Basic Law for the Federal Republic of Germany (GG; *Grundgesetz*)) and from the very nature of fundamental rights. It limits the state's interference in the individual rights and freedoms of its citizens. As an expression of the citizen's general claim to freedom vis-à-vis the state, these rights may only be restricted by public authority to the extent that doing so would be indispensable for protecting the public interest. According to Wienbracke (2013, p. 148), the assessment of the principle of proportionality has four components: Firstly, all EU or national measures must have a legitimate purpose (the so-called *desired end* in EU law). Second, they must also be suitable for achieving or furthering the purpose pursued. Third, measures must be taken to achieve said purpose. Fourthly, it must not be disproportionate to the objective and purpose of public interest that they pursue, which is also referred to as *appropriateness* in the narrower sense. Upon closer inspection of the four components, the appropriateness test means that those affected by a state measure must not be excessively or unreasonably burdened. Therefore, balancing the various legal interests affected by a state measure is required. In this regard, the German Federal Constitutional Court (BVerfG; *Bundesverfassungsgericht*) has regularly ruled that the loss of freedom protected by fundamental rights must not be disproportionate to the public welfare objectives served by a restriction of fundamental rights (cf. BVerfG, 2020, para. 95). The legislator must strike an appropriate balance between general and individual interests. In so doing, the so-called *prohibition of excessiveness* must be observed. To this end, the scope and weight of the interference must be balanced against the importance of the law in question for the effective fulfilment of the tasks of the state. Within narrow limits that must always be observed, an individual impairment may be accepted in favour of the so-called *overriding common good of society*. The common good of society is a desirable societal state, which can be prioritised after an appropriate balance has been struck. Due to its fundamental social meaning, it thus serves as a benchmark for determining the social character

of law in general, which is of interest for the underlying fairy tale. This idea will be developed in the later evaluation (under Section 4).

3. Legal overview of the DMA

A basic legal understanding of the underlying Regulation is needed to follow the *practical approach*. There is little doubt that large platform undertakings, such as Google and others have a vital role as economic actors and drivers of innovation and efficiency in the 21st century. On the downside, some undertakings have become (too) powerful market players in recent years, thereby threatening the functionality of the digital sector. To provide a regulatory counterweight to this risk, the DMA is one of the pieces in the jigsaw of various European legislative initiatives that prioritise the individual and open up new opportunities for other market participants (European Commission, 2023). Even the supposedly weaker little tailor always finds his way using his wits, cunning, courage, and adaptability. That requires innovative ideas, such as throwing a bird instead of a stone to defeat giants in a stone-throwing contest (which occurred after the cheese-stone showdown). The same concept can be seen in the DMA: The European legislator is taking a bold and optimistic step. Instead of waiting and letting things take their course, the first regulatory measures have been taken, although they will be evaluated regularly. Naturally, this has not been immune from the scepticism and disapproval of those affected. However, this bold and optimistic step was necessary to ensure that the digital sector does not become a legal vacuum for some at the expense of many.

3.1 Background considerations on the development of the Regulation

In December 2020, the EC published the first proposal for a Regulation to promote contestable and fair markets in the digital sector. At the time, the EC was a global pioneer with this initiative, much like the brave little tailor who ventured out into the unknown. After going through the European legislative process with several amendments, the European Parliament and the Council adopted the DMA with an overwhelming majority in July 2022. The final text was published in the *Official Journal of the EU* on 12 October 2022 and entered into force on 1 November 2022. Due to its legal nature

as an EU Regulation, it became directly applicable in all EU Member States from 2 May 2023 without transposing into national laws.

In a nutshell, the EC considered three main problems when drafting the legislative proposal (cf. Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act), 2020, pp. 1 ff.). Firstly, the risk of weak competition in markets in the digital sector due to excessive control of entire platform ecosystems by large online platforms, which essentially cannot be challenged by existing or new market participants—regardless of how innovative and efficient they may be. Secondly, the risk of unfair terms and conditions for business users due to a high degree of economic dependency on online platforms. Therefore, business users generally have a poorer negotiating position, which could be exploited unfairly or be detrimental to the end user. The negative effects of such unfair practices on the economy and society were feared. Thirdly, until the introduction of the DMA, no standardised Regulation that could adequately sanction the harmful activities of online platforms existed in the EU. Finally, there was a risk of fragmented Regulation and supervision by the individual Member States (and still exists; see Herrmann and Kestler, 2024, pp. 143 ff.).

3.2 The dual objectives of the DMA

In order to adequately address the aforementioned problems, the DMA has two objectives: It aims to ensure the *contestability* and *fairness* of markets in the digital sector for business and end users of CPSs, thereby contributing to the smooth functioning of the internal market (see Art. 1(1) and (2), Recital 7 DMA). Both objectives are intertwined ("dual-function rotary switch", cf. Crémer et al, 2023, p. 989), which leads to a complex interpretation (Hoffmann, Herrmann and Kestler, 2024, p. 133). The dual objective of equal priority is intended to emphasise that the DMA is not (purely) a competition policy legislation but that the provisions are to be understood as complementary to the existing competition policy standards (Käseberg and Gappa, 2024, Art. 1, Rn. 5). The problem is that the legislation frequently mentions the objectives, such as in Art. 12(5), and in Recitals 31–34 DMA, the exact definition is left open (Crémer et al, 2023, p. 978; König, 2023a, Art. 1, Rn. 4 ff.). A lack of understanding of the objectives can lead

to more difficult implementation in the initial phase of the Regulation, as there is little case law on interpretating of the DMA so far.[7]

An indication of how to specify the objective of contestability in the DMA can be found in Arts. 12(5) lit. (a)(i) and (ii). According to this, the contestability of CPSs is limited if a gatekeeper practice is capable of impeding innovation and limiting choice for business and end users by creating or strengthening barriers to entry or expansion (i), or, alternatively, preventing other operators from having the same access to a key input as the gatekeeper (ii). The contestability of the CPS and the associated ecosystems is particularly limited by the CPS's inherent features, especially by network effects, strong economies of scale of individual services, and data advantages. For a better understanding of fairness, Art. 12(5) lit. (b) can help. According to this, a gatekeeper practice shall be considered unfair where there is an imbalance between the rights and obligations of business users, and the gatekeeper obtains an advantage from business users that is disproportionate to the service provided by the latter to the former (see Recital 32). In particular, the legislator had in mind the case where gatekeepers, by virtue of their gateway function and overwhelming bargaining power, engage in conduct that prevents others from fully benefiting from their own contributions and set unilaterally unbalanced conditions for the use of their CPSs or services provided with, or in support of, their CPSs (see Recital 33). In sum, contestability is aimed at fundamental market structure problems and predatory practices, while fairness is geared towards the exploitative nature of certain CPSs.

3.3 The material and geographical scope

The material scope of the DMA relates to markets in the digital sector where gatekeepers operate (see Art. 1(1) and Recital 7). The term *digital sector* is legally defined in Art. 2(4), and includes all products and services s provided by means of, or through, information society services within the meaning of Art. 2(3) DMA in conjunction with Art. 1(1) lit. (b) Directive (EU) 2015/1535, lays down a procedure for providing information in

7 To date, claimants have brought five actions before the CJEU to challenge decisions taken in the context of the gatekeeper designation procedure: 'ByteDance Ltd v. EU Commission' (2024a and 2024b); 'Meta Platforms v. EU Commission' (2024) and 'Apple v. EU Commission' (2024a and 2024b). All cases concern the disputed position as gatekeeper, not the interpretation of fairness and contestability.

the field of technical regulations and rules on information society services. The rules include any service normally provided for remuneration at a distance, by electronic means and at the individual request of a recipient of services. This broad understanding of the term is limited by the personal requirement that *gatekeepers* must be active in these markets. Gatekeepers are the sole addressees of the DMA. It was not the legislator's intention to include all undertakings operating in the digital sector in the material scope of the Regulation per se. Rather, the material scope was deliberately kept small in order to account for the economic characteristics of digital markets. Examples include the pronounced network effects and the dependence on large amounts of data, which lead to large economic power in the hands of a few undertakings. According to Art. 2(1), a gatekeeper is an undertaking that provides CPSs and has been designated as such by the EC pursuant to Art. 3, which is quoted (in part) below for ease of reference.

> *1. An undertaking shall be designated as a gatekeeper if:*
> *(a) it has a significant impact on the internal market;*
> *(b) it provides a core platform service which is an important gateway for business users to reach end users; and*
> *(c) it enjoys an entrenched and durable position, in its operations, or it is foreseeable that it will enjoy such a position in the near future.*
>
> *2. An undertaking shall be presumed to satisfy the respective requirements in paragraph 1:*
> *(a) as regards paragraph 1, point (a), where it achieves an annual Union turnover equal to or above EUR 7,5 billion in each of the last three financial years, or where its average market capitalisation or its equivalent fair market value amounted to at least EUR 75 billion in the last financial year, and it provides the same core platform service in at least three Member States;*
> *(b) as regards paragraph 1, point (b), where it provides a core platform service that in the last financial year has at least 45 million monthly active end users established or located in the Union and at least 10 000 yearly active business users established in the Union, identified and calculated in accordance with the methodology and indicators set out in the Annex;*
> *(c) as regards paragraph 1, point (c), where the thresholds in point (b) of this paragraph were met in each of the last three financial years.*
>
> *3. Where an undertaking providing core platform services meets all of the thresholds in paragraph 2, it shall notify the Commission thereof without delay and in any event within 2 months after those thresholds are met and provide it with the relevant information identified in paragraph 2. […]*
>
> *[…]*

Figure 1: Excerpt from Art. 3 DMA

The basic concept of the designation process is set out in Art. 3(1) and is based on three cumulative qualitative criteria. These criteria can be determined as fulfilled in two ways: First, operationally, by considering the thresholds under Art. 3(2), which represent quantitative rebuttable

presumptions. Secondly, through a market investigation under Art. 3(8) in conjunction with Art. 17. A key criterion for the designation process is that the relevant undertaking provides a CPS (defined in Art. 2(2)). These include, for example, online search engines, online social network services, or web browsers. While the list of CPSs is exhaustive, it can be further extended to include services in the digital sector by means of the ordinary legislative procedure in accordance with Art. 19(3) lit. a). It is important to note that providing a CPS is sufficient, i.e., the DMA does not require a conglomerate in an economic understanding or the control of an ecosystem of digital services (König, 2023b, Einleitung, Rn. 25, 26). Pursuant to Art. 3(3), an undertaking providing CPSs and meeting any of the thresholds set out in Art. 3(2) is obliged to notify and provide the relevant information to the EC. This obligation arises without delay and, in any case, within two months of the thresholds being met. The EC has the sole authority to designate an undertaking as a gatekeeper if all relevant criteria are met. The gatekeeper should be determined without undue delay and at the latest within 45 working days after receiving the complete information referred to in Art. 3(3). In this process, cooperation and coordination with national competent authorities (NCAs) enforcing competition rules to conduct investigations into potential non-compliance by gatekeepers with certain obligations under the DMA is possible (see Arts. 1(7), 37, 38, 41 and Recital 91).

The geographical scope of the DMA is laid out in Art. 1(1) based on the beneficiaries of the Regulation, namely businesses and end users, and refers to the EU. According to the legal definition in Art. 2(21), a business user refers to any natural or legal person acting in a commercial or professional capacity using CPSs for the purpose, or in the course, of providing goods or services to end users. In addition, according to Art. 2(20), an end user means any natural or legal person using CPSs other than as a business user. The distinction between the two types of users is based on how the platform is used: A business user uses CPSs to offer its products/services, while the party demanding the service is always the end user. It is irrelevant whether the person demanding the service is acting privately or as part of their professional activities. Therefore, anyone who uses a CPS to offer products or services for private purposes (e.g., private sellers on eBay) is considered an end user (Bongartz and Kirk, 2024, Art. 2, Rn. 107). The DMA applies to CPSs provided or offered by gatekeepers to business users established in the EU or end users established or present in the EU. The

place of establishment and location of the gatekeeper are irrelevant. The other law applicable to the provision of services is also irrelevant. The EC is thus building a bridge to the United States of America, where most of the gatekeepers appointed so far come from, without necessarily creating a global regulatory framework.[8] This endeavour brings to mind the story of the brave little tailor who, after killing seven flies with one blow, spoke of his accomplishment as follows: "'The town? [...] The whole world shall hear about this!' And his heart jumped for joy like a lamb's tail. The tailor tied the banner around his body and set forth into the world, for he thought that his workshop [the tailoring shop] was too small for such bravery" (Ashliman, 2005).

3.4 The gatekeeper's obligations and prohibitions

Two aspects are of great importance when considering the gatekeeper's obligations and prohibitions. First, to whom they apply and how they are designed, and second, the new *ex ante* control approach of the DMA. Starting with the first aspect, it is particularly important to understand that although gatekeepers are the sole addressees of the DMA, the behavioural obligations and prohibitions only apply to specific CPSs of the gatekeeper concerned. The DMA cannot be applied, as long as a gatekeeper service is not designated as a CPS. In other words, a gatekeeper must comply with all DMA obligations and prohibitions for each of its CPSs listed in the individual designation decisions of the EC (see Arts. 5(1), 6(1), and 3(9)), which, however, does extend to the entire undertaking. The obligations and prohibitions form the core of the Regulation and are laid down in Arts. 5–7, but could be updated in the future following market analyses. It is important to note that they are essentially the same for all gatekeepers and that there is no overarching system between the obligations and prohibitions, so that all gatekeepers and both obligations and prohibitions are considered equally (Göhsl and Zimmer, 2025, Art. 5, Rn. 2, 3). An overview of the three DMA articles containing the do's (obligations) and don'ts (prohibitions):

– Firstly, Art. 5 contains provisions that apply without further specification. Examples include the obligation not to prevent business users

8 The term *Brussels effect* is often used in this context, referring to the de facto adoption of EU law outside the European Single Market (for further information, see Bradford, 2020).

from offering products through other distribution channels at different prices or conditions (Art. 5 (3)) and the prohibition on requiring end or business users to an identification service, a web browser engine, a payment service, or technical services that support the provision of payment services (Art. 5(7)).

– Secondly, the provisions of Art. 6 are also directly applicable but may be further specified by an EC decision on a case-by-case basis under Arts. 8(2) or (3). The direct applicability results from the unconditional nature of the obligations. This means that the behavioural requirements set out in Art. 6 are already binding in themselves and do not necessarily require further implementing measures by the EC. For this reason, the wording of the official heading of Art. 6 should not be misleading, as it places the provisions of Art. 6 under the condition that they are "susceptible of being further specified under Art. 8". The possibility of further specification refers only to the EC's ability to determine the measures that a particular gatekeeper must take to comply with the obligations and prohibitions of Art. 6 and not, in the abstract, to the obligations and prohibitions themselves (Bueren and Weck, 2023, Art. 6, Rn 1). In addition, the EC may, on its own initiative or at the request of a gatekeeper, initiate specification proceedings under Art. 8. However, there is no right for a gatekeeper to initiate such a procedure. Rather, it is at the discretion of the EC to decide whether to engage in such a process, respecting the principles of equal treatment, proportionality and good administration (cf. Art. 8(3)). Examples of obligations under Art. 6 include the prohibition on treating services and products offered by the gatekeeper more favourably than similar services or products offered by third parties in the ranking and related indexing and crawling and the obligation for the gatekeeper to apply transparent, fair and non-discriminatory conditions to such ranking (Art. 6(5)). The DMA has a broad understanding of rankings (see definition in Art. 2(22)) which includes, but is not limited to, algorithmic rankings. Moreover, an obligation not to impose general conditions for terminating the provision of CPSs that are disproportionate (Art. 6(13)) are defined.
– Thirdly, Art. 7 contains far-reaching interoperability obligations for (simplified) messaging services, such as WhatsApp, as these are particularly sensitive to network effects due to the frequent lack of connectivity between communication services from different providers. The background to this interoperability consideration is that users understandably prefer services that other party to the conversation also uses. As such,

services with many users become increasingly attractive and economically stronger due to high usage shares, which, in turn, can lead to consumer dependency and reduce competition in the relevant market.

The second aspect of great importance is the DMA's new *ex ante* control approach. Under this approach, the aforementioned obligations and prohibitions for gatekeepers providing CPS are classified as permitted or prohibited even before the behaviour has occurred. Therefore, all of the DMA's obligations are immediately and directly applicable without the need for a concretising decision by the EC ("self-executing"; cf. Podszun, 2023, p. 1). Why is this *ex ante* approach new? Under European competition law, which has so far been the main legal instrument to tackle behaviour that threatens competition in the EU's single market, the EC can only act if the undertaking concerned has already breached a legal obligation (so-called *ex post* control approach). One reason is that, under the central European competition rules of Arts. 101 and 102 of the Treaty on the Functioning of the European Union (TFEU), investigation procedures require a specific analysis that can only be conducted *ex post* (i.e., after a competition problem has emerged) and may take too long (Madiega, 2022, p. 2). The EC has now skilfully transferred responsibility for compliance with the Regulation to the addressee at an early stage. Consequently, gatekeepers must ensure and demonstrate compliance with the obligations, which must be effective to achieve the objectives and relevant obligations of the Regulation (see Art. 8(1)). As a side note, the DMA is not seen as European competition law; therefore, the established *ex post* control approach does not fit here. Instead, Art. 1(6) clarifies that both regimes apply in parallel. However, the relationship between the DMA and national competition law is controversial due to the unclear scope of Art. 1(6) s. 2 lit. (b), which shall not be further explained here due to the introductory focus of this Chapter.[9]

3.5 Enforcement and penalties for non-compliance

The EC is the sole enforcement authority (sole enforcer) of the DMA, and has full discretion over whether to open a proceeding under the DMA. The EC's procedural, investigative, and decision-making powers are regulated in Art. 20 et seq. To optimise procedures within the EC and to pool

9 For further discussion of this problem see Graef, 2024; Gryllos, 2024; Moreno Belloso and Petit, 2023; Robertson, 2024.

resources, a DMA unit has been formed within the EC, which consists of a joint team of members of the Directorates-General for Competition ("DG COMP") and Communications Networks, Content and Technology ("DG CONNECT"). By contrast, NCAs have only a supporting role in the enforcement procedure. Indeed, the DMA allows them to cooperate and coordinate when enforcing national competition rules for gatekeepers, as well as to initiate investigations into compliance with the DMA and report their findings to the EC. For instance, the German legislator has granted such powers to the German Federal Cartel Office (BKartA; *Bundeskartellamt*) in the 11th amendment to the German Competition Act (GWB; *Gesetz gegen Wettbewerbsbeschränkungen*). In case of overlapping investigations under the DMA, the NCA concerned should inform the EC before taking its first investigative measure into possible non-compliance by gatekeepers with certain obligations and prohibitions under the DMA.

As noted above, the DMA's obligations and prohibitions are self-executing: Gatekeepers are legally obliged to implement their do's and don'ts. They must ensure this, inter alia, by establishing a compliance function, and are subject to audit and reporting obligations, which place the burden of proof of compliance with the DMA on the gatekeepers. In case of breaching an obligation or prohibition, gatekeepers face fines of up to 10% of their total global turnover or up to 20% in the event of a repeat offence (see Arts. 29–30). The wording of Art. 30(1) ("may impose") indicates that the EC has discretion in imposing a fine. Therefore, the EC is not obliged to impose a fine and cannot be forced by third parties. In fixing the amount of a fine, the EC shall consider the gravity, duration, and recurrence, as well as possible delays caused to the proceedings by the gatekeeper (Art. 30(4)). In addition, the EC may impose periodic penalty payments under Art. 31, which may also be imposed cumulatively with fines as per the *ne bis in idem* principle, which prohibits double jeopardy in the same case. The periodic penalty payments shall not exceed 5% of the gatekeeper's average daily global turnover per day in the preceding financial year. From a monetary perspective, the total amount of possible fines can be a highly sensitive issue for gatekeepers, as the fines are not imposed on the CPS that breaches an obligation or prohibition but on the undertaking as a whole. Consequently, it is hoped that this will have a strong deterrent effect.

4. Assessment of social aspects of the DMA

Based on the legal overview, this section more closely inspects the research question: Is the DMA a Regulation with a social character? In light of the earlier foundational reflections on law and social science, the DMA is not a Regulation with an explicitly stated aim or objective to serve society, such as the German SGB. However, this does not mean that the DMA does not implicitly serve society—much like how fairy tales do not represent only one view of human existence and behaviour. In order to make the social character of the DMA more tangible and to identify its specific social aspects, the earlier consideration of the *overriding common good of society* is used as a benchmark for this mapping exercise, which also accords with the proposed *practical approach*. Therefore, a selection of aspects is identified in the DMA that may constitute explicit or implicit social criteria, considered in light of the overriding common good of society. This selection is not exhaustive, as other or additional aspects may be used depending on the benchmark chosen and the focus of further investigation. An overview:

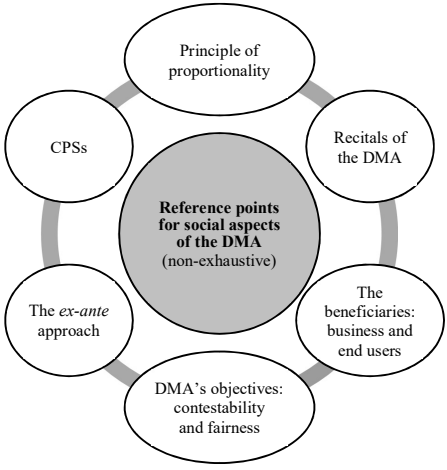

Figure 2: Overview of non-exhaustive reference points for social aspects of the DMA (created by the author)

4.1 Explicit references to the principle of proportionality in the DMA

As shown, the common good of society is an important element in examining proportionality when testing the appropriateness (in the narrower sense) of a European or state action and at the same time, it is a suitable criterion when analysing the social character of law in general. The principle of proportionality is explicitly mentioned on several occasions within the DMA, such as in Recitals 27, 28, 29, 65, 75, and 107, and Arts. 8(3), 23(10). As stated in Recital 107, in accordance with the principle of proportionality as set out in Art. 5(4) TEU, the DMA does not go beyond what is necessary in order to achieve its objectives. This illustrates that while priority is given to achieving its objectives, the Regulation also sets limits when considering individual cases. This ensures, among other things, the proper functioning of the internal market, which is one of the core objectives of the EU (Huerkamp and Nuys, 2024, Art. 18, Rn. 34). Therefore, the inclusion of the principle of proportionality is a strong expression of a social aspect in the DMA.

4.2 The recitals

A second possible starting point for a social aspect can be found in the DMA's recitals. Prior to the DMA's introduction, several Member States had already enacted laws addressing unfair practices and the contestability of digital services, such as Germany's Section 19a of the GWB. However, this led to an inconsistent level of regulation across the EU, with the risk of internal market fragmentation and higher compliance costs. The European legislator has recognised this problem (cf. explanations under Section 3.1.). Recitals 6 and 31 thus state that the identified unfair practices of large platform undertakings can negatively affect the European economy and society in the internal market. These practices have created the need for a clear and unambiguous set of harmonised rules to address these issues. These considerations by the European legislator clearly show that the protection of European society as a whole was one of the intentions of the

regulatory process. Indeed, the desire for this protection strongly reflects the Regulation's social aspect.

4.3 The beneficiaries

The beneficiaries of the Regulation provide a third possible starting point for a social aspect. As mentioned, these are the business and end users of CPSs in the EU. Under the present definition of society as a large and heterogeneous group of people whose co-existence and interaction are ordered and organised (Lehner, 2011; Luhmann, 1995), both beneficiaries – at least in the form of any natural person—are part of European society as a whole. Both are key elements in designating an undertaking as a gatekeeper under Art. 3 (see above). The provision of services to many business and end users signals the existence of dependencies and a resulting imbalance in bargaining power (whatever its causes). In this respect, it indicates unfair market conditions (Bueren and Weck, 2023, Art. 3, Rn. 54). At the same time, high user numbers of at least 45 million monthly active end users established or located in the EU and at least 10,000 yearly active business users established in the EU in the last financial year show the influence of a few CPSs on large parts of European society. For example, the CPS Facebook, which belongs to the designated gatekeeper Meta Platforms, Inc., had 408 million monthly active end users in the fourth quarter of 2023 alone (Meta Platforms Inc., 2024). In contrast, approximately 449 million people had their usual residence in an EU Member State as of 1 January 2024 (Eurostat, 2024). Of course, not every person in Europe uses Meta; multiple visits by individual users are also possible. Nevertheless, these figures are an impressive illustration of how one specific CPS can reach a huge swathe of society. In purely numerical terms, the European legislator has thus prioritised the protection of society's common good over the economic interests of a few large platform undertakings. Consequently, these considerations also imply a strong social aspect of the DMA.

4.4 The regulatory objectives

A fourth approach to a social criterion can be found in the DMA's dual objectives of contestability and fairness of digital-sector markets. A major underlying question in drafting the legal text was whether democratic

societies should accept the behaviour of large platform undertakings to their own detriment. The DMA has clearly rejected this with its stated objectives. The fairness objective considers that users of CPSs should be afforded the highest level of protection, which can promote user trust in digital platform undertakings by ensuring the protection of their rights. By creating a level playing field from a contestability perspective, the DMA seeks to ensure that no CPS exercises excessive market power, such as by spreading disinformation or exploiting user data. Consequently, small and medium-sized enterprises (SMEs) should be able to enter the market and compete, thereby leading to more diverse, innovative, and resilient digital economy. Ultimately, this can also benefit users by giving them a wider choice of services and products and by improving the quality and security of CPSs. However, it is not only users who are empowered but society as a whole. Based on the underlying question, the political representatives of European society set limits to almost unfathomable digital powers, using overarching objectives to do so. These objectives express their vision of how society should relate to platform undertakings and, thus, at its core, a social aspect.

4.5 The ex ante control approach

A fifth approach to a social criterion is the DMA's new *ex ante* control approach to gatekeeper obligations. The European legislator believes that the self-execution of the DMA's obligations and prohibitions has a strong deterrent effect. Ideally, harmful behaviour should not occur in the first place. In this way, the welfare of the beneficiaries, and thus of a large part of European society, is addressed and protected early. Therefore, this approach also supports social aspect due to time constraints.

4.6 Core platform services

Finally, CPSs may also be an appropriate reference point for the DMA's social aspects. Indeed, the legislator intended that certain types of services, such as online intermediation services, online search engines, operating systems, or online social networks, should fall within the scope of the DMA because of their ability to affect a large number of users, which entails a risk of unfair business practices (see Recital 14). Affecting many users

also means affecting a large part of European society. All these CPSs have in common that they can map society in the digital world, figuratively speaking, thereby representing a digital copy of social conditions in the analogue world. Therefore, the real social condition is inextricably linked to its digital counterpart. For instance, online social networking is legally defined in Art. 2(7) DMA, as a platform that enables end users to connect and communicate with each other, share content, and discover other users and content across multiple devices and, in particular, via chats, posts, videos, and recommendations. In short, the service must cumulatively have contact, content-sharing, and discovery functions—thereby mirroring real-world behaviour. So far, Facebook, Instagram, LinkedIn and TikTok have been identified as this type of CPS. By definition, they all have a significant de facto influence on social life in the digital space. It was not for nothing that the EC at the beginning of this Chapter boldly demanded that the same should apply in the offline and online world. Overall, the legislator also considered social aspects when deciding on the CPSs.

5. Conclusion & considerations for further (interdisciplinary) research

> *"'Boy, make the jacket for me, and patch the trousers, or I will hit you across your ears with a yardstick! I have struck down seven with one blow, killed two giants, led away a unicorn, and captured a wild boar, and I am supposed to be afraid of those who are standing just outside the bedroom!' When those standing outside heard the tailor say this, they were so overcome with fear that they ran away, as though the wild horde was behind them. None of them dared to approach him ever again." (Note: This is the end of the fairy tale The Brave Little Tailor; Ashliman, 2005)*

At the end of his fairy tale, the brave little tailor once again had to use cunning (and luck) to defeat all of his opponents. The young king's daughter had just married him when she learned of his true origins and realised that they had made a king out of a tailor. She complained to her father, the old king, and asked for his help. Yet the king's armour-bearer, who had overheard this conversation, was favourably disposed towards the young man and told him of the attack the old king was preparing. "I'll put a stop to that," said the little tailor (Ashliman, 2005), and, fortunately, he did. It is hoped that the DMA will also be a success for the EC in its fight against the machinations of the big platform undertakings. For social as much as economic reasons, this success story must not go as far as the end of "The Brave Little Tailor" and drive those undertakings out of the EU. The respective gatekeepers have already become essential to the

EU's analogue and digital society. Nevertheless, the previous discussion has shown that the DMA weighs the economic advantages of the gatekeepers against the common good of society, with the latter outweighing the former. However, it would be wrong to assume that the DMA is a Regulation with an explicitly social character or explicitly formulated objectives. Rather, the DMA is a Regulation with several *implicit* social aspects that form its social character. Such implicit social aspects include, for example, the legislative recitals, the beneficiaries of the Regulation, certain CPS, and the objectives of the DMA. Further research is needed in line with the *practical approach* developed in this Chapter. Therefore, this Chapter, written primarily from a legal perspective, would like to invite social scientists to explore the social aspects of the Regulation further. As shown, the social science perspective on law is particularly underrepresented in research. The DMA can provide a starting point for further research, but the underlying problem is, of course, more comprehensive and can be applied 1:1 to other legal texts. Just as the law consumes social science as a trend-setting discourse to supplement its worldview, so too can the reverse be enriching if one is open to the similarly foreign (like the brave little tailor with the cheese and the stone). Possible further interdisciplinary research questions might include the following:

- Should the DMA promote social issues?
- When are the DMA's objectives fair and contestable for society?
- What factors in the DMA most influence the behaviour of gatekeepers?
- How does the designation as a gatekeeper influence the behaviour of other undertakings in digital markets?
- How aware are the beneficiaries of the DMA of the rights and obligations introduced by the Regulation?
- How does the DMA affect consumer trust in digital platforms?
- How does the DMA affect marginalized groups and their ability to participate in digital markets?
- What are the challenges in enforcing the DMA across diverse national contexts within the European Union?
- What role do non-EU countries play in shaping or responding to the DMA as a regulatory model?

In this context, the question of the relationship between law and the social sciences, as well as the influence of society on law in general, must also be considered. As outlined, this relationship depends on, among other things, the circumstances and the attitude of the observer. Even as interdisciplinary

research on the DMA is desired, a unanimous opinion can never be reached. However, this can also be an advantage. Therefore, the following should be noted in the spirit of the underlying fairy tale: If the brave little tailor continues to defend himself against the digital giants successfully, the idea of a fair and contestable digital market will still be alive tomorrow. These successes could pave the way for further legal acts with an (implicit or—to take a bold step further—even explicit) social character that could benefit (European) society as a whole.

References

'Apple v. EU Commission' (2024a) Case no. T-1079/23. *Official Journal of the EU* C/2024/562, 8 January 2024 [Online]. Available at: http://data.europa.eu/eli/C/2024/562/oj (Accessed: 27 January 2025).

'Apple v. EU Commission' (2024b) Case no. T-1080/23 *Official Journal of the EU* C/2024/563, 8 January 2024 [Online]. Available at: http://data.europa.eu/eli/C/2024/563/oj (Accessed: 27 January 2025).

'Basic Law for the Federal Republic of Germany' (2024) in the revised version published in the Federal Law Gazette Part III, classification number 100-1, as last amended by the Act of 20 December 2024 [Online]. *Federal Law Gazette* 2024 I, no. 439. Available at: https://www.gesetze-im-internet.de/englisch_gg/englisch_gg.html (Accessed: 27 January 2025).

'BVerfG' (2020) Case no. 1 BvR 3214/15, ECLI:DE:BVerfG:2020:rs20201110.1bvr321415.

'ByteDance Ltd v. EU Commission' (2024a) Case no. T-1077/23, ECLI:EU:T:2024:478.

'ByteDance Ltd v. EU Commission' (2024b) Case no. C-627/24 P. *Official Journal of the EU* C/2024/6639, 11 November 2024 [Online]. Available at: https://eur-lex.europa.eu/eli/C/2024/6639/oj/eng (Accessed: 27 January 2025).

'Das Erste Buch Sozialgesetzbuch – Allgemeiner Teil – (Artikel I des Gesetzes vom 11. Dezember 1975, BGBl. I S. 3015), das zuletzt durch Artikel 4 des Gesetzes vom 19. Juli 2024 geändert worden ist' (2024) [Online]. *BGBl. 2024 I Nr. 245*. Available at: https://www.gesetze-im-internet.de/sgb_1/SGB_1.pdf (Accessed: 27 January 2025).

'Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services' (2015), *Official Journal of the EU* L241/1 [Online]. Available at: http://data.europa.eu/eli/dir/2015/1535/oj (Accessed: 27 January 2025).

'Fédération Charbonnière de Belgique v. High Authority of the European Coal and Steel Community' (1956) Case no. 8-55, ECLI:EU:C:1956:11.

'Gesetz gegen Wettbewerbsbeschränkungen in der Fassung der Bekanntmachung vom 26. Juni 2013 (*BGBl. I S. 1750, 3245*), das zuletzt durch Artikel 6 des Gesetzes vom 5. Dezember 2024 (*BGBl. 2024 I Nr. 400*) geändert worden ist' (2024) [Online]. Available at: https://www.gesetze-im-internet.de/gwb/GWB.pdf (Accessed: 27 January 2025).

'Internationale Handelsgesellschaft mbH v. Einfuhr- und Vorratsstelle für Getreide und Futtermittel' (1970) Case no. 11-70, ECLI:EU:C:1970:114.

'Meta Platforms v. EU Commission' (2024) Case no. T-1078/23, ELI: http://data.europa.eu/eli/C/2024/561/oj, OJEU C/2024/561, 8 January 2024.

'Proposal for a Regulation of the European Parliament and of the Council on contestable and fair markets in the digital sector (Digital Markets Act)' (2020) COM/2020/842 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52020PC0842 (Accessed: 27 January 2025).

'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)' (2022) *Official Journal of the EU* L265/1, 12 October [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925 (Accessed: 27 January 2025).

'Treaty on European Union' (2012) *Official Journal of the EU* C 326/13, 26 October [Online]. Available at: https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF (Accessed: 27 January 2025).

Ashliman, D. L. (2005) *The Brave Little Tailor*. The Grimm Brothers' Children's and Household Tales (Grimms' Fairy Tales) compiled, translated, and classified by D. L. Ashliman [Online]. Available at: https://sites.pitt.edu/~dash/grimm020.html (Accessed: 27 January 2025).

Bluhm, L. (2023) 'Volksmärchen – Buchmärchen – Kunstmärchen' in Bluhm, L. and Neuhaus, S. (eds.) *Handbuch Märchen*. Berlin: J.B. Metzler, pp. 3–8.

Bongartz, P. and Kirk, A. (2024) 'Art. 2 DMA - XXI. Business user (No. 21) (Rn. 102–108)' in Podszun, R. (ed.) *Digital Markets Act – article-by-article commentary*. London: Bloomsbury Publishing, Rn. 107.

Bornstein, B.H. (2016) 'Law and social science: how interdisciplinary is interdisciplinary enough?' in Willis-Esqueda, C. and Bornstein, B.H. (eds.) *The witness stand and Lawrence S. Wrightsman, Jr.* New York: Springer Science+Business Media, pp. 113–128.

Bradford, A. (2020) *The Brussels effect: how the European Union rules the world*. New York: Oxford University Press.

Breton, T. (2020) *Europe fit for the digital age: Commission proposes new rules for digital platforms*. European Commission [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2347 (Accessed: 27 January 2025).

Bueren, E. and Weck, T. (2023) 'Art. 3 DMA Benennung von Torwächtern' in Säcker, J., Bien, F., Meier-Beck, P. and Montag, F. (eds.) *MüKoEuWettbR, DMA*. 4th ed. München: C.H. Beck, Rn. 54.

Carpi, D. and Leiboff, M. (2016) *Fables of the law: fairy tales in a legal context*. Berlin, Boston: De Gruyter.

Crémer, J. et al. (2023) 'Fairness and contestability in the Digital Markets Act', *Yale Journal on Regulation*. Vol. 40(973), pp. 973–1012.

Derber, M. (1963) 'What The Lawyer Can Learn From Social Science', *Journal of Legal Education*. Vol. 16(2), pp. 145–154.

Diederichsen, U. (2008) *Juristische Strukturen in den Kinder- und Hausmärchen der Brüder Grimm*. Kassel: Unidruckerei der Universität Kassel.

Doddridge, Sir J. (1631) *The English lawyer* [Online]. London: Assignes of I. More. Available at: https://archive.org/details/bim_early-english-books-1475-1640_the-english-lawyer_doddridge-sir-john_1631 (Accessed: 27 January 2025).

European Commission (2023) *Communication from the EU Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – 2023 Digital Compass: the European way for the digital decade*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0118 (Accessed: 27 January 2025).

Eurostat (2024) *Population on 1 January 2024* [Online]. Available at: https://ec.europa.eu/eurostat/databrowser/view/demo_pjan/default/table?lang=en (Accessed: 27 January 2025).

Frey, D., Berthold, V. and Bürgle N. (2023) 'Sozialwissenschaften' in Bluhm, L. and Neuhaus, S. (eds.) *Handbuch Märchen*. Berlin: J.B. Metzler, pp. 541–545.

Geiger, T. (1987) *Vorstudien zu einer Soziologie des Rechts*. 4th ed. Berlin: Duncker & Humblot.

Göhsl, J.-F. and Zimmer, D. (2025) 'Art. 5 – Grundlagen' in Immenga, U. and Mestmäcker, E.-J. (eds.) *Wettbewerbsrecht*. München: C.H. Beck, Rn. 2, 3.

Graef, I. (2024) 'Regulating digital platforms: Streamlining the interaction between the Digital Markets Act and national competition regimes' in Graef, I. and van der Sloot, B. (eds.) *The legal consistency of technology regulation in Europe*. Oxford: Hart Publishing, pp. 157–176.

Grimm, J. and Grimm, W. (1812) 'Von einem tapfern Schneider'. *Kinder- und Hausmärchen (KHM no. 20)*. Band 1. Berlin: in der Realschulbuchhandlung. pp. 77–88. [Online]. Available at: https://www.deutschestextarchiv.de/book/show/grimm_maerchen01_1812 (Accessed: 27 January 2025).

Gryllos, G. (2024) 'The New Digital Landscape: Interaction between the DMA and Rules of national and EU law governing the conduct of gatekeepers', *Concurrences - Revue des droits de la concurrence - Competition Law Review*. no. 1-2024, pp. 40–56.

Habermas, J. (1992) *Faktizität und Geltung Beiträge zur Diskurstheorie des Rechts und des demokratischen Rechtsstaats*. Berlin: Suhrkamp.

Herrmann, L. and Kestler, L. (2024) 'Wettbewerbsrechtliche Herausforderungen durch international heterogene Gatekeeper-Regulierung – Plädoyer für ein strategisches Umdenken' in Buchheim, J., Steinröter, B., Kraetzig, V. and Mendelsohn, J.K. (eds.) *Plattformen – Grundlagen und Neuordnung des Rechts digitaler Plattformen*. Baden-Baden: Nomos, pp. 143–162.

Hoffmann, J., Herrmann, L. and Kestler, L. (2024) 'Gatekeeper's potential privilege – the need to limit DMA centralisation', *Journal of Antitrust Enforcement*, 12(1), pp. 126–147.

Hopt, K.J. (1975) 'Was ist von den Sozialwissenschaften für die Rechtsanwendung zu erwarten?', *JuristenZeitung*. 30. Jahrgang, no. 11/12, pp. 341–349.

Huerkamp, F. and Nuys, M. (2024) 'Art. 18 DMA Proportionality stricto sensu' in Podszun, R. (ed.) *Digital Markets Act – article-by-article commentary*. London: Bloomsbury Publishing, Rn. 34.

Kähler, L. (2018) 'Die asymmetrische Interdisziplinarität der Rechtswissenschaft' in Rehberg, M. (ed.), *Der Erkenntniswert von Rechtswissenschaft für andere Disziplinen.* Wiesbaden: Springer, pp.107–151.

Käseberg, T. and Gappa, S. (2024) 'Art. 1 DMA Objectives of the DMA' in Podszun, R. (ed.) *Digital Markets Act – article-by-article commentary*. London: Bloomsbury Publishing, Rn. 5.

Kißler, L. (1984) *Recht und Gesellschaft – Einführung in die Rechtssoziologie*. Stuttgart: UTB.

König, M. (2023a) 'Art. 1 DMA Bestreitbare und faire Märkte als Normzweck' in Säcker, J., Bien, F. Meier-Beck, P. and Montag, F. (eds.) *MüKoEuWettbR, DMA.* 4th ed. München: C.H. Beck, Rn. 4 ff.

König, M. (2023b) 'Einleitung' in Säcker, J., Bien, F. Meier-Beck, P. and Montag, F. (eds.) *MüKoEuWettbR, DMA*. 4th ed. München: C.H. Beck, Rn. 25, 26.

Lehner, F. (2011) *Sozialwissenschaft*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Lenaerts, K. (2021) *Proportionality as a matrix principle promoting the effectiveness of EU law and the legitimacy of EU action* [Online]. Available at: https://www.ecb.europa.eu/press/conferences/shared/pdf/20211125_legal/ECB-Symposium_on_proportionality_25_November_2021.en.pdf (Accessed: 27 January 2025).

Lox, H., Lutkat, S. and Kluge, D. (eds.) (2007) *Dunkle Mächte im Märchen und was sie bannt - Recht und Gerechtigkeit im Märchen. Forschungsbeiträge aus der Welt der Märchen.* Vol. 32. Kiel: Königsfurt-Urania Verlag.

Luhmann, N. (1995) *Das Recht der Gesellschaft*. Frankfurt am Main: Suhrkamp [Online]. Available at: https://luhmann.ir/wp-content/uploads/2021/07/Das-Recht-der-Gesellschaft.pdf (Accessed: 27 January 2025).

Luhmann, N. (1999) 'Recht als soziales System', *Zeitschrift für Rechtssoziologie*. Vol. 20(1), pp. 1–13.

Madiega, T. (2022) *Digital Markets Act, briefing EU legislation in progress*. European Parliament [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690589/EPRS_BRI(2021)690589_EN.pdf (Accessed: 27 January 2025).

Meta Platforms Inc. (2024) *Facebook monthly active users (MAU) in Europe as of 4th quarter 2023 (in million MAU).* Statista [Online]. Available at: https://www.statista.com/statistics/745400/facebook-europe-mau-by-quarter/ (Accessed: 27 January 2025).

Moreno Belloso, N. and Petit, N. (2023) 'The EU Digital Markets Act (DMA): A Competition Hand in a Regulatory Glove', *European Law Review.* Vol. 48, no. 4, pp. 391–421.

Müller, L. (1985) *Das tapfere Schneiderlein – List als Lebenskunst*. Freiburg im Breisgau: Verlag Kreuz.

Once upon a Law (2022) [Online]. Available at: https://onceuponalaw.org/ (Accessed: 27 January 2025).

Parajuli, G. and Lamicchane, B.P. (2019) 'Social function of law from jurisprudential outlook', *Nepal Law Review*, Vol. 28(1–2), pp. 140–158 [Online]. Available at: https://www.nepjol.info/index.php/nlr/article/view/57526 (Accessed: 27 January 2025).

Pfeifer, W. et al. (1993) *sozial.* Digitales Wörterbuch der Deutschen Sprache [Online]. Available at: https://www.dwds.de/wb/etymwb/sozial (Accessed: 27 January 2025).

Podszun, R. (2023) 'From competition law to platform regulation – regulatory choices for the Digital Markets Act', *Economics*, 17(1) [Online]. Available at: https://www.degruyter.com/document/doi/10.1515/econ-2022-0037/html#Harvard (Accessed: 27 January 2025).

Pöge-Alder, K. (2023a) 'Forschungsgeschichte' in Bluhm, L. and Neuhaus, S. (eds.) *Handbuch Märchen*. Berlin: J.B. Metzler, pp. 529–533.

Pöge-Alder, K. (2023b) 'Mündliches Erzählen' in Bluhm, L. and Neuhaus, S. (eds.) *Handbuch Märchen*. Berlin: J.B. Metzler, pp. 445–451.

Pötzsch, H. (2009) *Die Deutsche Demokratie*. 5th ed. Bonn: Bonifatius Verlag.

Rehbinder, M. (1973) 'Die gesellschaftlichen Funktionen des Rechts' in Albrecht, G., Daheim, H. and Sack, F. (eds.) *Soziologie – Sprache, Bezug zur Praxis, Verhältnis zu anderen Wissenschaften.* Opladen: Westdeutsche Verlag, pp. 354–368.

Robertson, Viktoria H.S.E (2024) 'The complementary nature of the Digital Markets Act and the EU antitrust rules', *Journal of Antitrust Enforcement.* 12(2), pp. 325–330.

Rosenstock, J., Singelnstein, T. and Boulanger, C. (2019) 'Versuch über das Sein und Sollen der Rechtsforschung. Bestandsaufnahme eines interdisziplinären Forschungsfeldes' in Boulanger, C., Rosenstock, J. and Singelnstein, T. (eds.) *Interdisziplinäre Rechtsforschung – Eine Einführung in die geistes- und sozialwissenschaftliche Befassung mit dem Recht und seiner Praxis*. Wiesbaden: Springer, pp. 3–29.

Rottleuthner, H. (2021) 'Rechtswissenschaft als Sozialwissenschaft' in Hilgendorf, E. and Joerden, J.C. (eds.) *Handbuch Rechtsphilosophie.* 2nd ed. Berlin: J.B. Metzler, pp. 264–266.

Shapiro, F.R. and Pearse M. (2012) 'The most-cited law review articles of all time', *Michigan Law Review*, Vol. 110(8), pp. 1483–1520.

Siegel, D.M. and McDaniel, S.H. (1991) 'The Frog Prince: tale and toxicology', *American Journal of Orthopsychiatry*, Vol. 61(4), pp. 558–562.

Vestager, M. (2020) 'Europe fit for the Digital Age: Commission proposes new rules for digital platforms'. *EU Commission press release of 15 December 2020* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/de/ip_20_2347 (Accessed: 27 January 2025).

Wienbracke, M. (2013) 'Der Verhältnismäßigkeitsgrundsatz'. *Zeitschrift für das Juristische Studium (ZJS)*, Vol. 2, pp. 148–155.

Wuchty, S., Jones, B.F. and Uzzi, B. (2007) 'The increasing dominance of teams in production of knowledge', *Science*, Vol. 316(5827), pp. 1036–1039.

Zacher, H.F. (1981) 'Sozialrecht und soziale Marktwirtschaft' in Gitter, W., Thieme, W. and Zacher, H.F. (eds.) *Im Dienste des Sozialrechts – Festschrift für Georg Wannagat zum 65. Geburtstag am 26. Juni 1981*. Köln: Carl Heymanns Verlag, pp. 715–762.

Eyes Shut, Fingers Crossed: The EU's Governance of Terrorist Content Online under Regulation 2021/784

Valerie Albus

Abstract

This chapter introduces the legislative background, key provisions, and main academic debates surrounding the EU's Terrorist Content Online Regulation (TCO Regulation). The TCO Regulation was the first EU instrument to introduce legally binding rules for hosting service providers regarding the moderation of illegal content, thereby paving the way for subsequent EU Regulations, such as the Digital Services Act. The TCO Regulation establishes a new set of responsibilities for hosting service providers. On the one hand, they must respond to removal orders issued by national competent authorities and take down terrorist content within one hour. On the other, hosting service providers must take preventive measures to ensure that terrorist content remains off their platform, thereby contributing to the prevention of radicalisation and, potentially, terrorist acts. Regrettably, the modalities of the TCO Regulation may undervalue the complex assessments required to determine whether a text, image, or video constitutes terrorist content. Short deadlines and high fines, along with the fact that some Member States do not require a judicial review to issue removal orders, raise concerns regarding the over-removal of content and related risks for fundamental rights. At the same time, the limited transparency obligations for hosting service providers are a missed opportunity to assert public oversight over platforms' (often automated) content moderation practices. While the EU's push for increased responsibility may have prompted hosting service providers to intensify their fight against terrorist content, the TCO Regulation created a system in which the EU Member States choose to remain ignorant as to how this is achieved.

1. Introduction

The spread of terrorist content on online platforms has become a significant security concern over the past decade. Terrorist groups have exploited social media and video-hosting services to disseminate their messages and recruit new followers. Over time, not only the radicalisation of individuals, but also terrorist acts themselves have become more internet-centric. The most recognised example is the 2019 terrorist attack in Christchurch, New Zealand, in which 51 people were murdered and many more injured. Prior to the attack, the perpetrator published a manifesto online and livestreamed the shooting using Facebook Live. This reignited discussions among policymakers about the role of online platforms in the planning and execution of terrorist acts.

Around the same time, over 18,000 kilometres away, the EU institutions in Brussels were negotiating Regulation 2021/784, better known as the Terrorist Content Online Regulation (hereafter, the TCO Regulation). One year earlier, the European Commission tabled its proposal for a Regulation to introduce legally binding rules for hosting service providers on how to deal with terrorist content. The proposal aimed to create so-called removal orders that would allow national competent authorities to compel hosting service providers to remove any such content within one hour. The Regulation's scope aimed to encompass all service providers that enable users to store and disseminate content to the public. This includes social media platforms, such as Facebook, Instagram, and X, as well as video-sharing services like YouTube or Twitch.

After lengthy negotiations, the TCO Regulation was adopted on 29 April, 2021, and became applicable on 7 June, 2022. It now applies to all hosting service providers operating within the EU, irrespective of their place of main establishment (Art. 1(2) TCO Regulation). This includes service providers that are based outside of the EU but provide their services to European users. This approach has allowed the EU to govern the moderation of terrorist content beyond its borders.

The TCO Regulation appeals to the "particular societal responsibilities" of hosting service providers (Recital 5 TCO Regulation). These are expressed in several new duties that such providers must fulfil in order to protect their users from terrorist content. Aside from actualising the aforementioned removal orders, hosting service providers are required to take preventive measures to ensure that their services are not being misused to spread terrorist content. Consequently, hosting service providers

have become the protagonists in the fight against terrorist content: It is primarily *their* responsibility to choose and implement the technological solutions needed to ensure that their platforms stay "clean". Accordingly, their role transcends mere compliance, in that it also involves proactive enforcement, similar to that of public authorities (Tosza, 2021, p. 16). This has prompted scholars to examine the broader shifts in the enforcement landscape brought about by the TCO Regulation, considering that it fosters new modes of EU security integration (Bellanova and De Goede, 2021).

Certainly, even before the TCO Regulation entered into force, many hosting service providers already moderated user-uploaded content, thereby placing limits on freedom of expression and public participation online (Jørgensen and Pedersen, 2017). The novelty of the TCO Regulation is that, for the first time, the EU legislator defined *what* content should be removed and *how*. This has naturally generated discussions on whether the EU has struck the right balance between enlisting hosting service providers in the fight against terrorist content and safeguarding users' fundamental rights to freedom of expression and information.

Being *the first of its kind* makes the TCO Regulation a particularly interesting object of study. The Regulation created path-dependencies, determining the course of EU governance of illegal content more broadly. For example, removal orders were conceived in the Regulation's elaboration and have since inspired similar provisions in the Digital Services Act (DSA)[1] and sectoral legislation. To a certain extent, the TCO Regulation thereby pioneered the growing EU framework that aims to increase accountability of online service providers vis-à-vis European users.

This chapter aims to provide an introduction to the legislative text, covering its legislative history, main innovations, and key provisions. It begins with a broad overview of the background and scope of the Regulation (Section 1), followed by a detailed examination of its most important provisions (Section 2). Throughout the chapter, reference is made to the main scholarly debates surrounding the TCO Regulation, focusing on the role of hosting service providers in law enforcement and related fundamental rights concerns. Additionally, relying on the first transparency reports of

1 For more information on the DSA, see Chapter 4 'The Digital Services Act: Online Risks, Transparency and Data Access' by Marie-Therese Sekwenz and Rita Gsenger. Also, see Chapter 5, 'The Digital Services Act – an appropriate response to online hate speech?' by Pascal Schneiders and Lena Auler.

Facebook and Google, the chapter offers some (limited) empirical insights into the Regulation's first two years of application.

2. Overview

The following overview highlights several milestones in the legislative history of the TCO Regulation (1.1) before contextualising its legal basis in the EU Treaties (1.2), its scope of application (1.3), and the definition of terrorist content (1.4).

2.1 Legislative history

Against the backdrop of a heightened terrorist threat in Europe during the 2010s and concerns over terrorist propaganda acting as a "catalyst" for radicalisation (Recital 5 TCO Regulation), it is somewhat unsurprising that the first EU legislative proposal tackling illegal content focused on the dissemination of terrorist content. It is important to note that the TCO Regulation did not fill a complete legislative vacuum at the time. Several EU instruments regulating specific aspects of illegal content were already in place prior to its proposal and adoption.

Most importantly, Directive 2000/31/EC on electronic commerce ("the e-commerce Directive") had already harmonised the conditions under which intermediaries could be held liable for hosting illegal content, including terrorist content. Article 14 of the e-commerce Directive set out the general principle: Providers of intermediary services were exempt from liability in the EU if they did not have actual knowledge of illegal activity or information on their platforms and, upon obtaining such knowledge, acted expeditiously to remove or disable access to this information.[2]

In addition, sectoral legislation, such as Directive 2018/1808 on audiovisual media services and Directive 2011/93/EU to combat the sexual abuse and exploitation of children and child pornography, had been adopted earlier during the 2010s. However, these Directives did not create legally binding obligations for hosting service providers to act against illegal content, but merely laid down common definitions and minimum standards to be implemented by Member States.

2 This principle is now also enshrined in Art. 6(1) of the DSA. For further reading on the EU's system of intermediary liability, see Frosio (2020) and Wilman (2020).

After initial efforts to enhance voluntary cooperation between EU Member States and hosting service providers, such as through the EU Internet Forum launched by the European Commission in 2015 (see Mitsilegas and Salvi, 2024, p. 192), the idea of a binding EU instrument to counter illegal content began gaining traction in 2017. The European Commission first issued Communication COM/2017/0555 on 28 September, 2017, which outlined guidelines and principles to enhance the responsibility of online platforms for illegal content. This communication placed special emphasis on the business dimension of illegal content and how such content was undermining users' trust in the digital single market. The Commission maintained that, as gatekeepers of content and information, online platforms had a societal responsibility to prevent criminals from exploiting their services to spread illegal content (Communication COM/2017/0555, p. 2).

The idea of a societal responsibility of online service providers was adopted in Commission Recommendation 2018/334 of 1 March, 2018, on measures to effectively tackle illegal content online. In short, the recommendation concluded there to be a need for the EU legislator to harmonise the rules on combatting illegal content online. The Commission thus set the scene for the very broad scope of its future legislative action: The Recommendation defined illegal content as *any* information that does not comply with EU or Member States' law. Recommendation 2018/334 also stressed that online service providers should systematically enhance their cooperation with Member State authorities, such as by establishing effective points of contact and fast-track procedures to remove illegal content upon request (Recommendation 2018/334, 2018, point 22). It should be recalled here that recommendations have no binding force, but merely allow EU institutions to suggest a line of action without imposing any legal obligations.

In parallel with these efforts at the EU level, several Member States had already unilaterally adopted legislation tackling illegal content online. For instance, the German Network Enforcement Act (2017) required online platforms to delete manifestly unlawful content within 24 hours. Likewise, France adopted the Avia Law (2020), which obliged platforms to remove a range of illegal online content, and especially hate speech. However, this law was later declared to be largely unconstitutional by the French Constitutional Council.[3] The principal drawback of these national initiatives was their limited geographical scope. To ensure effective cooperation between

3 See the decision of the French Constitutional Council n° 2020-801 DC of 18 June, 2020.

the law enforcement authorities and online service providers of different countries, it was necessary to agree on an EU-wide solution.

On 12 September, 2018, the European Commission presented its proposed Regulation COM/2018/640 to counter the dissemination of terrorist content online. After lengthy interinstitutional negotiations spanning six trilogues, the TCO Regulation was finally adopted on 29 April, 2021, and became applicable on 7 June, 2022.

2.2 Legal basis

The TCO Regulation was adopted on the basis of Article 114 of the Treaty on the Functioning of the European Union (TFEU), which lays down the procedure under which the European Parliament and the Council may adopt harmonising measures which "have as their object the establishment and functioning of the internal market".

This choice may seem unexpected, especially as the TCO Regulation heavily draws from substantive criminal law and contributes to enforcing corresponding standards in the digital sphere. The legal basis may seem all the more surprising considering that, since the adoption of the Lisbon Treaty, the EU legislator has been empowered to approximate Member States' criminal procedures and harmonise substantive criminal law (Art. 82 and 83 of the TFEU; see Mitsilegas, 2016). So, why did the European Commission put forward a legal basis for the internal market to adopt the TCO Regulation?

The Commission had to make pragmatic choices when drafting the TCO Regulation. Although Art. 82 of the TFEU empowers the EU to adopt minimum rules in the area of criminal procedure, such measures must be based on the principle of mutual recognition of judgments (De Pasquale and Pesce, 2021). Put simply, this principle requires judicial authorities to automatically recognise and execute judicial decisions emanating from other Member States in the same manner as a domestic decision.[4] For example, if a French court issues a European arrest warrant for a person residing in Germany, the German authorities must recognise this decision and surrender the person to France.

As the main purpose of the TCO Regulation was to create duties for *service providers*, the proposal would not have fit in with the mutual recog-

4 For a comprehensive analysis of the principle of mutual recognition in EU law, see Janssens (2013).

nition framework, which relies on cooperation between *judicial authorities* – courts and public prosecutors. In other words, the TCO Regulation would have been an entirely different instrument if it had been adopted under the EU's framework for criminal law.

Aside from these constraints, some additional reasons render the question of the legal basis important from the perspective of the Member States. By virtue of Protocols 21 and 22, Ireland benefits from special opt-out privileges and Denmark is to be automatically excluded from Title V measures, which cover criminal law cooperation (Protocol 21 on the position of the United Kingdom and Ireland in respect of the Area of Freedom Security and Justice; Protocol 22 on the position of Ireland). Thus, by adopting the TCO Regulation on the basis of Art. 114 TFEU, the EU ensured that it would become applicable in all Member States – including Ireland, where many online platforms have their European headquarters.

Consequently, to adopt the Regulation on the legal basis of Art. 114 of the TFEU, the crime prevention goal of the measure was subordinated to the objective of promoting a safe digital single market. Mitsilegas (2016) described this phenomenon as a "functional criminal law spill-over from Title V to other parts of the Treaty" (p.6). This spill-over consists of criminal law measures being adopted under the institutional rules of other policy fields to circumvent the constraints inherent in Title V. The TCO Regulation appears to constitute an example of such a spill-over.

Therefore, when reading the legislative text, one gets the impression that the TCO Regulation awkwardly sits in two chairs. On the one hand, it builds on substantive criminal law and stresses that it should contribute "to achieve the sustained prevention of radicalisation in society" (Recital 2 TCO Regulation). On the other, the Regulation has an internal market rationale, emphasising that a European approach to combatting terrorist content is essential for protecting the functioning of the digital single market.

2.3 Scope of application

Pursuant to Art. 1(2), the TCO Regulation "applies to hosting service providers offering services in the Union, irrespective of their place of main establishment, insofar as they disseminate information to the public". Thus, the Regulation's scope centres around three different notions: "hosting",

"offering services in the Union", and "disseminating information to the public".

According to Art. 2(1) "hosting" consists of the "storage of information provided by and at the request of a content provider". Providers of social media (e.g., Facebook, LinkedIn, X) and video, image, and audio-sharing services (e.g., YouTube, Instagram) are thus covered by the Regulation's scope. In addition, the recitals state that the TCO Regulation should cover file-sharing and other cloud services insofar as these are used to make the stored information available to the public at the direct request of the user (Recital 14 TCO Regulation). The recitals also specify that interpersonal communication services, such as email or private messaging, should fall outside the scope of the Regulation (Recital 14). However, these recitals are not legally binding and only provide interpretative guidance. If the meaning of a provision in the TCO Regulation is unclear, it is ultimately the task of national courts and the Court of Justice of the European Union (CJEU) to rule on its applicability in a given case.

The notion of "offering services in the Union" should be understood as "enabling natural or legal persons in one or more Member States to use the services of a hosting service provider which has a substantial connection to that Member State or those Member States" (Art. 2(4) TCO Regulation). The notion of "substantial connection" refers to the connection of a hosting service provider with one or more Member States resulting either from its place of establishment or from specific factual criteria (Art. 2(5) TCO Regulation). Such factual criteria include having a significant number of users in one or more Member States or the targeting of its activities to one or more Member States.

This results in a very broad geographical scope of application. The Regulation covers not only hosting service providers established in the EU, but also those in third countries. The goal of this broad scope is to ensure that all hosting service providers operating in the EU's digital single market are subject to the same requirements, regardless of their country of main establishment (Recital 15 TCO Regulation). This also allows the EU to govern beyond its borders and set a potentially global regulatory standard.

Finally, "dissemination to the public" refers to "the making available of information, at the request of a content provider, to a potentially unlimited number of persons" (Art. 2(3) TCO Regulation). The Regulation's recitals provide further guidance on this notion. Indeed, they state that this should entail "making the information easily accessible to users in general, without requiring further action by the content provider, irrespective of whether

those persons actually access the information in question" (Recital 14 TCO Regulation).

2.4 Definition of terrorist content

Art. 2(7) establishes what types of material should be considered terrorist content for the purpose of the TCO Regulation. It refers to material which:

(a) incites the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541, where such material, directly or indirectly, such as by the glorification of terrorist acts, advocates the commission of terrorist offences, thereby causing a danger that one or more such offences may be committed;
(b) solicits a person or a group of persons to commit or contribute to the commission of one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
(c) solicits a person or a group of persons to participate in the activities of a terrorist group, within the meaning of point (b) of Article 4 of Directive (EU) 2017/541;
(d) provides instruction on the making or use of explosives, firearms or other weapons or noxious or hazardous substances, or on other specific methods or techniques for the purpose of committing or contributing to the commission of one of the terrorist offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541;
(e) constitutes a threat to commit one of the offences referred to in points (a) to (i) of Article 3(1) of Directive (EU) 2017/541.

The relevant offences to which the TCO Regulation refers are laid down in Directive 2017/541 on combating terrorism ("Terrorism Directive"). This Directive establishes minimum rules regarding the definition of terrorist offences and penalties, and harmonised victims' rights in the EU. Art. 3(1) (a) to (i) of the Directive defines the relevant terrorist offences:

1. Member States shall take the necessary measures to ensure that the following intentional acts, as defined as offences under national law, which, given their nature or context, may seriously damage a country or an international organisation, are defined as terrorist offences where committed with one of the aims listed in paragraph 2:

(a) attacks upon a person's life which may cause death;
(b) attacks upon the physical integrity of a person;
(c) kidnapping or hostage-taking;
(d) causing extensive destruction to a government or public facility, a transport system, an infrastructure facility, including an information system, a fixed platform located on the continental shelf, a public place or private property likely to endanger human life or result in major economic loss;
(e) seizure of aircraft, ships or other means of public or goods transport;
(f) manufacture, possession, acquisition, transport, supply or use of explosives or weapons, including chemical, biological, radiological or nuclear weapons, as well as research into, and development of, chemical, biological, radiological or nuclear weapons;
(g) release of dangerous substances, or causing fires, floods or explosions, the effect of which is to endanger human life;
(h) interfering with or disrupting the supply of water, power or any other fundamental natural resource, the effect of which is to endanger human life;
(i) illegal system interference, as referred to in Article 4 of Directive 2013/40/EU of the European Parliament and of the Council [...] in cases where Article 9(3) or point (b) or (c) of Article 9(4) of that Directive applies, and illegal data interference, as referred to in Article 5 of that Directive in cases where point (c) of Article 9(4) of that Directive applies.

For the purpose of Art. 2(7)(c) of the TCO Regulation, which defines as terrorist content any material which "solicits a person or a group of persons to participate in the activities of a terrorist group", a terrorist group's activities are defined in reference to Art. 4(b) of the Directive:

> (b) participating in the activities of a terrorist group, including by supplying information or material resources, or by funding its activities in any way, with knowledge of the fact that such participation will contribute to the criminal activities of the terrorist group.

Scheinin (2019) was highly critical of the EU legislator's choice to define terrorist content with reference to the Terrorism Directive. He argued that the Directive's definitions were conceived for the evidence-based adversarial process of a criminal trial and cannot serve, at the same time, for administrative decisions ordering the removal of online content. The Directive's definitions contain such elements as "intent" or "aim", or require proof

that a person had "knowledge" of the fact their participation would contribute to the criminal activities of a terrorist group. According to Scheinin (2019), whether these criteria are fulfilled in an individual case cannot be determined by reference to the text, video, or image alone, but requires a careful contextual assessment, including evidence beyond the piece of content itself. The fact that the TCO Regulation completely disregards this complexity creates significant risks for freedom of expression and information.

Similarly, Mitsilegas and Salvi (2024) shed light on the "digital exceptionalism" underlying the TCO Regulation. Their in-depth analysis demonstrates that the EU's regulatory approach to governing terrorist content online has departed from the criminalisation of illegal speech in the offline environment. The authors show that the Regulation over-criminalises online speech through broad definitions of terrorist offences and content, which risks undermining the principles of legality and proportionality. At the same time, this approach results in an increased risk of over-removal and ultimately comes at the expense of freedom of expression and information.

In practice, it is not always straightforward to determine what material falls within the Regulation's scope. Art. 1(3) of the Regulation excludes material disseminated for educational, journalistic, artistic, research, or awareness-raising purposes from its scope. In many cases, intention and context are thus determining factors. In addition, radical, polemic, or controversial views that are expressed in the context of public debate on sensitive political questions should also not be considered terrorist content (Recital 12 TCO Regulation). However, the line between a radical political statement and terrorist content may be very thin. A thorough contextual assessment is, therefore, crucial for distinguishing terrorist content from material covered by freedom of expression.

The recitals to the Regulation specify which factors should be considered when assessing whether material constitutes terrorist content: "the nature and wording of statements, the context in which the statements were made and their potential to lead to harmful consequences in respect of the security and safety of persons" (Recital 11 TCO Regulation). Furthermore, if the material was produced or disseminated by someone on the EU's list of persons, groups, and entities involved in terrorist acts and subject to restrictive measures, this should constitute an important factor in the assessment (Recital 11).

An example can demonstrate the practical difficulty of determining whether content should be removed under the TCO Regulation. As stated above, the Regulation excludes material disseminated for educational purposes from its scope. However, this exception only raises new questions: How does one determine if a text, image, or video has an educational purpose? Does this depend on the identity of the user who uploaded it (i.e., whether they are a teacher or professor)? Or does it depend on their affiliation with an educational or research institution? What about activist groups that aim to educate the public about terrorist activity? And what of anonymously uploaded material?

As this sub-section has shown, determining whether a piece of content should be removed under the TCO Regulation can be highly complex and dependent on many factors that must be established through a nuanced and contextual assessment. However, as the next section shows, the modalities of the TCO Regulation fail to address this complexity. This is especially the case where the removal of content is decided by the hosting service providers themselves using algorithmic content moderation systems.

3. Key provisions

The main innovation of the TCO Regulation is the creation of so-called removal orders (2.1). These can be internal or cross-border, meaning that they can also be addressed to hosting service providers established in different Member States or third countries (2.2). Where it has been established that hosting service providers were exposed to terrorist content, the Regulation requires them to take additional measures to prevent the dissemination of such content on their platforms (2.3). Finally, the Regulation obliges hosting service providers to publish an annual transparency report on how they are dealing with terrorist content (2.4).

3.1 Removal orders

Removal orders provide a basis for competent national authorities to compel hosting service providers to remove or disable access to terrorist content within one hour. Art. 3 of the TCO Regulation lays down the procedure to be followed.

First, the competent authority shall address the removal order to the main establishment of the hosting service provider or to its legal represen-

tative by electronic means capable of producing a written record under conditions that allow the authentication of the sender to be established and the date and time of the order specified (Art. 3(5)).

It is left to the Member States to designate the authorities empowered to issue removal orders.[5] The Regulation does not lay down any conditions that must be met in this regard, meaning that this could potentially be judicial or administrative authorities. The designated authorities range from law enforcement to specialised agencies working on organised crime or counterterrorism. Many Member States have designated multiple authorities, enabling both law enforcement and specialised administrative bodies to issue removal orders. For example, Germany designated both its Federal Criminal Police Office and the Federal Network Agency. Other countries seem to view the fight against terrorist content as a purely administrative matter. Austria, for example, only designated its Communications Authority. Depending on the Member State, the removal order is therefore not subject to any judicial review at the issuing stage.

The deadline to remove or disable access to terrorist content in all Member States is one hour after receipt of the removal order (Art. 3(3) TCO Regulation). This deadline has attracted substantial academic criticism. Following the publication of the proposed Regulation, Coche (2018) warned that the short timeframe, paired with the unclear definition of terrorist content, would "undoubtedly magnify the risks of over-removal of content" (p.12). In a detailed analysis of the origins and framework of removal orders, Rojszczak (2023) concurred, considering that the one-hour time limit "de facto eliminates the possibility of a more detailed legal analysis of a specific case" (p.17).

The hosting service providers' discretion for executing removal orders is minimal. In particular, they are not required to examine the order's admissibility but may only invoke a limited list of technical grounds to justify their non-execution. If they cannot comply with the removal order on grounds of force majeure, de facto impossibility, or if the removal order is incomplete or contains manifest errors, hosting service providers are required to inform the issuing authority of this (Art. 3(7) and (8) TCO Regulation). This information, however, only suspends the deadline, mean-

5 For an overview of the authorities that have been designated by the Member States, see the list of national competent authorities and contact points published by the European Commission (2025).

ing that the one-hour time limit begins once the grounds for non-execution have ceased to exist.

Certainly, hosting service providers that have received a removal order shall have the right to challenge it before the courts of the Member State of the issuing authority (Art. 9(1)). The Member States had to implement effective procedures for exercising this right. Nevertheless, even if a hosting service provider intends to take legal action, this does not entail a suspension of their obligation to execute the removal order.

The TCO Regulation lays down serious penalties for non-compliance (Art. 18). To this end, Member States had to adopt rules on penalties, which can be of an administrative or criminal nature. The type and level of penalty are decided on a case-by-case basis, depending on the nature, gravity, and duration of the infringement, whether the infringement was intentional or negligent, as well as the financial strength and size of the hosting service provider. If a hosting service provider systemically and persistently fails to comply with removal orders, penalties as high as 4% of their global turnover of the preceding business year can be imposed. Thus, further to the one-hour deadline, the high penalties create another incentive for hosting service providers to refrain from conducting more detailed assessments of removal orders.

Finally, hosting service providers shall make information on the removal order available to the user who uploaded the content (Art. 11). This duty entails either informing the individual of the reasons behind the removal and their rights to challenge it or providing them with a copy of the order. This obligation may be suspended when the public interest requires this information to be withheld, such as if this could threaten an ongoing criminal investigation.

3.2 Cross-border removal orders

Removal orders can be internal or cross-border in character. In other words, the issuing authority can address removal orders to hosting service providers established in their own or another Member State, or even outside the EU. As a reminder, the TCO Regulation also applies to hosting service providers that are established in third countries but offer their services in the EU. Generally speaking, the same procedure, duties, deadlines, and penalties apply as in internal cases. This subsection therefore only

highlights some differences between cross-border and internal removal orders.

For cross-border removal orders, there is an additional requirement to notify competent authorities in the Member State where the hosting service provider is established (Art. 4(1) TCO Regulation). For example, if the German Federal Network Agency wants to order the removal of terrorist content published on Instagram, which is owned by Meta Platforms Ireland, they must send a copy of the order to the Irish authorities.

This notification requirement is important because the Member State of establishment may scrutinise the validity of the removal order against the TCO Regulation and EU fundamental rights law (Art. 4(3)). In the above example, this would mean that the Irish authorities assess whether the cross-border removal order fulfilled the Regulation's conditions and respected the EU Charter of Fundamental Rights, and especially freedom of expression. This allows the authorities in the Member State of establishment to protect users from abusive removal orders. An example of such an order would be one that is not targeted at specific items of content, but aims to remove all content uploaded by a specific user. Another example could be an order that is abused to prevent activists or political dissidents from communicating with the public. If the authorities in the Member State of establishment find that the removal order infringes the Regulation or the Charter, they should adopt a reasoned opinion to that effect within 72 hours of receipt. This will cause the removal order to cease having legal effect, and the hosting service provider will have to reinstate the content and access thereto (Art. 4(7)).

For cross-border removal orders, the Regulation also foresees a more active role for hosting service providers: They may send a reasoned request to the competent national authority in their Member State to scrutinise the order as described in the previous paragraph (Article 4(4)). To return to the German example, this would mean that Instagram could contact the competent authorities in Ireland and ask them to assess the removal order received from the German Federal Network Agency. This gives hosting service providers an important role in preserving legality and respect for fundamental rights: If they suspect that a cross-border removal order raises problems, they can alert the competent authorities in their Member State, who will have to issue a reasoned decision.

This provision may become important in practice. It is to be expected that the Member States that are home to many bigger hosting service providers receive a higher number of notifications regarding such removal

orders. Ireland, for example, is the Member State of establishment of Meta and Google, two companies offering a range of services that fall into the TCO Regulation's scope. We can thus expect that the Irish authorities receive a comparatively high number of notifications. In such a scenario, hosting service providers can act as important filters. They can flag problematic orders and thereby draw the competent authority's attention to those which require further scrutiny. Nevertheless, the same concerns as for internal removal orders apply here as well: Due to the one-hour deadline and high fines that hosting service providers face for non-execution, they may not have the time or incentive to do this in practice. Ultimately, it is always safer for the service provider to immediately comply with a removal order, and thus avoid hefty fines.

3.3 Specific measures to address the dissemination of terrorist content

Beyond dealing with removal orders, the TCO Regulation requires hosting service providers that have been exposed to terrorist content to take additional measures to protect their users against such content.

This procedure is laid down in Art. 5 of the TCO Regulation and applies to hosting providers who have a history of such exposure. This is the case where a provider has received two or more removal orders in the previous 12 months. Where this is established, they shall take additional measures to address the misuse of their services (Art. 5(4)). In case of non-compliance, the same provisions regarding penalties apply as for (cross-border) removal orders (Art. 18).

Hosting service providers have broad discretion to determine the type of measures they choose to achieve this goal. As suggested by the Regulation, these measures may include appropriate technical and operational measures or capacities, but also mechanisms for users to report terrorist content or those for user moderation (Art. 5(2)). The hosting service provider may, for example, decide to hire specialised staff or invest in developing technological tools to better detect and remove terrorist content. This may include upload filters, which allow for the automatic recognition and blocking of content – a highly controversial practice that is also being debated in the context of other types of illegal content, such as child sexual abuse material or copyright infringements (see Romero Moreno, 2020).

Scholars have warned that the broad discretion afforded to hosting service providers under Art. 5 significantly enhances their role in "policing"

online content. Carrera et al (2022, p. 11) considered that the TCO Regulation thereby "assigns service providers with 'law enforcement duties' to remove, disable access to, or assess nature of online content in ways that are both reactive […] and proactive".

The proactive measures required under Art. 5 have also prompted the question of whether the Regulation impacts the EU's system of intermediary liability. As a reminder, providers of intermediary services – including hosting services – are exempt from liability in the EU if they do not have actual knowledge of illegal activity or information on their platforms and, upon obtaining such knowledge, act expeditiously to remove or disable access to it (see Section 1.1). In this regard, Kuczerawy (2019, p. 1) observed a general shift "from liability to responsibility". She maintained that the EU is moving away from its traditional, negligence-based liability system towards proactive measures, such as those required under the TCO Regulation.

Another aspect that has been raised in this connection is the prohibition of general monitoring. As a rule, Member States may not impose a general obligation for hosting service providers to monitor the information they transmit or store, nor a general fact-finding obligation regarding illegal activity (Art. 15 e-commerce Directive; Art. 8 DSA). However, crucially, the prohibition of general monitoring is addressed to the Member States, not the service providers themselves. Hence, this does not prevent hosting service providers from undertaking such far-reaching monitoring activities voluntarily. According to Carrera et al (2022), the TCO Regulation does not exclude the use of automated tools, and thus legitimises automated filtering and content blocking as a way for hosting service providers to comply with their obligations under Art. 5. Connected to this, Frosio (2018) maintained that the introduction of proactive measures leads to a de facto delegation of enforcement duties to private actors and the algorithmic tools they use. This is particularly problematic where such tools are used to block images and videos that have been previously labelled as terrorist content without any administrative or judicial oversight.

Art. 5(1) of the TCO Regulation states that the proactive measures taken by hosting service providers should not unduly encroach on users' freedom of expression and information by over-removing material that does not constitute terrorist content. The Regulation further stresses that these measures should be applied in a diligent and non-discriminatory manner (Art. 5(3)). However, the Regulation only provides for very limited public oversight in this regard. Pursuant to Art. 5(5) of the Regulation, hosting service providers shall report to the competent authority on the specific

measures they have taken to comply with the Regulation within three months of receiving the decision and on an annual basis thereafter. Several considerations raise doubts as to the potential of these reports to provide meaningful public oversight regarding the hosting service providers' content moderation practices.

First of all, so far, the transparency reports published by hosting service providers (see Section 2.4) go into little detail as to how terrorist content is detected, removed, and blocked.[6] Of course, it should be noted that these reports are publicly accessible, while those addressed solely to the competent authorities could go into greater detail in this respect. However, it is unlikely that hosting service providers will voluntarily report more than what is strictly required by Article 5.

In addition, if hosting service providers rely on algorithmic moderation systems to fight the spread of terrorist content, they may be bound by contractual secrecy or trade secrets, which limits what they can disclose about the technology used. Curtin and Fia (forthcoming) outlined this problem regarding public authorities' use of AI systems. Secrecy may limit access to training data, algorithms, and technical documentation, which impinges on transparency and the possibility of exercising public oversight. The same concerns apply in the context of the TCO Regulation: Without comprehensive access to technical components and documentation, hosting service providers can use secrecy to shield themselves from public scrutiny regarding their content moderation practices and whether these are applied in a non-discriminatory manner.

Furthermore, competent national authorities have no vested interest in conducting thorough reviews of the preventive measures taken under Article 5. The TCO Regulation ultimately relies on the rationale that hosting service providers should internally develop and implement solutions to address the spread of terrorist content. As long as platforms remain "clean", public authorities may limit themselves to a superficial review and avoid closely examining how this is achieved.

6 In the early years of the German Network Enforcement Act, transparency reports did not meet lawmakers' expectations either, raising doubts about their effectiveness in clarifying content moderation practices. For more information, see Heldt (2019).

3.4 Transparency obligations

Finally, the TCO Regulation outlines a number of transparency obligations, which should contribute to holding hosting service providers accountable for their content moderation practices vis-à-vis their users.

First of all, hosting service providers must clearly outline their policy for addressing terrorist content in their terms and conditions (Art. 7(1) TCO Regulation). This may include an explanation of how specific measures function, as well as the potential use of automated tools.

Moreover, hosting service providers are required to publish transparency reports detailing the actions they have taken to address the dissemination of terrorist content (Art. 7(2)). These reports should include, amongst other things, information about the measures taken in relation to the identification and removal of terrorist content, as well as measures to prevent the reappearance of this material, the number of items of terrorist content removed following removal orders, and specific measures undertaken (Art. 7(3)). The reports should also specify whether the removal orders were complied with and, if not, the grounds for non-compliance. In addition, the reports should detail the number and outcome of complaints handled by the hosting service provider, decisions imposing penalties, as well as the number and outcome of administrative or judicial review proceedings brought by the hosting service provider.

As of June 2024, hosting service providers have had to publish two transparency reports: The first of which covering the period following the entry into force of the TCO Regulation in 2022, and the second covering the full year of 2023. These reports provide initial insights into the TCO Regulation's practical application.

Transparency reports from Meta and Google have indicated that the number of removal orders is still relatively low. For 2023, Meta reported 143 requests for removal orders for Facebook (Facebook Transparency Report, 2023, p. 8). Notable, in addition to the low number, is that the majority of orders were deemed not compliant with the conditions for their issuing. The report has specified that, for Facebook, only 15 requests were, in fact, valid orders issued by competent authorities. Among these, only 10 led to content being removed or access thereto being restricted in the EU. Google's transparency report paints a similar picture, stating that they received no removal orders from competent authorities under the TCO Regulation in 2023 (Google Transparency Report, 2023, p. 2).

For now, terrorist content is removed almost exclusively following the platforms' internal policy. Meta cited 6.1 million items of content removed for violating Facebook's policies on "Dangerous Organizations and Individuals", "Violence and Incitement", and "Coordinating Harm and Promoting Crime" (Facebook Transparency Report, 2023, p. 9). According to Meta, these policies are "congruent with the Regulation's definition of 'terrorist content'" (Facebook Transparency Report, 2023, p. 5). Google cited over 16.3 million items of terrorist content that were removed in 2023 (Google Transparency Report, 2023, p. 2). However, the report failed to specify how many of these would have been covered by the TCO Regulation.

Nevertheless, it would be premature to conclude that the relative underuse of removal orders suggests that the Regulation is not being applied. National authorities may require time to integrate removal orders into their practices, potentially causing delays in the implementation of the Regulation. In addition, the removal of the vast majority of content according to internal policies demonstrates the effectiveness of preventive tools used by the platforms to combat the spread of terrorist content. In this regard, both providers have stated that their content moderation relies on a combination of automated systems, human review, and user reports (Facebook Transparency Report, 2023, p. 2; Google Transparency Report, 2023, p. 1).

One might argue that, if terrorist content is removed directly by the platforms, and national authorities have no need to intervene, the TCO Regulation has achieved its goal. However, in the absence of more detailed information on what content is removed following the platforms' internal policies, and how these overlap with the Regulation's definitions, it is hard to discern whether the platforms are complying with EU rules or simply over-removing content.

4. Conclusion

By introducing legal obligations regarding how to deal with terrorist content, the TCO Regulation marked the beginning of the EU's efforts to enhance the responsibility of online platforms for the content they host and disseminate. The Regulation establishes a new set of responsibilities for hosting service providers. On the one hand, they must respond to removal orders issued by national competent authorities by taking down terrorist content within a one-hour deadline. On the other, hosting service

providers must also take preventive action. If they have been exposed to terrorist content, they must adopt specific measures to ensure that their platforms remain free of such content. The Regulation thereby fundamentally changes the enforcement landscape: Hosting service providers do not merely have to comply with legal requirements, but actively contribute to the prevention of radicalisation and, potentially, terrorist acts.

Determining whether a text, image, or video constitutes terrorist content can be highly context-dependent and technical. Traditionally, courts establish this through an evidence-based procedure, considering not only the content itself, but also contextual factors. Regrettably, the modalities of the TCO Regulation do not do justice to this complexity and create significant risks for abuse. The short deadlines and high fines, along with the fact that some Member States do not require judicial review to issue removal orders, have raised concerns regarding the over-removal of content and the associated risks to freedom of expression and information.

Moreover, the TCO Regulation legitimises, and even incentivises, the use of algorithmic moderation systems to detect and remove terrorist content. Hosting service providers are thus likely to rely on algorithmic tools and AI to comply with the Regulation's requirement to take preventive measures to stop the spread of terrorist content. In this regard, the Regulation would have provided an opportunity to assert public oversight by requiring hosting service providers to publish detailed reports on what content is removed under the Regulation and how this content was detected. Instead, the Regulation only requires them to provide minimal information on their content moderation practices, and the first transparency reports show that platforms are typically unwilling to share more than what is required in this regard. The TCO Regulation thus created a system where hosting service providers are responsible for the removal of terrorist content, but the EU Member States cannot know – or, indeed, prefer not to know – how this is done.

Even if the TCO Regulation led to hosting service providers intensifying their fight against terrorist content, whether its implementation can be termed a success would remain in doubt. While the EU's push for preventative action may have helped keep terrorist content off social media and video-sharing platforms, we seem to have gained no clarity on how this is achieved.

References

Bellanova, R. and de Goede, M. (2021) 'Co-producing security: platform content moderation and European security integration', *Journal of Common Market Law Studies,* 60(5), pp. 1–19.

Carrera, S., Mitsilegas, V., Stefan, M. and Vavoula, N. (2022) *Towards a principled level playing field for an open and secure online environment. Regulation, enforcement and oversight of online content moderation in the EU and the United Kingdom*. CEPS Task Force Report [Online]. Available at: https://cdn.ceps.eu/wp-content/uploads/2022/10/CEPS-Task-Force-Report_Online-Content-Regulation.pdf (Accessed: 27 January 2025).

'Charter of Fundamental Rights of the European Union' (2012) *Official Journal* C 326, 26 October, pp. 391-407 [Online]. Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=uriserv:OJ.C_.2012.326.01.0391.01.ENG (Accessed: 27 January 2025).

Coche, E. (2018) 'Privatised enforcement and the right to freedom of expression in a world confronted with terrorism propaganda online', *Internet Policy Review,* 7(4), pp. 1–17.

'Commission Recommendation (EU) 2018/334 of 1 March 2018 on measures to effectively tackle illegal content online' (2018) *Official Journal* L 63, pp. 50-61, [Online]. Available at: http://data.europa.eu/eli/reco/2018/334/oj (Accessed: 27 January 2025).

'Consolidated version of the Treaty on the Functioning of the European Union' (2012) *Official Journal* C 326, 26 October, pp. 47-390 [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2012/oj (Accessed: 27 January 2025).

'Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 22) on the position of Denmark' (2012) *Official Journal* C 326, 26 October, pp. 299-303 [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2012/pro_22/oj (Accessed: 27 January 2025).

'Consolidated version of the Treaty on the Functioning of the European Union Protocol (No 21) on the position of the United Kingdom and Ireland in respect of the area of freedom, security and justice' (2016) *Official Journal* 202, 7 June, pp. 295-297, [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2016/pro_21/oj (Accessed: 27 January 2025).

Curtin, D. and Fia, T. (forthcoming) 'Cracking Secrecy Dominance in European AI Regulation'.

De Pasquale, P. and Pesce, C. (2021) 'Article 82 (principle of mutual recognition)' in Blanke, H. and Mangiameli, S. (eds.) *Treaty on the Functioning of the European Union – a commentary: volume I: preamble, Articles 1–89*. Cham: Springer International Publishing, pp. 1559–1580.

'Directive 2000/31/EC on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market' (2000) *Official Journal* L 178, 17 July, pp. 1-16 [Online]. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed: 27 January 2025).

'Directive 2011/93/EU on combating the sexual abuse and sexual exploitation of children and child pornography, and replacing Council Framework Decision 2004/68/JHA' (2011) *Official Journal* L 335, 17 December, pp. 1-14 [Online]. Available at: http://data.europa.eu/eli/dir/2011/93/oj (Accessed: 27 January 2025).

'Directive (EU) 2017/541 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA' (2017) *Official Journal* L 88, 31 March, pp. 6-21 [Online]. Available at: http://data.europa.eu/eli/dir/2017/541/oj (Accessed: 27 January 2025).

'Directive (EU) 2018/1808 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities' (2018) *Official Journal* L 303, 28 November, pp. 69-92 [Online]. Available at: http://data.europa.eu/eli/dir/2018/1808/oj (Accessed: 27 January 2025).

European Commission (2017) Communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions, tackling illegal content online. Towards an enhanced responsibility of online platforms COM/2017/0555 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0555 (Accessed: 27 January 2025).

European Commission (2025) *List of national competent authority (authorities) and contact points*. European Commission [Online]. Available at: https://home-affairs.ec.europa.eu/policies/internal-security/counter-terrorism-and-radicalisation/prevention-radicalisation/terrorist-content-online/list-national-competent-authority-authorities-and-contact-points_en (Accessed: 31 January 2025).

Facebook (2024) *European Union terrorist content online transparency report*. Facebook [Online]. Available at: https://transparency.meta.com/sr/eu-online-report-fb-feb29-24 (Accessed: 27 January 2025).

French Constitutional Council, 'Décision n° 2020-801 DC of 18 June, 2020' (2020) *Journal Officiel de la République Française* n°0156, 25 June [Online]. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031998/ (Accessed: 27 January 2025).

Frosio, G. (2018) 'Why keep a dog and bark yourself? From intermediary liability to responsibility', *Oxford International Journal of Law and Information Technology,* 26(1), pp. 1–38.

Frosio, G. (ed.) (2020) *The Oxford handbook of online intermediary liability*. Oxford: Oxford University Press.

'Gesetz zur Verbesserung der Rechtsdurchsetzung in sozialen Netzwerken (Netzwerkdurchsetzungsgesetz - NetzDG)' BGBl. I 2017, p. 3351 [Online]. Available at: https://www.gesetze-im-internet.de/netzdg/BJNR335210017.html (Accessed on: 27 January 2025).

Google (2024) *Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online transparency report*. Google [Online]. Available at: https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-26_2023-1-1_2023-12-31_en_v1.pdf (Accessed: 27 January 2025).

Heldt, A., (2019) 'Reading between the lines and the numbers: an analysis of the first NetzDG reports', *Internet Policy Review*, 8(2), pp. 1–18.

Janssens, C. (2013) *The principle of mutual recognition in EU law*. Oxford: Oxford University Press.

Jørgensen, R.F. and Pedersen, A.M. (2017) 'Online service providers as human rights arbiters' in Taddeo, M. and Floridi, L. (eds.) *The responsibilities of online service providers*. Cham: Springer International Publishing, pp. 179–199.

Kuczerawy, A. (2019) 'General monitoring obligations: a new cornerstone of internet regulation in the EU?' in Centre for IT & IP Law (ed.) *Rethinking IT and IP law – celebrating 30 years CiTiP*. Antwerp: Intersentia, pp. 141–148.

'LOI n° 2020-766 du 24 juin 2020 visant à lutter contre les contenus haineux sur internet (Avia Law)' (2020). *Journal Officiel de la République Française*, n°0156, p.11, 25 June [Online]. Available at: https://www.legifrance.gouv.fr/jorf/id/JORFTEXT000042031970 (Accessed: 27 January 2025).

Mitsilegas, V. (2016) *EU criminal law after Lisbon: rights, trust and the transformation of justice in Europe*. Oxford: Hart Publishing.

Mitsilegas, V. and Salvi, C. (2024) 'Digital exceptionalism, freedom of expression and the rule of law: the case of targeting terrorist content online', *Rivista Eurojoust,* 2(2024), pp.181–205.

'Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online' (2021) *Official Journal* L 172, 17 May, pp. 79-109. [Online]. Available at: http://data.europa.eu/eli/reg/2021/784/oj (Accessed: 27 January 2025).

'Regulation (EU) 2022/2065 on a single market for digital services and amending Directive 2000/31/EC (Digital Services Act)' (2022) *Official Journal* L 277, 27 October, pp. 1-102, [Online]. Available at: http://data.europa.eu/eli/reg/2022/2065/oj (Accessed: 27 January 2025).

Rojszczak, M. (2023) 'Gone in 60 minutes: distribution of terrorist content and free speech in the European Union', *Democracy and Security*, 20(2), pp. 179–209.

Romero Moreno, F. (2020) 'Upload filters and human rights: implementing Article 17 of the directive on copyright in the digital single market', *International Review of Law, Computers & Technology,* 34(2), pp. 153–182.

Scheinin, M. (2019) 'The EU regulation on terrorist content: an emperor without clothes', *Verfassungsblog*. 30 January 2019 [Online]. Available at: https://verfassungsblog.de/the-eu-regulation-on-terrorist-content-an-emperor-without-clothes/ (Accessed: 27 January 2025).

Tosza, S. (2021) 'Internet service providers as law enforcers and adjudicators. A public role of private actors', *Computer Law & Security Review,* 43, pp. 1–17.

Wilman, F. (2020) *The responsibility of online intermediaries for illegal user content in the EU and the US*. Cheltenham: Edward Elgar Publishing.

What the Political Advertising Regulation Can Do for Researchers (and Vice Versa)

Max van Drunen

Abstract

This chapter evaluates how the EU's Political Advertising Regulation empowers researchers to scrutinize political advertising. The Political Advertising Regulation is one of the main new EU regulations that explicitly aims to strengthen research into the (online) information ecosystem. The chapter first analyses why the EU empowers researchers to scrutinize political advertising, distinguishing between the limits of 'hard' regulation on political advertising, the need to enable political advertisers' accountability to the electorate, and the need for a better long-term understanding of the way political advertising is conducted. It then analyses the research opportunities the Political Advertising Regulation opens up. It provides an overview of the data the regulation makes available on all online political advertising, and the data researchers can request from service providers further back in the value chain, such as data analytics companies. It also evaluates the limitations of the newly accessible data, as well as the research opportunities it opens up. The chapter closes by evaluating the research opportunities opened up by the new obligations imposed on political advertising, focusing on which ads are considered 'political' in practice by platforms, which groups become harder to reach due to the regulation's new restrictions on targeting, and the Commission's new power to set binding rules on the design of political advertising labels based on insights from scientific research.

1. Introduction

The 2018 Cambridge Analytica controversy presented the EU legislature with a rather complex challenge. On the one hand, the ability to microtarget voters with political ads tailored to their personality seemed to pose a new technological threat to European democracy that called for legislative action. On the other hand, the lack of transparency in online

advertising made it difficult to determine the extent to which political advertisements were actually being targeted and with what effect. While platforms increased the transparency of online political advertising after 2018, these voluntary efforts have been widely criticised for failing to include sufficiently precise and comprehensive data needed for research into targeted political advertising (Ausloos et al, 2020; Dubois et al, 2022; Edelson et al, 2021, 2019; Kreiss and Barrett, 2020). In short, the EU was forced to regulate a problem that a lack of data prevented it from fully understanding. This issue was compounded by the fact that any regulation the EU does pass must comply with both freedom of expression principles that limit stringent restrictions imposed on political advertising, as well as EU Member States' hesitancy to regulate political advertising on the EU level.

Faced with these constraints, the EU has turned its attention to researchers. The Regulation on the Transparency and Targeting of Political Advertising (Regulation 2024/900) (commonly referred to as the Political Advertising Regulation, or PAR) is one of the primary pieces of new EU regulation specifically designed to enable research into the online information environment (Ausloos et al, 2023). Through this regulation, the EU aims to provide the transparency needed to hold political advertisers—and the companies that create and distribute their ads—accountable, while also supporting research that provides a more general understanding of the way political advertisements are being distributed (recitals 64 and 73 PAR).

This chapter evaluates how the PAR empowers researchers to scrutinise political advertising. Section 2 begins by discussing the kinds of political advertising activities covered by the PAR and why the EU aims to empower researchers to scrutinise political advertising. Section 3 then describes the new data the PAR makes available to researchers through ad libraries and data access requests. Finally, Section 4 evaluates what research is required to evaluate and apply the transparency and targeting restrictions the PAR imposes.

2. A brief introduction to the Political Advertising Regulation

2.1 What is political advertising?

Article 3(3) of the PAR provides the first definition of political advertising in EU law (for an analysis of existing national definitions, see van Drunen,

Helberger and Ó Fathaigh, 2022), covering both actor- and issue-based political advertising. First, a message falls within the PAR's definition of political advertising if it is "by, for, or on behalf of a political actor". Article 3(4) further specifies eight categories of political actors, including candidates for or holders of elected office at any level (from EU to local); members of local, regional, and national governments or EU institutions (excluding the Court of Justice of the EU, the European Central Bank, and the Court of Auditors), as well as individuals in leadership roles within political parties. However, purely private or commercial messages from political actors—such as an advertisement by a local councillor for their tax auditing business—are not covered.

Second, the PAR applies to messages that are "liable and designed to influence the outcome of an election or referendum, voting behaviour or a legislative or regulatory process, at Union, national, regional or local level" (Article 3(2)(b) PAR). A clear-cut example would be an ad by a fossil fuel group encouraging individuals to call their representatives to vote against an upcoming regulation or an ad by a climate NGO emphasising the need to address the climate crisis in the upcoming election. In more ambiguous cases, the PAR stipulates that there must be "a clear and substantial link" between the message and its potential influence on these outcomes (recital 23 PAR). The PAR lists a wide array of factors to determine this link, such as the timing, content, source, and intended audience of the message (recital 23 PAR). However, because these factors are so broad, they provide limited guidance on what is and is not political advertising. As a result, the practical scope of the PAR's definition of issue-based ads largely depends on how courts and regulators interpret and apply these factors.

The definition of political advertising also covers a wide range of activities, including the "placement, promotion, publication, [and] delivery" and even the "preparation" of political messages (Article 3(2) PAR). Concretely, the PAR refers to entities such as political consulting and PR firms, ad-tech platforms, data brokers, and data analytics companies as examples of organisations potentially providing political advertising services during the preparation phase (recital 1 PAR). Similarly, the PAR acknowledges a wide range of dissemination methods, including influencer endorsements, sponsored search results, and product placements, as well as newspapers, television, radio, mobile apps, websites, platforms, and computer games (recital 2 PAR). In short, the PAR covers nearly every activity associated with political messaging; the broad scope of its definition is perhaps best illustrated by the fact that legislators found it necessary to clarify that ancil-

lary services—such as cleaning and catering—do not qualify as political advertising services (recital 39 PAR).

The PAR only covers the preparation or publication of messages "normally provided for remuneration or through in-house activities or as part of a political advertising campaign" (Article 3(2) PAR). The regulation contains further exceptions for political opinions expressed in a personal capacity, for political opinions expressed without specific payment and in media under editorial responsibility (i.e., TV but not social media platforms such as YouTube (van Drunen, 2020; recital 8 EMFA), and for platforms (or other intermediaries) that allow users to upload content for free. As this web of exceptions suggests, the notion that political advertising constitutes paid-for political speech was surprisingly controversial during the political process (European Partnership for Democracy, 2023; van Drunen et al, 2023). On the one hand, a looser payment criteria would make it easier to address hidden advertising. It would also avoid creating an unfair advantage for large political actors, who do not need to pay external political service providers for tasks they can assign to in-house employees (hence the reference to in-house activities in Article 3(2) of the PAR). On the other hand, political speech that is unpaid benefits from the highest fundamental rights protections, and including it under the scope of the PAR would quickly run afoul of these protections (Dobber et al., 2019).

Finally, several exceptions should be noted. The PAR is only applicable to political advertising disseminated in the EU or directed at EU citizens (Article 2(1) PAR). It does not apply to official information regarding the organization of and participation in elections, official information disseminated to the public by, for, or on behalf of public authorities (as long as it is not liable and designed to influence voting behaviour), or the presentation of candidates in public spaces in the media (as long as it is provided for by law, free, and ensures equal treatment (Article 3(2) PAR).

2.2 Why does the Political Advertising Regulation empower researchers?

Government intervention in political advertising is a sensitive issue, as the right to freedom of expression affords considerable protection to political speech, even when it involves payment (Animal Defenders International v United Kingdom, 2013; TV Vest v Norway, 2008, para. 60). EU regulation of political advertising is particularly contentious due to the broad spectrum of approaches across Member States. Some countries, like Germany,

completely ban political advertising during certain periods or on certain media, while others, such as the Netherlands, have left political advertising largely unregulated (ERGA, 2021; van Hoboken et al., 2019). Any EU regulation aiming to set a uniform legal standard for political advertising must account for these national differences, as well as the historical hesitance of Member States to regulate speech at the EU rather than the national level (Bayer, 2024, pp. 87-106; van Drunen, Helberger and Ó Fathaigh, 2022).

In this context, transparency is an attractive proposition. It allows political actors to communicate freely with the public as they see fit while enabling Member States to impose stricter standards on the content of political advertising. At the same time, transparency can strengthen political accountability by ensuring that researchers have access to the data needed to scrutinise political actors and inform the public when political advertising is used in controversial ways (recitals 64 and 73 PAR). For example, following the 2024 European Parliamentary elections, the Belgian newspaper *De Tijd* worked with researchers to investigate how Belgian political parties targeted their advertisements. They found that the far-right party Vlaams Belang had systematically excluded individuals with an interest in African countries or Turkish football clubs from their ads, which often took an anti-migration stance. These practices skirted the EU's and Meta's ban on ethnic profiling (Verhaeghe, 2024). In this situation, EU law arguably strengthened journalists' ability to act as a public watchdog for powerful political actors by making additional data available to researchers. However, it is important to note that increased transparency does not necessarily change the behaviour of political actors. The effectiveness of transparency depends, among other things, on journalists and researchers making use of the newly provided data, as well as political parties being sensitive to the scrutiny they may face (Leerssen et al, 2021; Marchal et al, 2024).

Empowering researchers in the long term is necessary for fostering a deeper understanding of the political advertising landscape, which could inform the need for and design of future regulations of political advertising (Ausloos et al, 2023; Leerssen, 2023; van Drunen and Noroozian, 2024). Currently, the PAR, alongside other EU digital regulations such as the Digital Services Act (DSA)[1], aims to achieve two goals: regulating

1 For more information on the DSA, see Chapter 4 'The Digital Services Act: Online Risks, Transparency and Data Access' by Marie-Therese Sekwenz and Rita Gsenger and Chapter 5 'The Digital Services Act – an appropriate response to online hate speech?' by Pascal Schneiders and Lena Aulers.

perceived problems in the online information environment while ensuring researchers have access to the data necessary to understand what these problems are. In the case of the PAR, the Cambridge Analytica scandal triggered concerns over the ability of targeted advertising to manipulate and discriminate between voters, prompting EU legislators to restrict the use of (sensitive) data (recitals 6 and 74 PAR). However, much remains unclear about the ways and extent to which political advertisers engage in manipulative or discriminatory targeting practices, the actual effects of such practices on voting behaviour, and the conditions under which these effects manifest (Dobber, 2020; Kruikemeier et al, 2023; Votta, 2024). This uncertainty challenges regulators' ability to effectively govern the online information environment. One key benefit of the PAR is that it potentially improves our understanding of the specific ways in which political advertising can undermine democracy, enabling future regulations to address these challenges in a more empirical manner.

Finally, the reason why regulation is necessary to ensure the transparency required for accountability and a better understanding of the political advertising landscape is that the online environments in which political advertising occurs are in the hands of private actors. These actors have little incentive to provide access to the data needed for additional regulation or to hold their advertisers accountable (Ausloos et al, 2020, p. 88; Leerssen, 2023). Additionally, the personalised nature of targeted advertising limits researchers' ability to study these practices without the cooperation of the companies involved (Bodó et al, 2017). Unlike ads on TV or in newspapers, targeted ads are typically visible only to the person who receives them. As a result, researchers studying online political advertising have had to rely on challenging methodologies, such as data donations, or seek the cooperation of platforms to gain direct access to data. However, the data access regimes that platforms have voluntarily provided (e.g., voluntary ad libraries, Social Science One) have been limited in both scope and functionality (Edelson et al, 2021; Kirk and Teeling, 2021; Kreiss and Barrett, 2020; Leerssen, 2023). Regulation, at least in theory, offers an alternative solution by forcing private actors to provide data to researchers.

3. Research rights in the Political Advertising Regulation.

The PAR provides two kinds of transparency measures for researchers: making data available to everyone through ad libraries and making data

available to restricted groups submitting data access requests. This section discusses both measures in turn.

3.1 Ad libraries

The PAR requires that certain information (for a full overview, see Table 1) about political advertisements be available to everyone through publicly accessible databases (ad libraries). Article 39 of the DSA already required very large online platforms and search engines (defined in Article 33 of the DSA as having over 45 million monthly active users in the EU; henceforth referred to as large platforms and search engines) to create such ad libraries (Leerssen et al, 2021). The added value of the PAR is that large platforms and search engines must include political advertisements in their ad libraries in real-time, along with additional information regarding in particular the way these ads were funded and targeted. Moreover, it stipulates that the Commission will operate an ad library for all online political ads and has the authority to mandate the inclusion of further information in ad libraries based on scientific and technological developments (Articles 12(6) and 19(5) PAR).

Table 1. An overview of the information Article 39 of the DSA and Articles 12(1) and 19(1)(c, e) of the PAR require ad libraries to contain. Text in bold is only required under the PAR and, therefore, only applicable to political ads. Versions of this table based on earlier versions of the PAR have appeared in Buri et al. (2022) and van Drunen et al. (2024).

Type	Disclosure
Content	Content of the ad.
	Whether it is a political ad.
Identity	Name of the product/service/brand being advertised.
	Identity **and contact details** of **(the entity ultimately controlling)** the advertiser.
	Identity **and contact details** of **(the entity ultimately controlling)** the funder.
Timing	Dissemination period for the ad.

Type	Disclosure
	Referenda, elections, or regulatory processes with which the ad is linked.
Funding	**Aggregate benefits all service providers received for the ad and ad campaign.**
	Whether these benefits came from public or private sources and from inside or outside the EU.
	Methodology for calculating these benefits.
Reach	Number of individuals reached (**in terms of the number of views and engagements with the ad** per Member State and target group).
Targeting	Whether the ad was targeted.
	Targeting goals, mechanisms, and logic, including the main parameters used for targeting/exclusion **and the reasons for choosing these.**
	Categories of personal data used for targeting or ad-delivery.
	Meaningful information on the use of AI in targeting or ad delivery.
	A link to the internal policy describing how political advertising targeting or ad delivery techniques were used.
Moderation	If the ad has been removed, a statement of reasons why and how it was removed.
	Whether a previous version of the ad has been removed for violating the PAR.
Legal rights	**How to participate in the elections/referenda with which the ad is linked.**
	A link to the EU ad library.
	A link to the notice and takedown mechanism.
	A link to effective means to exercise GDPR rights.

The data made available through ad libraries is subject to a significant caveat: no single actor is under a strong obligation to verify whether it is complete and correct. Although political advertisers are legally required to truthfully disclose the political nature of their ad and supply the information listed in the PAR (Article 7(1) PAR), publishers are only required to ensure the accuracy of information regarding the reach of the ad, the money spent on it, how this amount was calculated, and how individuals can exercise certain legal rights (Article 12(2) PAR). For other information, including whether an ad is correctly identified as political, political advertising service providers are only required to check whether the infor-

mation advertisers have supplied is "manifestly erroneous", meaning that it "is apparent from the content of the advertisement, the identity of the sponsor, or the context in which the relevant service is provided, without further verifications" (Article 7(4), recital 45 PAR). These relatively lax obligations appear ineffective at addressing researchers' complaints regarding platforms' efforts to ensure political ads are correctly labelled in ad libraries (Edelson et al, 2019, 2020; Kirk and Teeling, 2021).

The additional data made available in ad libraries under the PAR offers modest benefits to researchers. Notably, it requires more detailed information on the funding of political advertisements, including their source, the total amount spent on the campaign, and any non-monetary benefits. Additionally, the PAR mandates the provision of more specific data on the targeting and reach of political advertisements. For reach, platforms must disclose the number of views and engagements; for targeting, the additional data primarily concerns general information about the functioning, goals, and use of targeting. However, this is unlikely to provide researchers with a more fine-grained view of how political advertisements are targeted.

While the current data provided in ad libraries may be of limited utility to researchers, the PAR allows the Commission to adopt a delegated act that can expand the list of required information in response to "technological developments, market practices, relevant scientific research, developments in supervision by competent authorities, and relevant guidance issued by competent bodies" (Article 12(6) PAR). For researchers working with data from ad libraries, this means that it is valuable to explicitly identify concrete pieces of information missing from ad libraries that would better enable the scrutiny of political advertising. This feedback could help inform the Commission on how to exercise its power to adopt a delegated act. However, it should be noted that the Commission's power to adapt ad libraries through delegated acts is not unlimited. The Council and Parliament have two months to veto any delegated act the Commission proposes and can strip the Commission of its power to adopt delegated acts at any time (Kaeding and Stack, 2015). Moreover, delegated acts cannot change "essential elements" of the underlying regulation, namely those that require political choices by the legislature and a balancing of the interests at stake (Chamon, 2018, p. 239; Schütze, 2011, p. 662). Finally, the Commission can only amend the list of information requirements if such changes are "necessary for the wider context of the political advertisement and its aims to be understood" (Article 12(6) PAR).

The Commission will also operate a central ad library that includes all political advertisements disseminated online, and large online platforms and search engines must send the advertisements published on their services to that database immediately. Other publishers (such as smaller platforms, influencers, online newspapers, and radio stations) must do so within 72 hours (Article 13(5) PAR). Moreover, the Commission is required to set out binding rules (an *implementing act*) on a common data structure, standardised metadata, and shared API to ensure that all online political advertisements can be researched through a single portal (Article 13(6) PAR).

The ad library operated by the Commission offers several potentially significant benefits for researchers. First, it facilitates cross-publisher research by aggregating all online political advertisements–whether from large or small platforms, search engines, influencers, online newspapers, and other sources—into a single database with a unified data structure. Second, outsourcing the operation of an ad library to the Commission may improve functionality. Platforms lack strong incentives to invest in a well-functioning ad library that allows researchers to scrutinise their advertisers. Conversely, both the Commission and researchers have a shared interest in enabling scrutiny of the electoral process, assuming that the independence of the Commission entity operating the ad library is safeguarded. This creates an opportunity for a more direct and efficient process through which the Commission's ad library can be adapted based on researchers' needs (van Drunen and Noroozian, 2024).

3.2 Data access requests

The PAR establishes two new rights to data access, as demonstrated in Table 2. Much of the information that can be requested is similar to the information included in the ad libraries. The added value of the PAR is that data can also be requested from political advertising service providers and controllers, which include actors further back in the political advertising value chain, as well as offline publishers and political parties themselves. The next section analyses from whom data can be requested and which researchers are empowered to request such data.

Table 2. Information vetted researchers can request from political advertising service providers (Articles 17 and 9 PAR), publishers (Articles 17 and 11-12 PAR), and controllers (Articles 20 and 19 PAR).

From whom data can be requested	**What data can be requested**	
Political advertising service providers	Ad context	The ad or campaign with which their service was connected.
		The identity and contact details of the (entity ultimately controlling the) advertiser, and for legal persons, their place of establishment.
		The election, referendum, legislative or regulatory process with which the political advertisement is linked.
	Service	The specific service provided.
	Funding	The amounts they invoiced and the value of other benefits they received for their service.
		The private/public, EU/non-EU origin of these funds.
		Publishers: any information in the transparency notice they are required to have (see Table 1).
Controllers using targeting or ad-delivery techniques	Internal policies	The internal policy describing the use of targeting or ad-delivery techniques (must also be publicly accessible).
		An internal annual risk assessment of the use of targeting techniques or ad-delivery techniques on the fundamental rights and freedoms (must also be publicly accessible).
	Records on the use of targeting	Records on the use of targeting or ad-delivery techniques, the relevant mechanisms and parameters used.
		Whether AI was used to target or deliver a political ad.
		Targeting goals, mechanisms, and logic, including the main parameters used for targeting/exclusion and the reasons for choosing these.
		Categories of personal data used for targeting or ad-delivery.
		Meaningful information on the use of AI in targeting or ad delivery.

3.2.1 From whom can data be requested?

Vetted researchers can request data from political advertising service providers (Article 17 PAR) and controllers (Article 20 PAR). Political advertising service providers are simply defined as any natural or legal person who provides services consisting of political advertising. Given the broad definition of political advertising, this covers a wide array of actors (e.g., influencers, data brokers, PR agencies). However, there are three main exceptions to the political advertising services from which data can be requested. First, intermediary services regulated under the DSA that are provided without payment (monetary or otherwise) (Article 3(g) PAR) are not covered. For the purposes of political advertising, this means that social media companies allowing users to post content for free are not covered (though their advertising services would be); although, if the users themselves receive payment to post political messages on such platforms, they do provide a political advertising service (for a broader discussion on political influencers, see Gregorio and Goanta, 2022). Second, "purely ancillary services" are not covered, as such services complement political advertisement but do not directly influence how it is prepared or distributed (Article 3(6) PAR). The examples listed in the PAR (e.g., graphic/sound design, financing, transportation, sales) indicate that the bar to qualify as an ancillary service is high. This interpretation is bolstered by the PAR's goal of facilitating research into political advertising, which is broadly defined as covering anything from preparation to the ultimate dissemination of a political message. Finally, the information under Article 9 of the PAR (which is most of the information listed in Table 1) may not be requested from micro-undertakings, which can, at most, meet one of the following criteria: a total balance sheet of €350,000, net turnover of €700,000, and an average of ten employees during the previous financial year (Article 3(1) Directive 2013/34/EU).

Furthermore, some of the information researchers may request is only held by political advertising publishers (Articles 11, 12 PAR), a subcategory of political advertising service providers that bring a political advertisement into the public domain. The information that can be requested from publishers is identical to the information that must be included in the ad library. However, while the ad library only includes online political advertisements, researchers have the right to request data from any publisher, including, for example, TV, radio, press publishers, and influencers.

Article 20 of the PAR empowers researchers to request data from controllers that use ad delivery or targeting techniques. The PAR borrows the concept of *controller* from data protection law, where it is defined as the actor that determines the means and purposes of the way data is processed (EDPB, 2020; Finck, 2021). Although the scope of this concept is somewhat contentious, as it determines which actor is responsible for compliance with the GDPR, in the context of the PAR, it is important to note that the European Data Protection Board (consisting of all EU data protection authorities, commonly referred to as EDPB) has maintained that both the parties spreading political advertisements and the platforms distributing them can qualify as controllers (Blasi Casagran and Vermeulen, 2021; EDPB, 2021). Similarly, the PAR explicitly clarifies that in-house activities by political parties are covered by the chapter in which Article 20 PAR is included.

Both controllers and political advertising service providers must provide the requested information as soon as possible (within a month at the latest) and in machine-readable format (if technically possible). Companies may refuse requests that are manifestly unclear, excessive, or concerning information they do not have. They may also charge a reasonable and proportionate fee (at most, the administrative costs of providing the information) if processing the request involves significant costs. Companies bear the burden of proof when they refuse requests or argue providing the information involves significant costs (Article 17 PAR).

3.2.2 Who can request data?

The PAR's data access rights only apply to vetted researchers (as well as members of civil society organisations, political actors, electoral observers, and journalists), the criteria of which are laid out in Article 40(8) of the DSA. They partially cover the personal characteristics of the researcher, who must be affiliated with a research organisation (such as a university) and commercially independent. However, the criteria laid out in Article 40(8) of the DSA primarily concern the specific research that is carried out. While some of the criteria are relatively easy to satisfy, such as the need to disclose the funding of the research, make the results publicly available free of charge, and take appropriate data security and confidentiality measures, others impose substantive limitations. Most notably, research may only be carried out to better understand potential measures to mitigate systemic risks (defined elsewhere in the DSA as the dissemination of illegal content

and risks to issues involving fundamental rights, democracy, and health) and the data and timeframe in which it is provided is necessary and proportionate to the purpose of the research.

Though the criteria in Article 40(8) of the DSA were designed to establish the right to request data provided in Article 40(4) of the DSA, they are a poor fit for the data access right stipulated in the PAR. First, the PAR does not provide any mechanisms through which "vetted researchers" can be vetted. Under Article 40(4) of the DSA, this would be done by the Member State in which the platform from which data is requested is established. The PAR, however, applies to a much broader group of companies and, in any case, does not empower any public authority to vet researchers (a similar issue arises in the context of Article 40(12) of the DSA). Therefore, it seems likely that the company from whom data is requested may reject the request if the researcher does not appear to meet the criteria of Article 40(8) of the DSA, after which the researcher can resubmit their request or attempt to enforce their right to request data through litigation.

Fundamentally, it is questionable whether the limitations imposed on the research carried out by vetted researchers using the PAR are necessary at all. No similar limitations are imposed on civil society organisations, political actors, electoral observers, and journalists who may use the same access right. This indicates that the information covered by the PAR's data access right is not of such a sensitive nature that access must be severely restricted. Pragmatically, it may be easier for researchers to collaborate with civil society organisations if their requests to access data are denied for failing to satisfy the criteria in Article 40(8) of the DSA.

4. How research can support the Political Advertising Regulation

In addition to providing new data for research, the PAR also increases the need for research into political advertising. Below, I highlight three specific areas where research could support political advertising governance.

4.1 Defining political ads

One of the main contributions of the PAR is its introduction of a new definition of political advertising. Introducing such a definition is important, as it reduces platforms' discretion to determine which ads are political and, thus, subject to additional scrutiny and targeting limits. At the same

time, the PAR's definition of political advertising currently leaves much room for interpretation regarding when, exactly, an advertisement is liable and designed to influence voting behaviour or regulatory processes. For example, should a promoted fundraising post by a digital rights NGO, a Patagonia ad calling attention to climate change to sell sustainable jackets, or an ad by a fossil fuel company showcasing their green initiatives be classified as political advertising?

The new definition introduced in the PAR is too vague to provide a definitive answer to these questions. Determining where the line between political and non-political advertisements is drawn in practice is crucial, as this distinction determines what political speech is subject to legal targeting and transparency restrictions and what speech is not. Legal research is necessary to assess how regulators and courts categorise political advertisements. Legal scholars could, for instance, assess how widely courts and regulators apply the PAR's definition of political advertisements, which criteria (according to Article 8(c) of the PAR) are decisive in practice, and how the definition of political advertisements should be understood from a fundamental rights perspective. Equally as important, however, is empirical research into how publishers, particularly platforms, apply the definition of political advertisements. This can offer valuable insights into which aspects platforms prioritise when classifying an ad as political. More broadly, it is essential to assess the effectiveness of platforms' efforts to identify political ads. Since the PAR requires political ads to be labelled and included in the general ad libraries established by the DSA, researchers could potentially scrutinise how effectively platforms identify political ads by comparing the group of ads they classify as political with non-political ads in the ad library. Such an analysis could, for example, reveal how effectively platforms like TikTok—who do not allow political ads—enforce their ban and whether messages from certain types of actors are more often qualified as political advertising (and thus subject to more stringent rules) than those of others communicating about the same issue (e.g., NGOs and fossil fuel companies communicating about climate change).

4.2 When should political advertising be prohibited?

While the PAR mainly relies on transparency to limit the potential negative effects of political advertising, it also bans certain instances of political advertising. Specifically, it bans:

- In the three months before an election or referendum, political advertising by actors that are not EU citizens/permanent residents with voting rights in that election or referendum/companies owned by such citizens or permanent residents (Article 5 PAR).
- Targeting or delivering political ads using data not collected from the data subject by the controller (Article 18(1)(a) PAR).
- Targeting or delivering political ads using data for which individuals have not provided explicit consent for the specific purpose of political advertising (Article 18(1)(b) PAR).
- Targeting or delivering political ads using sensitive data, such as ethnicity, religion, or political opinions (Article 18(1)(c) PAR; Article 9 GDPR).[2]
- Targeting or delivering political ads using data of people whom the controller knows with reasonable certainty to be one year below the voting age (Article 18(2) PAR).

Since these bans change who can pay to communicate with which voters, it is critical that research scrutinises how they do so. At least two topics are particularly worthy of further consideration. First, researchers could assess how the regulatory burden imposed by the PAR strengthens political parties' dependency on platforms and weakens the ability of smaller parties to reach voters. Every party does not have the capability to comply with the PAR's obligations, especially the need to collect data directly from individuals and with their consent to use it for political advertising. Thus, the PAR may inadvertently strengthen the position of actors with the means to collect such data, most notably larger platforms and political parties. Research has already indicated platforms wield significant influence over the political advertising landscape (Dommett et al, 2024; Votta, 2024).

Second, researchers could assess how the PAR shapes individuals' access to political information. This is particularly important regarding prohibitions on using the data of young people and data that reveals an individual's ethnicity, religion, political opinion, or other attributes qualified as sensitive under Article 9 of the GDPR (Blasi Casagran and Vermeulen, 2021; Quinn, 2021). While these bans were imposed to prevent manipulation and discrimination, they may simultaneously make it difficult for political actors to reach out to and mobilise the political power of those groups. The Netherlands, for example, has several small parties representing ethnic or religious groups. Targeted political advertising can be an efficient way to

2 For more information on the GDPR, see Chapter 14 'EU data protection law in action: introducing the GDPR' by Julia Krämer.

reach and build the political power of these smaller groups rather than the general electorate. To better evaluate the proportionality of the PAR's measures to prevent manipulation and discrimination and assess how broad concepts, such as data revealing one's ethnicity or political opinions, should be interpreted, it is crucial that their impact on the access of the affected voter groups to political information is scrutinised.

4.3 Effective labels for political advertisements

In addition to ad libraries and data access requests, labels are an important transparency tool in the PAR's management of political advertising. Their primary function is to ensure the individuals exposed to political advertisements are empowered to make informed choices. To that end, Article 11 of the PAR requires that each political advertisement has a label that:

- Clarifies it is a political advertisement.
- Discloses the identity of (the entity ultimately controlling) the sponsor.
- If applicable:
  - Identifies the election, referendum, or legislative/regulatory process to which the ad is linked.
  - Discloses that the ad has been subject to targeting or ad delivery techniques.
- Links to a transparency notice with further information (see Table 1).

Existing research has clearly shown that the format of the label significantly affects its impact on individuals, particularly because individuals often do not pay attention to the information on the label (Dobber, Kruikemeier, Helberger, et al., 2023; Dobber, Kruikemeier, Votta, et al., 2023). Like other legislation, such as the GDPR, the PAR imposes general requirements that labels are clear and prominent. However, the PAR goes a step further by requiring the Commission to adopt specific, binding rules (an *implementing act*) for the format and template of labels (Article 11(3) PAR). These rules must ensure that labels are adapted to the specific characteristics of the medium on which the political advertisement is disseminated (e.g., radio, TV, or online). They must also account for "the latest technological and market developments, relevant scientific research, and best practices" (Article 12(7) PAR).

In the short term, the PAR creates a pressing need for further research into the best ways to design labels that ensure voters are made aware of the political and targeted nature of the ads they see. Ideally, such research

would also account for the different media platforms (e.g., online videos or text posts, TV, radio) on which users might encounter political ads. In the longer term, the PAR's reliance on labelling raises questions about the effectiveness of such labels as a safeguard against the manipulation of voters. Particular attention should be paid to the effectiveness of different combinations of information criteria and how labels impact different societal groups across various media or in different countries. By identifying where labels might fail to protect voters, such research could help policymakers assess where additional safeguards are needed.

5. Conclusion

The PAR expands our understanding of two key aspects of political advertising. First, the new data access rights provide (albeit limited) insights into the traditionally opaque value chain before a political ad is published. Second, improvements to ad libraries strengthen oversight of the distribution of online political ads by adding data on funding and targeting and by requiring that large platforms include political ads in real-time. Similarly, the ad library operated by the Commission may offer significant functional improvements and facilitate research not only into political ads distributed through large platforms' advertising systems but also into all online political ads, whether from smaller platforms, influencers, websites, or other sources.

Nevertheless, substantial aspects of political advertising transparency remain largely unregulated. No actor has a strong obligation to ensure the data provided to researchers is accurate or complete. Additionally, key aspects of the political advertising process remain hidden from view. For example, advertisers regularly upload datasets to platforms to either target individuals in that dataset (custom audience targeting) or have the platform target individuals that resemble those in the dataset (lookalike audience targeting). Platforms can also exercise significant influence over the way an advertisement is distributed within the target group by the advertiser. The PAR does not make much data available on either of these aspects of the ad distribution process. Therefore, it is crucial to ensure that the increased transparency of political ads, especially those online, does not draw attention away from these aspects of the political process.

References

Animal Defenders International v United Kingdom (2013) 48876/08 [Online]. Available at: https://hudoc.echr.coe.int/eng#{%22tabview%22:[%22document%22],%22itemid%22:[%22001-119244%22]} (Accessed: 9 June 2019).

Ausloos, J., Meiring, A., Buijs, D., et al. (2023) *Information Law and the Digital Transformation of the University: Part II. Access to Data for Research*. Amsterdam: Institute for Information Law [Online]. Available at: https://www.uva.nl/binaries/content/assets/uva/nl/over-de-uva/over-de-uva/beleid-en-financien/digitale-agenda/part-ii-access-to-data-for-research.pdf (Accessed: 22 January 2025).

Ausloos, J., Leerssen, P., ten Thije, P. (2020) Operationalizing Research Access in Platform Governance: What to Learn from Other Industries? AlgorithmWatch [Online]. Available at: https://algorithmwatch.org/de/wp-content/uploads/2020/06/GoverningPlatforms_IViR_study_June2020-AlgorithmWatch-2020-06-24.pdf (Accessed: 22 January 2025).

Bayer, J. (2024) *Digital Media Regulation within the European Union: A Framework for a New Media Order*. Nomos Verlagsgesellschaft [Online]. Available at: https://www.nomos-elibrary.de/10.5771/9783748945352/digital-media-regulation-within-the-european-union (Accessed: 22 January 2025)

Blasi Casagran, C. and Vermeulen, M. (2021) 'Reflections on the Murky Legal Practices of Political Micro-Targeting from a GDPR Perspective', International Data Privacy Law, 11(4), pp. 348–359.

Bodó, B., Helberger, N., Zuiderveen Borgesius, K., Möller, J. (2017) 'Tackling the Algorithmic Control Crisis: The Technical, Legal, and Ethical Challenges of Research into Algorithmic Agents', *Yale Journal of Law and Technology*, 19.

Buri, I., Chapman, M., Culloty, E., et al. (2022) *New Actors and Risks in Online Advertising* (ed. Max Zeno van Drunen). Council of Europe, European Audiovisual Observatory.

Chamon, M. (2018) 'Limits to Delegation under Article 290 TFEU: The Specificity and Essentiality Requirements Put to the Test', *Maastricht Journal of European and Comparative Law*, 25(2), pp. 231–245.

Dobber, T. (2020) *Data & Democracy: Political Microtargeting: A Threat to Electoral Integrity?* University of Amsterdam [Online]. Available at: https://dare.uva.nl/search?identifier=40d14da9-1fad-4b14-81bf-253b417f1708 (Accessed: 22 January 2025).

Dobber, T., Kruikemeier, S., Helberger, N., et al. (2023) 'Shielding Citizens? Understanding the Impact of Political Advertisement Transparency Information', *New Media & Society*, 26(11),pp. 6715-6735.

Dobber, T., Kruikemeier, S., Votta, F., et al. (2023) 'The Effect of Traffic Light Veracity Labels on Perceptions of Political Advertising Source and Message Credibility on Social Media', *Journal of Information Technology & Politics*, 22(1), pp. 1–16.

Dobber, T., Ó Fathaigh, R., Zuiderveen Borgesius, F.J. (2019) 'The Regulation of Online Political Micro-Targeting in Europe', *Internet Policy Review*, 8(4) [Online]. Available at: https://doi.org/10.14763/2019.4.1440 (Accessed: 23 January 2025).

Dommett, K., Kefford, G., Kruschinski, S., et al. (2024) *Data-Driven Campaigning and Political Parties: Five Advanced Democracies Compared. Journalism and Political Communication Unbound*. Oxford, New York: Oxford University Press.

Dubois, P.R., Arteau-Leclerc, C., Giasson, T. (2022) 'Microtargeting, Social Media, and Third Party Advertising: Why the Facebook Ad Library Cannot Prevent Threats to Canadian Democracy' in Garnett, H.A. and Pal, M. (eds.) *Cyber-Threats to Canadian Democracy*. Montreall: McGill-Queen's University Press, pp. 236-269.

Edelson, L., Chuang, J., Franklin Fowler, E., Franz, M., Ridout, T.N. (2021) *Universal Digital Ad Transparency* (No. ID 3898214). Knight First Amendment Institute, New York [Online]. Available at: https://doi.org/10.2139/ssrn.3898214 (Accessed: 23 January 2025).

Edelson, L., Lauinger, T., McCoy, D. (2020) 'A Security Analysis of the Facebook Ad Library', in *2020 IEEE Symposium on Security and Privacy (SP)*, May 2020, pp. 661–678

Edelson, L., Sakhuja, S., Dey, R., et al. (2019) 'An Analysis of United States Online Political Advertising Transparency', *arXiv:1902.04385* [cs]. Epub ahead of print 12 February 2019.

EDPB (2020) *Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR*. September. EDPB [Online]. Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (Accessed: 15 February 2022).

EDPB (2021) *Guidelines 8/2020 on the Targeting of Social Media Users*. 13 April. Brussels [Online]. Available at: https://edpb.europa.eu/system/files/2021-04/edpb_guidelines_082020_on_the_targeting_of_social_media_users_en.pdf (Accessed: 3 March 2022).

ERGA (2021) *Notions of Disinformation and Related Concepts*. ERGA [Online]. Available at: https://erga-online.eu/wp-content/uploads/2021/03/ERGA-SG2-Report-2020-Notions-of-disinformation-and-related-concepts-final.pdf (Accessed: 3 March 2022).

European Partnership for Democracy (2023) 'Civil Society Open Letter on the Ongoing Negotiations Regarding the Regulation of Political Advertising' [Online]. Available at: https://epd.eu/news-publications/civil-society-open-letter-on-the-ongoing-negotiations-regarding-the-regulation-of-political-advertising/ (Accessed: 22 March 2024).

Finck, M. (2021) 'Cobwebs of Control: The Two Imaginations of the Data Controller in EU Law', *International Data Privacy Law*, 11(4), pp. 333–347.

Gregorio, D.G. and Goanta, C. (2022) 'The Influencer Republic: Monetizing Political Speech on Social Media', *German Law Journal*, 23(2), pp. 204–225.

Kaeding, M. and Stack, K.M. (2015) 'Legislative Scrutiny? The Political Economy and Practice of Legislative Vetoes in the European Union', *Journal of Common Market Studies*, 53(6), pp. 1268–1284.

Kirk, N. and Teeling, L. (2021) 'A Review of Political Advertising Online During the 2019 European Elections and Establishing Future Regulatory Requirements in Ireland', *Irish Political Studies*, 0(0), pp. 1–18.

Kreiss, D. and Barrett, B. (2020) 'Democratic Tradeoffs: Platforms and Political Advertising', *Ohio State Technology Law Journal*, 16(2), pp. 493–519.

Kruikemeier, S., Vliegenthart, R., Guldemond, P., van Remoortere, A., Vermeer, S., Vrielink, J. (2023) 'Is Politieke Microtargeting in Advertenties ECHT Gevaarlijk Voor Onze Democratie?', *StukRoodVlees* [Online]. Available at: https://stukroodvlees.nl/is-politieke-microtargeting-in-advertenties-echt-gevaarlijk-voor-onze-democratie/ (Accessed: 23 January 2025).

Leerssen, P. (2023) *Seeing What Others Are Seeing: Studies in the Regulation of Transparency for Social Media Recommender Systems*. University of Amsterdam [Online]. Available at: https://dare.uva.nl/search?identifier=18c6e9a0-1530-4e70-b9a6-35fb37873d13 (Accessed: 23 January 2025).

Leerssen, P., Dobber, T., Helberger, N., et al. (2021) 'News from the Ad Archive: How Journalists Use the Facebook Ad Library to Hold Online Advertising Accountable', *Information, Communication & Society*, 0(0), pp. 1–20.

Marchal, N., Hoes, E., Klüser, K.J., Hamborg, F., Alizadeh, M., Kubli, M., Katzenbach, C. (2024) 'How Negative Media Coverage Impacts Platform Governance: Evidence from Facebook, Twitter, and YouTube', *Political Communication*, 0, pp. 1–19. https://doi.org/10.1080/10584609.2024.2377992.

PAR. (2024) *Regulation (EU) 2024/900 of the European Parliament and of the Council of 13 March 2024 on the Transparency and Targeting of Political Advertising. Official Journal* L, 2024/900, 20.3.2024 [Online]. Available at: https://eurlex.europa.eu/eli/reg/2024/900/oj (Accessed: 23 January 2025).

Quinn, P. (2021) 'The Difficulty of Defining Sensitive Data—The Concept of Sensitive Data in the EU Data Protection Framework', *German Law Journal,* 22(8), pp. 1583–1612.

Schütze, R. (2011) '"Delegated" Legislation in the (new) European Union: A Constitutional Analysis', *The Modern Law Review,* 74(5), pp. 661–693.

TV Vest v Norway (2008) 21132/05, 11 December [Online]. Available at: https://hudoc.echr.coe.int/eng?i=001-90235 (Accessed: 23 January 2025).

Van Drunen, M. (2020) 'The post-editorial control era: how EU media law matches platforms' organisational control with cooperative responsibility', *Journal of Media Law,* 12(2), pp. 166–190.

Van Drunen M., Helberger, N. and Fahy, R. (2024) 'European approach(es) to regulating targeted political advertising: Money, data, and more' in Lilleker, D., Jackson, D., Kalsnes, B., Mellado, C., Trevisan, F., and Veneti, A. (eds.) *Routledge Handbook of Political Campaigning*. London: Routledge, pp. 58-71

Van Drunen, M., Helberger, N., and Ó Fathaigh, R. (2022) 'The Beginning of EU Political Advertising Law: UnifyingDemocratic Visions through the Internal Market', *International Journal of Law and InformationTechnology*, 30(2), pp. 181–199.

Van Drunen, M., Helberger, N., Schulz, W., et al. (2023) *The EU is going too far with political advertising!* [Online]. Available at: https://dsa-observatory.eu/2023/03/16/the-eu-is-going-too-far-with-political-advertising/ (Accessed: 22 March 2024).

Van Drunen, M., and Noroozian, A. (2024) 'How to design data access for researchers: A legal and software development perspective', *Computer Law & Security Review,* 52, 105946.

Van Hoboken, J., Appelman, N., Ó Fathaigh, R., et al. (2019) *The legal framework on the dissemination of disinformation through Internet services and the regulation of political advertising*. Amsterdam: Instituut voor Informatierecht [Online]. Available at: https://www.ivir.nl/publicaties/download/Report_Disinformation_Dec2019-1.pdf (Accessed: 23 January 2025).

Verhaeghe, O. (2024) 'Vlaamse partijen flirten met het toelaatbare in advertenties sociale media', *De Tijd*, 21 May [Online]. Available at: https://www.tijd.be/verkiezingen/federaal/vlaamse-partijen-flirten-met-het-toelaatbare-in-advertenties-sociale-media/10546741.html (Accessed: 23 January 2025).

Votta, F. (2024) *A Dance with Data: Unravelling the Supply and Demand Side of Political Microtargeting*. PhD Thesis. University of Amsterdam.

The EU Directive on Copyright in the Digital Single Market

Lisa Völzmann

Abstract

This chapter provides an introduction or refresher to the key provisions and objectives of the Directive on Copyright in the Digital Single Market (DCDSM) that should be accessible to readers with no prior legal knowledge. The Directive aims to harmonise copyright laws across European Union (EU) Member States to prevent legal fragmentation in the Digital Single Market. This chapter discusses the most debated articles of the DCDSM: Articles 3 and 4, the text and data mining provisions; Article 15, the press publisher's right; and Article 17, the liability of intermediaries. Each article's scope and stakeholders – such as creators, publishers, and platforms – are discussed, followed by the objectives and an up-to-date reception of the provision. This chapter explores the DCDSM's aims of creating legal certainty, enhancing innovation, and protecting a free and pluralistic press, as well as addressing the implications for copyright protection and risks of overblocking.

1. Introduction

1.1 Objective

The Directive, commonly referred to as the DCDSM (e.g. Angelopoulos, 2023, p. 4), CDSM Directive (e.g. Geiger and Jütte, 2021, p. 517), or DSM Directive (Vesala, 2023, p. 355), aims to foster the Digital Single Market and harmonise national copyright laws within the EU (Directive 2019/790, recital 1, 2).

The DCDSM does not overhaul the copyright system and should be understood as an adjustment of existing copyright laws to the digital market. Copyright is fundamentally ruled by national laws, with thirteen EU Directives and two EU Regulations harmonising the legal landscape among Member States. The EU operates on the principle of conferral, meaning ev-

ery law the EU enacts needs to be based on a competence conferred to the EU by the Member States (TEU, 2012, Arts. 4, 5). The legislative basis for the DCDSM is Article 114 in the Treaty of the Functioning of the European Union (TFEU),[1] which gives the EU the competence to create legislation that fosters the single market (DCDSM, 2019, preamble; Proposal for an Directive on Copyright in the Digital Single Market, 2016, p. 4). Article 114 of the TFEU is the legal basis for most EU digital laws, such as the GDPR or Data Act.[2]

Building a European single market, also called an internal or common market, is one of the core objectives of the EU. The single market seeks to guarantee the free movement of goods, capital, services, and people. In 2015, the EU announced the Digital Single Market Strategy, recognising that a single market requires lifting not only physical but also digital borders. The DCDSM aims to remove barriers to the free movement of goods and services by regulating copyright works (Rosati, 2021, pp. 6, 14). To summarise, the Directive's goal is to encourage innovation, creativity, investment, and the production of new content to prevent the fragmentation of the internal market (DCDSM, Art. 1(1), recital 2).

1.2 Legal Nature

As a Directive, the DCDSM is a type of European legislation that needs to be transposed into national law by EU Member States. Consequently, it is addressed to the Member States, while Regulations are directly addressed to citizens, companies, and all other entities in the EU. With the DCDSM, creators, platforms, and users are subject to the national law that is issued on the basis of the Directive by the Member States. In contrast, an EU Regulation would subject them to the European legal act itself. Examples of

1 The DCDSM preamble also cites Art. 53(1) and 62 TFEU as the legal basis, although these are of secondary importance compared to Art. 114 TFEU (cf Rosati, 2021, p. 14). Arts. 53(1) and 62 TFEU provide the legal basis for the recognition of qualifications between Member States and "for the coordination of the provisions laid down by law, regulation or administrative action in Member States concerning the taking up and pursuit of activities as self-employed persons" (*TFEU*, 2012, Art. 53(1)).

2 For more information on the GDPR, see Chapter 14 'EU data protection law in action: introducing the GDPR' by Julia Krämer and Chapter 13 'IoT Data within the Context of the Data Act: Between Opportunities and Obstacles' by Prisca von Hagen.

digital Regulations that apply directly to natural and legal persons in the EU are the Digital Services Act (2022) and Digital Markets Act (2022).[3]

The DCDSM was adopted in April 2019, and the deadline for transposition for the Member States passed on 7 July 2021. However, the last Member State, Poland, implemented the Directive in September 2024. Germany implemented the EU Copyright Directive with the *Gesetz zur Anpassung des Urheberrechts an die Erfordernisse des digitalen Binnenmarktes*, which includes the introduction of the new *Urheberrechts-Diensteanbieter-Gesetz* and amendments to the *Urheberrechtsgesetz*. The latter includes the implementation of Articles 3 and 4 DCDSM (cf *Urheberrechtsgesetz*, 2021, §§ 44b, 60d), which are discussed in the next section.

2. Articles 3 and 4 DCDSM: Text and Data Mining Exceptions

2.1 Scope

Articles 3 and 4 DCDSM include exceptions to copyright and related rights for text and data mining,[4] which is defined in Article 2(2) DCDSM as "any automated analytical technique aimed at analysing text and data in digital form in order to generate information". Article 3 DCDSM provides an exception allowing the reproduction and extraction of information for text and data mining for scientific research purposes.[5] This exception allows research organisations and cultural heritage institutions to perform text and data mining on works to which they have lawful access, meaning the

3 For more information on the Digital Services Act, see Chapter 4 '' by Marie-Therese Sekwenz and Rita Gsenger or Chapter 5 '' by Pascal Schneiders and Lena Auler. Further information on the Digital Markets Act, see Chapter 6 'The brave little tailor v. digital giants: A fairy-tale analysis of the social character of the DMA' by Liza Herrmann.

4 Art. 3(1) DCDSM refers to the right to reproduction under the InfoSoc Directive and the Database Directive, the press publishers' right in Art. 15 DCDSM, and the database right under the Database Directive. Art. 4(1) DCDSM includes rights in computer programs under the Software Directive, alongside the previously mentioned (for further information see Margoni/Kretschmer, 2022, p. 686).

5 Relevant for Article 3 and 4 DCDSM are recitals 5–18. Recitals are part of the preamble of the DCDSM as a European legal text: they are not the binding law itself but give contextual background and interpretative guidance (Klimas and Vaiciukaite, 2008; *TFEU*, 2012, Art. 296). Working with the recitals is valuable for social scientists as they offer a framework that connects the legal text to the socio-political context in which it operates.

content is either freely accessible or access has been granted through a contractual agreement, such as a subscription (DCDSM, 2019, recital 14; Rosati, 2021, pp. 34-35) . An example of a case where a research organisation could use copyrighted material is a team of university researchers that uses a subscription-based database to text and data mine academic journal articles using Python to write a paper on research trends.

Article 4 DCDSM extends text and data mining permissions to other users for any purpose, including commercial use, if the user has lawful access to the data and, additionally, the rightholders have not explicitly reserved their rights. A reservation to make reproductions or extract from a database must be clear and explicit (e.g., machine-readable, DCDSM, 2019, recital 18) to be enforceable, leading to a prohibition of text and data mining for other users.

2.2 Stakeholders

2.2.1 Research Organisations, Cultural Heritage Institutions, and Other Users

A research organisation is an entity that conducts scientific research and operates on a not-for-profit basis or within a public interest mission recognised by an EU Member State (see the exact definition in Art. 2(1) DCDSM). A cultural heritage institution is defined as "a publicly accessible library or museum, an archive or a film or audio heritage institution" (DCDSM, 2019, Art. 2(3)). Article 3 DCDSM limits the beneficiaries of the research exception to those working in the public sector (Manteghi, 2023, p. 448). As a result, individuals and organisations in the private sector, such as journalists, independent researchers, small and medium-sized enterprises (SMEs), and other commercial entities, are not able to conduct text and data mining research under Article 3 DCDSM (Manteghi, 2023, p. 448). However, these other users fall under Article 4 DCDSM.

2.2.2 Rightholders

The term rightholder, which is frequently used in the DCDSM, is not explicitly defined. However, a systematic interpretation suggests that it means natural and legal persons holding copyright or related rights, including directly named authors (e.g. recitals 3, 6, 7 DCDSM). These copyrights are

governed by the national laws of the Member States within the framework established by EU Directives and Regulations. Generally, a copyright is an exclusive right to use and distribute an original work (for more details, see e.g., Ginsburg, 2018). The standard duration of copyright protection in the EU is the author's life plus 70 years after their death (Copyright Term Directive, 2006, Art. 1(1)) .

If the content subject to text and data mining is part of a database, the database right can apply alongside the copyright. The database right is a separate intellectual property right under the EU Database Directive (Database Directive, 1996), which grants a right to the creators of databases who have made "a substantial investment" in "the obtaining, verification, or presentation of the contents" of the database (Database Directive, 1996, Art. 7(1)). This right protects against the unauthorised extraction or re-utilisation of the whole or a substantial part of the contents of a protected database (Database Directive, 1996, Art. 7(1); for more details, see Rosati, 2021, pp. 35-37, 83-85).

2.3 Objectives and Perspectives

2.3.1 Creating Legal Certainty

Articles 3 and 4 DCDSM offer more legal certainty compared to the legal framework before the adoption of the Directive (Manteghi, 2023, p. 446) by clarifying the lawfulness of text and data mining (Geiger and Jütte, 2022, p. 55). The objective of these articles is to ensure greater legal clarity in the execution of text and data mining and thereby create more certainty to encourage innovation in the research community and private sector (DCDSM, recital 8, 18) . Furthermore, Articles 3 and 4 DCDSM aim to prevent fragmentation in the single market because some Member States have already introduced national text and data mining exceptions (European Commission, 2016, § 4.3.1.; Rosati, 2021, p. 39).

2.3.2 Enhancing Innovation

This harmonisation enables cross-border research cooperation and, therefore, fosters the objective of Article 3 DCDSM to facilitate scientific progress and enhance the EU's competitive position as a research area (DCDSM, 2019, recital 10). Article 4 DCDSM is designed to support inno-

vation and artificial intelligence (AI) development across various sectors, as text and data mining is seen as essential for the development and operation of AI (Manteghi, 2023, p. 444). However, one criticism suggests that too few beneficiaries are listed under Article 3 DCDSM. For example, Manteghi (2023, p. 449) proposes expanding the scope of Article 3 DCDSM to allow any person or entity to conduct text and data mining for scientific research, provided they have lawful access to the content.

3. Article 15 DCDSM: Press Publishers' Right

3.1 Scope

One of the most contentious articles of the DCDSM is Article 15 (draft Article 11; Angelopoulos, 2023, p. 4; Dusollier, 2020, p. 1004),[6] which establishes the press publishers' right for the duration of two years from the date of publication (DCDSM, 2019, Art. 15(4)). Article 15 DCDSM gives (1) press publishers, like the French *Le Monde*, an intellectual property right to license the online use of their press publications by so-called (2) information society service providers, like the news aggregator Google News.[7] This means Google News has to obtain a licence from press publisher *Le Monde* before displaying excerpts from press articles on their website. The (3) authors of these press articles can claim an appropriate share of the revenue from press publishers like *Le Monde*.

3.2 Stakeholders

3.2.1 Press Publishers

The Directive does not explicitly define who qualifies as a press publisher. However, recital 55 DCDSM states that the "publisher of press publications should be understood as covering service providers, such as news publishers or news agencies, when they publish press publications within the meaning of this Directive". A press publication within the meaning of the Directive is "a collection composed mainly of literary works of a jour-

6 Relevant recitals for Article 15 DCDSM are 54-49.

7 Cf the decision No. 20-MC-01 of the French competition authority (Autorité de la concurrence, 2024).

nalistic nature" that constitute "an individual item within a periodical or regularly updated publication" with "the purpose of providing the general public with information related to news or other topics" and "is published in any media under the initiative, editorial responsibility and control of a service provider" (DCDSM, 2019, Art. 2(4)). Examples of press publications are daily newspapers, magazines, and news websites (DCDSM, 2019, recital 56), like the above-mentioned *Le Monde* or Spiegel Online. Excluded from the scope are "periodical publications published for scientific or academic purposes, such as scientific journals" (DCDSM, 2019, Art. 2(4), recital 56).

Key exceptions to the scope of Article 15 DCDSM are that the right does not extend to the "private or non-commercial use of press publications by individual users" (DCDSM, 2019, recital 55) and does not apply to the use of hyperlinks to the press publications (DCDSM, 2019, Art. 15(1), recital 57). Additionally, the right does not cover the use of "mere facts reported in press publications" (DCDSM, 2019, recital 57) or individual words or very short extracts of press publications (DCDSM, 2019, recital 58). The use of press publications for the purposes of scientific research is generally exempted, provided that the non-commercial nature of the research activity justifies such use.

3.2.2 Information Society Service Providers

An information society service provider must offer a service that is "normally provided for remuneration, at a distance, by electronic means, and at the individual request of a recipient of services" (DCDSM, Art. 2(5); Directive (EU) 2015/1535, 2015, Art. 1(1)(b); for more details, see Rosati, 2021, pp. 83-85). This broad definition includes a variety of online services, like news aggregators such as Google News, social media networks such as Facebook or X, video-sharing platforms like YouTube, and search engines like Google (*VG Media v Google,* 2017; Furgal, 2023, p. 661). These information society service providers take the content created by authors and other rightholders that is published by press publishers and display it on their websites. The press publisher right aims to enhance the market power of press publishers, allowing them to negotiate more effectively with these large digital platforms.

3.2.3 Authors and Other Rightholders

The fact that press publishers receive a copyright does not affect the authors' copyright. Article 15(5) DCDSM states that authors of works in press publications are entitled to an "appropriate share" of the revenue that press publishers receive for the use of their publications. The implementation of this revenue-sharing mechanism is left to the discretion of EU Member States. For example, Italy determines that authors are entitled to between 2% and 5% of the "fair compensation" they receive (cf Angelopoulos, 2023, p. 33), while Germany mandates that authors should receive a minimum share of one-third of the income the press publisher generated from the use of their copyright rights (*Urheberrechtsgesetz*, 2021, § 87k).

3.3 Objectives and Perspectives

3.3.1 Protecting a Free and Pluralist Press

On a broader level, the press publisher's right is intended to help press publishers continue to provide reliable information and support the "sustainability of the publishing industry" in the digital age (DCDSM, 2019, recital 55), as well as ensuring quality journalism and a "free and pluralist press" (DCDSM, 2019, recital 54). However, Article 15 DCDSM also has received criticism for inhibiting the free flow of information on the internet. Notwithstanding the exceptions mentioned, every use of a press publication would require permission, which raises transaction costs and, ultimately, the display of content (European Copyright Society, 2018, p. 3). This stipulation could negatively impact the freedom of information for the general public.

3.3.2 Shifting Power Dynamics

However, an objective of Article 15 DCDSM is to improve legal certainty (Proposal for an Directive on Copyright in the Digital Single Market, 2016, p. 5) by strengthening the legal rights of press publishers and ensuring that they receive fair remuneration for the use of their publications. Recital 54 DCDSM points out the challenges press publishers face in licensing their publications due to the increase in news aggregators and media monitoring services. While online services, like Google News, rely on reusing

press publications as a key aspect of their business model, press publishers face declining revenues (Rosati, 2021, p. 253). Article 15 DCDSM aims to counter this imbalance by improving the bargaining position of press publishers (Proposal for an Directive on Copyright in the Digital Single Market, 2016, p.5).

However, some argue that Article 15 DCDSM fails to achieve the objective of shifting the power and negotiation imbalance between press publishers and big tech companies, such as Google (Dusollier, 2020, p. 1006; Furgal, 2023, p. 650). This conflict is demonstrated by Google's reaction after France transposed the rights of press publishers into national law. The search engine left press publishers with the choice of either not being featured on the news aggregator and, therefore, losing visibility or granting a free licence (Dusollier, 2020, p. 1006). However, the French competition authority, Autorité de la concurrence, brought four cases, deciding that Google is abusing its dominant position by failing to conduct balanced negotiations. Press publishers' rights become even more critical in the face of the growing use of press publications in AI services like Gemini, formerly Bard (Autorité de la concurrence, 2024).

Additionally, it is argued that the rights of press publishers cause "disproportionate harm to media creators, to smaller publishers, to SMEs" (European Copyright Society, 2018, p. 4). While the bargaining power may improve for big press publishers like *Le Monde* or Spiegel Online, smaller independent publishers are potentially less relevant for information society service providers like Google News or Facebook, leading to fewer negotiations and only a limited shift in power dynamics.

4. Article 17 DCDSM: Intermediary Liability

4.1 Scope

Article 17 DCDSM, known as Article 13 during the drafting stages, is possibly the most controversial provision of the DCDSM (Angelopoulos, 2023, p. 4; Dusollier, 2020, p. 1008; Geiger and Jütte, 2021, p. 517; Metzger et al, 2017, p. 1).[8] Article 17 DCDSM establishes that online content-sharing service providers are directly liable for copyright-infringing content uploaded by their users. Therefore, YouTube (the online content-sharing

8 Relevant for Article 17 DCDSM are recitals 61–84.

service provider) can be held liable if a content creator (the user) uploads the copyright-protected music of a musician (the rightholder) without their permission. Under Article 17 DCDSM, YouTube (the online content-sharing service provider) must obtain authorisation from the musician (the rightholder) for the use of copyright-protected works.

Consequently, online content-sharing service providers need a copyright licence for all the content uploaded through their service (Dusollier, 2020, p. 1010). If they fail to obtain such authorisation, online content-sharing service providers must demonstrate that they have made best efforts to obtain the authorisation and ensure that unauthorised content is unavailable on their services (DCDSM, 2019, Art. 17(4)). If the online content-sharing provider fails to fulfil its obligations, it can be held liable, leading to the obligation to pay damages.

4.2 Stakeholders

4.2.1 Users

The term user is not defined in the DCDSM, but Article 17(1) DCDSM implies that a user is someone who shares copyrighted content through an online content-sharing services provider. A user can also be a copyright holder if they upload original content. However, Article 17 DCDSM regulates copyright infringements, so relevant for the application of the law are cases where, for example, a content creator uses copyrighted music in their videos uploaded to TikTok.

An exception to the intermediary liability is that users can upload and make available copyrighted works as part of their content for the purpose of "quotation, criticism, review" (DCDSM, 2019, Art. 17(7)(a), recital 70) or "caricature, parody or pastiche" (DCDSM, 2019, Art. 17(7)(a), recital 70). Pastiche imitates the style of another work, but other than parody, it pays homage to the original (Diepeveen, 2020). These exceptions protect forms of expression such as memes and parodic videos. The ratio for that is to strike a balance between fundamental rights outlined in the Charter of Fundamental Rights of the European Union: the freedom of expression and the arts of the user and the right to property, including intellectual property, of the rightholders (DCDSM, 2019, recital 70). Further protection of user interests is the complaint and redress mechanism that online content-sharing providers need to put in place to ensure their users can appeal

and seek redress if access to their content is deactivated or the content is removed (DCDSM, 2019, Art. 17(9), recital 70).[9]

4.2.2 Rightholders

Article 17 DCDSM aims to ensure that more of the revenue from user-generated content goes to the rightholder. This chapter explained the term righholder under 2.2.2.

4.2.3 Online Content-Sharing Service Providers

Online content-sharing services providers (OCSSP; e.g. Angelopoulos, 2023, p. 4) are defined by the DCDSM as "a provider of an information society service of which the main or one of the main purposes is to store and give the public access to a large amount of copyright-protected works or other protected subject matter uploaded by its users, which it organises and promotes for profit-making purposes" (DCDSM, 2019, Art. 2(6)). Examples include YouTube, Instagram, Facebook, TikTok, Vimeo, and SoundCloud.[10] Excluded from the OCSSP definition are not-for-profit online encyclopaedias (recital 62 DCDSM), like Wikipedia, and not-for-profit educational and scientific repositories (recital 62 DCDSM), like ArXiv.

Article 17 DCDSM establishes that these OCSSPs are liable for copyright-infringing content uploaded by their users. This is called direct intermediary liability because the intermediary, e.g. YouTube, between the content creator (user) and the musician (rightholder) is liable for the copyright infringement of the user. Under the previous legal framework of Article 14 of the E-Commerce Directive (2000/31/EC), intermediaries were not held responsible for content uploaded by users as long as they had no knowledge of illegal information, which includes copyright infringement but also, for example, hate speech. Intermediaries were only required to promptly remove unlawful content when notified (notice-and-takedown principle), giving them so-called safe harbour status (Dusollier, 2020, p.

9 Platforms with less than three years of operation, an annual turnover below 10 million euros, and less than 5 million unique monthly visitors have fewer obligations (DCDSM, 2019, recital 66, art. 17(6)).

10 However, Spotify does not classify as an OCSSP because it does not store or allow access to content uploaded by users. A digital music distributor must upload the music directly to Spotify (Spotify, 2024).

1010; Geiger and Jütte, 2021, p. 519). The direct intermediary liability of Article 17 DCDSM is seen as a paradigm shift (Geiger and Jütte, 2021, p. 517).

Many voices in the literature argue that online content-sharing providers would need to implement automated filtering, also known as upload filters, to fulfil the obligation to obtain a licence for all copyrighted material uploaded by users and, therefore, prevent them from uploading copyright-infringing content (Geiger and Jütte, 2021, pp. 517, 532). This debate is discussed in the next section.

4.3 Objectives and Perspectives

4.3.1 Risking Overblocking

The most discussed issue relating to Article 17 DCDSM is overblocking, a concern that platforms may over-cautiously and excessively filter user-generated content to avoid liability (Geiger and Jütte, 2021, p. 533), which could stifle free speech and creativity online.

Article 17(8) of the DCDSM states that online content-sharing providers, like TikTok, must not engage in the general monitoring of all user content on their platforms (DCDSM, Art. 17(8). recital 66). This principle was already incorporated in the E-Commerce Directive and cases before the Court of Justice of the European Union (CJEU), such as *Scarlet Extended SA v SABAM* (Case C-70/10) and *SABAM v Netlog NV* (Case C-360/10) reaffirm that general monitoring obligations are not permissible under EU law as they would infringe fundamental rights like the freedom of expression and information of users by restricting lawful sharing and accessing information (Geiger and Jütte, 2021, p. 531).

Poland has contested the DCDSM in the CJEU, claiming that the mandatory use of upload filters to prevent copyright infringement would result in preventive monitoring measures or, colloquially speaking, overblocking (Poland v European Parliament and Council of the European Union, 2022, no. 24) . The judgment of the CJEU in the case of *Poland v European Parliament and Council of the European Union* has established that to comply with EU law, Article 17 DCDSM must be implemented and applied in a balanced manner to prevent the immediate, prior blocking of content that does not clearly infringe copyright (Leistner, 2022). The Court recognised that Member States have some flexibility in how they implement

Article 17 DCDSM but ruled that there must be sufficient protections to safeguard users' rights. For example, the Court supported the ideas behind Germany's regulatory approach (Husovec, 2023, p. 194). The German Urheberrechts-Diensteanbieter-Gesetz (2021, §§ 9, 10) includes procedures for delayed takedowns. To avoid disproportionate blocking, when using automated procedures, certain presumed authorised uses must be made public until the conclusion of a complaints procedure (*Urheberrechts-Diensteanbieter-Gesetz*, 2021, § 9 I, II 1 Nr. 3). Such presumed authorised uses include minor uses of third-party works, such as uses of up to 15 seconds per film work or moving image, or uses of up to 15 seconds per audio track (Urheberrechts-Diensteanbieter-Gesetz, 2021, § 9 II 1 Nr. 3 and § 10 Nr. 1, 2). With such a so-called *de minimis* provision (Forte, 2022, p. 416), mandatory filtering does not equate to a violation of freedom of expression (Poland v European Parliament and Council of the European Union, 2022, Husovec, 2023).

In 2024, five years after the end of the implementation deadline of the DCDSM, Keller (2024) argues, based on the YouTube transparency reports, that overblocking is a marginal problem. He states that the false positive rate for blocking on YouTube amounts to only 0.005%. However, in their study on the impact of Article 17 DCDSM on YouTube copyright content moderation in Germany and France, Dergacheva and Katzenbach (2023, p. 17) find that content diversity is decreasing and copyright takedowns have increased since 2019, with a significantly stronger effect in France, which implemented the DCDSM earlier.

4.3.2 Strengthening Copyright Protection

The objective of Article 17 DCDSM is to contain the exploitation of copyrighted works online (Dusollier, 2020, p. 1008), which is known in policy jargon as "closing the value gap" (Rosati, 2021, p. 308). Article 17 DCDSM aims to encourage "the development of the licensing market", where rightholders can license their content to online content-sharing service providers (DCDSM, 2019, recital 61; European Commission, 2021, p. 6). Whether the copyright protection was strengthened and the value gap was closed remains an unanswered question (Keller, 2024), and we can expect the review of the Directive through the Commission no earlier than 7 June 2026 (DCDSM, 2019, Art. 30(1)).

5. Conclusion

This chapter illustrated that the DCDSM marks a significant shift in regulating digital copyright, striving to balance the interests of users, platforms, press publishers, and rightholders within the Digital Single Market. It emphasised four critical articles in the DCDSM.

Firstly, the chapter explained the text and data mining exceptions in Articles 3 and 4 of the DCDSM. These exceptions allow research organisations and cultural heritage institutions to perform text and data mining for works to which they have lawful access. Additionally, other users can conduct text and data mining if they have lawful access to the data and rightholders have not explicitly reserved their rights. The aim of Articles 3 and 4 DCDSM is to bring legal certainty to text and data mining practices and thereby enhance innovation in the EU internal market.

Secondly, the press publishers right was explained. Article 15 DCDSM gives press publishers, like *Le Monde*, an intellectual property right to license the online use of their press publications by so-called information society service providers, like the news aggregator Google News. The objective of Article 15 DCDSM is to protect a free and pluralistic press and shift power dynamics. However, its effectiveness is unclear.

Thirdly, the chapter outlined Article 17 DCDSM, which establishes the direct liability of online content-sharing service providers, such as YouTube, which must obtain licences for copyrighted content uploaded through their services by users. The implementation of Article 17 DCDSM has sparked significant debate, particularly regarding the potential for overblocking and its impact on freedom of expression. Whether Article 17 DCDSM, in fact, strengthens copyright protection remains to be seen.

The importance of the DCDSM is only amplified by the developments in AI technologies. With the increase of web scraping methods to collect big data from the internet to train large language models (LLMs), attention has shifted from Article 17 DCDSM to Articles 3 and 4 DCDSM (Keller, 2024). In addition, the use of press publications by LLMs has led to recent cases from the French competition authority regarding the rights of press publishers. This development indicates that the DCDSM remains a significant Directive in the EU's digital governance.

References

Angelopoulos, C. (2023) Articles 15 & 17 of the Directive on Copyright in the Digital Single Market Comparative National Implementation Report [Online]. Available at: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4899625 (Accessed: 24 January 2025).

Autorité de la concurrence (2024) *Related rights: the Autorité fines Google €250 million*, 20 March [Online]. Available at: https://www.autoritedelaconcurrence.fr/en/article/related-rights-autorite-fines-google-eu250-million (Accessed: 27 October 2024).

Dergacheva, D. and Katzenbach, C. (2023) 'Mandate to overblock? Understanding the impact of the European Union's Article 17 on copyright content moderation on YouTube', *Policy & Internet*, 16(2), pp. 362-383.

Diepeveen, L. (2020) *Parody and pastiche* [Online]. Available at: https://doi.org/10.1093/acrefore/9780190201098.013.1106 (Accessed: 24 January 2025).

'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')' (2000) *Official Journal* L 178, 17 July, pp. 1–16. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed: 19 January 2025).

'Directive 2006/116/EC of the European Parliament and of the Council of 12 December 2006 on the term of protection of copyright and certain related rights' *Official Journal* L 372, 27 December, p. 12–18 [Online]. Available at: http://data.europa.eu/eli/dir/2015/1535/oj (Accessed: 24 January 2025).

'Directive (EU) 2015/1535 of the European Parliament and of the Council of 9 September 2015 laying down a procedure for the provision of information in the field of technical regulations and of rules on Information Society services (codification)' (2015) *Official Journal* L 241, 17 September, p. 1–15, [Online]. Available at: http://data.europa.eu/eli/dir/2015/1535/oj (Accessed: 24 January 2025).

'Directive (EU) 2019/790 of the European Parliament and of the Council of 17 April 2019 on copyright and related rights in the Digital Single Market and amending Directives 96/9/EC and 2001/29/EC' (2019) *Official Journal* L 130, 17 May, p. 92–125 [Online]. Available at: http://data.europa.eu/eli/dir/2015/1535/oj (Accessed: 24 January 2025).

'Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases' (1996) *Official Journal* L 77, 27 March, pp. 20–28 [Online]. Available at: https://eur-lex.europa.eu/eli/dir/1996/9/oj/eng (Accessed: 27 January 2025).

Dusollier, S. (2020) 'The 2019 Directive on copyright in the digital single market: Some progress, a few bad choices, and an overall failed ambition', *Common Market Law Review*, 57, pp. 979–1030.

'EU copyright directive proposal' (2016) [Online]. Available at: http://data.europa.eu/eli/dir/2015/1535/oj (Accessed: 24 January 2025).

European Commission (2016) Commission Staff Working Document—Impact assessment on the modernisation of EU copyright rules—Part 1, SWD(2016)301 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016SC0301 (Accessed: 24 January 2025).

European Commission (2021) *Guidance on Article 17 of Directive 2019/790 on copyright in the digital single market.* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52021DC0288 (Accessed: 27 January 2025).

European Copyright Society (2018) Opinion on the proposed press publishers right [Online]. Available at: https://europeancopyrightsociety.org/wp-content/uploads/2018/06/2018_european-copyright-societyopinionpresspublishersright.pdf (Accessed: 27 January 2025).

Forte, G. (2022) 'Just a little bit: Comparing the de minimis doctrine in U.S. and German copyright regimes', *Arizona Journal of International & Comparative Law*, 39(3), pp. 415–442.

Furgal, U. (2023) 'The emperor has no clothes: How the press publishers' right implementation exposes its shortcomings', *GRUR International*, 72(7), pp. 650–664.

Geiger, C. and Jütte, B.J. (2021) 'Platform liability under Art. 17 of the copyright in the digital single market directive, automated filtering and fundamental rights: An impossible match', *GRUR International*, 70(6), pp. 517–543.

Geiger, C. and Jütte, B.J. (2022) 'Conceptualizing a "right to research" and its implications for copyright law: An international and European perspective', Joint PIJIP/TLS Research Paper Series No.7-2022 [Preprint]. [Online]. Available at: https://ssrn.com/abstract=4414085 (Accessed: 27 January 2025).

'Gesetz über die urheberrechtliche Verantwortlichkeit von Diensteanbietern für das Teilen von Online-Inhalten* (Urheberrechts-Diensteanbieter-Gesetz - UrhDaG)' [Online]. Available at: https://www.gesetze-im-internet.de/urhdag/BJNR121500021.html (Accessed: 26 January 2025).

'Gesetz über Urheberrecht und verwandte Schutzrechte (Urheberrechtsgesetz)' (2021) [Online]. Available at: https://www.gesetze-im-internet.de/urhg/BJNR012730965.html (Accessed: 26 January 2025).

Ginsburg, J. (2018) 'Copyright', in R. Dreyfuss and J. Pila (eds.) *The Oxford handbook of intellectual property law*. Oxford University Press, pp. 487–516.

Husovec, M. (2023) 'Mandatory filtering does not always violate freedom of expression: important lessons from Poland v council and European parliament', *Common Market Law Review*, 60(1), pp. 173–198.

Keller, P. (2024) 'Article 17 – five years later', Kluwer Copyright Blog [Online]. Available at: https://copyrightblog.kluweriplaw.com/2024/06/07/article-17-five-years-later/ (Accessed: 27 January 2025).

Klimas, T. and Vaiciukaite, J. (2008) 'The law of recitals in European Community legislation', *ILSA Journal of International & Comparative Law*, 15.

Leistner, M. (2022) 'The implementation of Art. 17 DSM Directive in Germany – A primer with some comparative remarks', *GRUR International*, 71(10), pp. 909–923.

Manteghi, M. (2023) 'In search of balance: Text, data mining and copyright in the Digital Single Market Directive from a fundamental rights perspective', *European Law Review*, 48(4), pp. 443–457.

Metzger, A. et al (2017) 'Selected aspects of implementing Article 17 of the Directive on copyright in the digital single market into national law – Comment of the European Copyright Society' *SSRN* [Online]. Available at: https://ssrn.com/abstract=3589323 (Accessed: 27 January 2025).

'Poland v European Parliament and Council of the European Union', Case 401/19 (2022). *Official Journal* C 237, 20 June, p. 2 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62019CA0401 (Accessed: 26 January 2025).

Rosati, E. (2021) *Copyright in the digital single market: Article-by-article commentary to the provisions of Directive 2019/790*. Oxford University Press.

Spotify (2024) 'Getting music on Spotify'. Available at: https://support.spotify.com/uk/artists/article/getting-music-on-spotify/ (Accessed: 23 October 2024).

'Treaty on the Functioning of the European Union' (2012) *Official Journal* C 326, 26 Oct ber, pp. 47-390 [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:12012E/TXT:en:PDF (Accessed: 26 January 2025).

Vesala, J. (2023) 'Developing artificial intelligence-based content creation: Are EU copyright and antitrust law fit for purpose?', *International Review of Intellectual Property and Competition Law*, 54, pp. 351–380.

'VG Media Gesellschaft zur Verwertung der Urheber- und Leistungsschutzrechte von Medienunternehmen mbH v Google Inc.' (2017) *Official Journal C 309*, 18 September, pp. 21–22 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62017CN0299 (Accessed: 26 January 2025).

The European Media Freedom Act. A Redoubt for Pluralism in an Increasingly Concentrated Landscape

Adelaida Afilipoaie & Heritiana Ranaivoson

Abstract

Concentration in the media sector has long been recognised as posing potential risks to pluralism. However, it was not until the Regulation (EU) 2024/1083 (the European Media Freedom Act, hereafter, EMFA) entered into force on 7 May, 2024, that "media pluralism" was addressed in an EU regulation. Notably built on the Audiovisual Media Services Directive (AVMSD), the EMFA seeks to address several key challenges to media pluralism by establishing a set of rules and mechanisms to promote media pluralism and independence. However, as it lacks a specific legal basis to intervene on cultural matters, it tends to use the reasoning of internal markets to do so. Examining the EMFA more closely, it quickly becomes apparent that its main focus is on news media, which is also revealed through the analysis of its Art. 22, placed at the core of this chapter. The obligatory involvement of National Regulatory Authorities (NRAs) in media merger assessments and the addition of the so-called "media pluralism test" are not without challenges, starting from the potential and vague recognition of video-sharing platforms (VSPs) and very large online platforms (VLOPs) as media service providers, as well as the reference to accounting for the "online environment" in the assessments and the extension to the somewhat symbolic involvement allocated to the NRAs. Although assessments under Art. 22 seem more suitably fitted to mergers involving traditional media, the reference to VSPs and VLOPs as potential media service providers invites more aspirational avenues. Nevertheless, the EMFA appears to advance transparency obligations, harmonising certain aspects pertaining to media merger assessments based on media pluralism reasoning, and recognising the key role played by NRAs in upholding national media laws and pluralism objectives.

1. Introduction

Media pluralism is widely recognised as a precondition of contemporary democracies (European Commission et al, 2022a). This multi-faceted notion combines the plurality of media ownership and sources (Valcke, 2011) with the diversity of content produced, distributed, and eventually consumed by citizens (Helberger, Karppinen and D'Acunto, 2018). Among the many goals of pluralism are the aims to foster political agreements, increase transparency, empower civil society, mitigate social conflicts, and pressure legal institutions to adhere to the rule of law. Pluralism attunes with editorial independence – both of which are necessary conditions for free information. Governance, regulatory frameworks, and ownership patterns within the media landscape play a crucial role in dictating how information is produced, distributed, and consumed (Karppinen, 2013).

However, media industries are characterised by high levels of concentration, with profound social, cultural, and political implications (Peruško, 2010; Mancini, 2018). Trappel and Meier (2022) argued that the consolidation trend among both the media and telecom companies has endangered the flows of information, diversity, and pluralism of views and opinions, thereby heightening social inequality. Yet, the relationship between media concentration and pluralism is ambiguous (Ranaivoson, 2019). Harcourt and Picard (2009, p. 4) argued that "the normative assumption that greater diversity of content and greater pluralism will exist when there is less concentration seems common sense. However, the explicit link of concentration to lower diversity of content and pluralism has never been established". Haraszti (2011, p. 14) referred to media pluralism as "everything from media types, interests such as ownership and control over the media, political and cultural viewpoints, and regional concerns, all of which have to be communicated or accessed through the media". There are several dimensions of media pluralism, including internal and external aspects. Reporters Sans Frontiers (2016) defined internal pluralism as the plurality of voices, analyses, expressed opinions, and issues within an outlet or organisation, and external pluralism as encompassing the number of outlets, disparate types of media, and the coexistence of privately and publicly owned media. Another dimension is viewpoint diversity, which, in contrast to internal pluralism, refers to the presence of different and competing perspectives across multiple media outlets, encompassing the entire media system. However, viewpoint diversity is not necessarily a consequence of external pluralism, nor is external pluralism required to secure it.

There are alternative ways to ensure that a concentrated market remains pluralistic, (e.g., competition or media law, support mechanisms, financial incentives, etc.). However, Helberger (2018) and Muñoz Larroa (2019) pointed out that the issue does not actually lie with the existence of a lack of diversity of supply and content, but rather with the diversity of media content that audiences are exposed to due to content filtering, the prioritisation and suppression of content, and recommendation algorithms which reinforce filter bubbles. These phenomena may reduce exposure diversity, a concept that deals with audiences' exposure to, consumption of, and engagement with a plurality of content. This concept was initially proposed by Napoli (1997) and has reappeared in more recent debates concerning media pluralism, concentration, and online platform power (Helberger, 2018; Seipp et al, 2023).

Moreover, in the borderless digital world, the principles of democracy and pluralism face both great opportunities and new challenges. For instance, Brogi et al (2021) argued that a greater number of players is not equivalent to an increased plurality, because online platforms emphasise specific content types and sources tailored to each individual user, which significantly influences their information choices. The power exercised by the so-called "internet information gatekeepers", who control information flows and "impact participation and deliberation in democratic culture" (Laidlaw, 2010, p. 266), is one of the reasons behind the heightened interest in promoting and protecting pluralism, as reflected in recent EU initiatives.

However, the EU lacks the explicit authority to regulate media, which forms part of the field of culture and is thus under the sole competence of the Member States, whose holding of regulatory prerogatives over their media sector has resulted in a fragmented regulatory approach (European Commission et al, 2022a). Although the EU does not have the exclusive legal basis to regulate the media sector, Art. 6 of the Treaty (TFEU) (Treaty on the Functioning of the European Union, 2012), confers the EU with the competence to "carry out actions to support, coordinate or supplement the actions of the Member States". Besides, the EU has the power to adopt laws to ensure that the internal market can function in such a way as to achieve that objective. To do so, it had to use Art. 114 TFEU[1] to propose the EMFA. This allowed the European Commission (hereafter,

1 Art. 114 TFEU is primarily used for harmonising regulations across the EU Member States in areas that affect the free movement of goods, services, capital, and people within the EU.

the Commission) to respond to the calls it had been receiving from other EU institutions for the past four decades for EU-wide regulatory action to address barriers to the functioning of the internal media market and to promote pluralism while safeguarding independence in the media market. However, except for the Council Directive 89/552/EEC (1989) Television Without Frontiers (TWFD) and its successor, Directive (EU) 2018/1808 (2018) Audiovisual Media Services Directive (AVMSD), the Commission's intervention remained outside secondary EU law.[2]

Art. 1 of the EMFA highlights that its scope is to "lay down common rules for the proper functioning of the internal market for media services", thus highlighting the threat posed by the fragmented national regulations as a prime reason for its intervention. Along these lines, the EMFA argues that the fragmentation of media ownership rules and the restrictions found at the national level can hinder media market players' operation and expansion across borders. Different approaches to media pluralism and editorial independence also hamper free movement, as does the occasionally-biased allocation of economic resources, such as public funds. However, the EMFA's recitals, alongside the Explanatory Memorandum (European Commission, 2022b) and the Recommendation (European Commission, 2022) accompanying the Regulation, repeatedly and explicitly refer to the objective of protecting the freedom of the media, freedom to provide (media) services, media pluralism, and editorial independence. In essence, the EU wishes to regulate pluralism and media freedom to respond to democratic threats, but, in so doing, it advances tortured arguments about regulating pluralism for economic reasons.

Beyond its recitals, the EMFA places media pluralism at its core, particularly in its Section 5 – Requirements for well-functioning media market measures and procedures – which was inspired by the issues identified following a public call for evidence[3] consultation (European Commission, 2021). Section 5 proposes to protect media pluralism by highlighting Mem-

2 In the context of the EU legal system, the Commission operates within two main types of law: primary law (i.e., foundational treaties and legal agreements that establish the EU, its institutions, and the overall legal framework) and secondary law (i.e., regulations, directives, decisions, recommendations, and opinions).

3 Among these respective issues, 81% of the 900 contributors found the safeguards for media independence and pluralism unsatisfactory. Therefore, academic institutions, companies, business associations, citizens, non-governmental organisations (NGOs), public authorities, and trade unions agreed to the need for regulatory convergence and cooperation between independent media regulators.

ber States' obligation to designate NRAs to assess the impact of media market concentrations on media pluralism and editorial independence. These NRAs – potentially designated among existing media regulators – are to conduct a separate assessment from the merger review conducted by the National Competition Authorities (NCAs). In certain cases (and as discussed further in Section 5), the NRAs will be assisted by the European Board for Media Services (the Board) and the Commission. As stipulated in Art. 8, the Board is established as a replacement and successor of the European Regulators Group for Audiovisual Media Services (ERGA) – which had a narrower scope for action limited to audiovisual media services only – and is composed of NRA representatives.

The remainder of the chapter discusses the following. First, we define the EMFA and its objectives. Second, we introduce Section 5 on media concentration and the link/risk to pluralism and independence. Once done, with the help of the Media Plurality Monitor's (MPM) market plurality indicators and the Commission's Recommendation accompanying the EMFA, we dissect Art. 22(2) lit. (a) to lit. (e). An outcome of this analysis is the identification of some of the necessary information that could help NRAs with their assessments.

2. Safeguarding media pluralism at the EU level

Starting in the 1980s, various EU Green Papers and Opinions have launched discussions on the possibility of coordinating certain media provisions at the EU level, including talks on safeguarding pluralism. In 1985, the Economic and Social Committee (that is, the EU's consultative body) stated that regulating the media structure should rest with the Member States so as to ensure that pluralism of information and opinions in the Union would not be threatened. The Commission then placed the protection of pluralism in the hands of the Member States, arguing that national arrangements can safeguard pluralism. In 1992, the Commission adopted a Green Paper on "Pluralism and media concentration in the single market. An assessment of the need for Community action", as a response to the Parliament's request to the Commission to propose measures aimed at preventing concentrations in the media sector from endangering media pluralism (Commission of the European Communities, 1992). Yet,

the Commission saw no need for a Community legislation[4] to safeguard pluralism, arguing that national regulatory frameworks would be better positioned to do so. The Commission's stance may have been influenced by how media policies fall under the jurisdiction of Member States – the latter generally being extremely hesitant to relinquish such jurisdiction. Still, at the EU level, coordination and harmonisation of various media-related provisions were agreed upon and established in the 1989 TWFD and its (revised) successor, the AVMSD. Both Directives linked media pluralism to competition, as unfair competition and concentration were recognised as threats to media pluralism.

To return to the same 1992 paper, the Commission recognised the importance of media ownership restrictions for safeguarding pluralism, explicitly nuancing that they cannot be replaced by applying general competition law – and, in particular, merger control. This was due to competition law having been established from an economic perspective. The Court of Justice of the European Union (CJEU), when dealing with case decisions, has repeatedly postulated that the assessment of concentrations must be done in accordance with the "economic outcome attributable to the concentration which is more likely to ensue" (Venit, 2013, p. 127). Art. 21(4) of the Regulation (EC) 139/2004, referred to as the EC Merger Regulation (The Council of the European Union, 2004) allows Member States to include in their merger assessments additional measures to protect legitimate interests, such as media plurality, as well as other public interests that must be recognised by the Commission. Although not focused on creating pluralism and diversity in the media, merger control can indirectly contribute to it by ensuring the proper functioning of competition in the internal market and the decentralisation of market power in the hands of the many, which reduces the control and power one entity can exercise over opinion-forming.

As the responsibility of media policies was placed in the hands of the Member States, current media-specific policies greatly vary across them – as shown in our prior research (Afilipoaie and Ranaivoson, 2023), where

4 Community legislation refers to the body of laws created under the framework of the former European Communities – which were part of the precursor organisations to the European Union, such as the European Economic Community (EEC) and the European Coal and Steel Community (ECSC). These laws were binding across Member States and essential for implementing and regulating the common policies of the Communities.

we systematically mapped all the media-specific policies and regulations, including national competition laws across all Member States, to identify the measures limiting media ownership.[5] These rules focus on "traditional" media, and rarely encompass online platforms. This reality, reinforced by the legacy media for EU regulatory interventions in the digital landscape to ensure a regulatory level playing field and fairer competition (Enli et al, 2019), fructified with the EU spearheading its digital regulatory agenda, thus paving the path for harmonisation.

In terms of the special assessments of media merger measures, we have previously highlighted (Afilipoaie and Ranaivoson, 2022) that half of the Member States involve their NRAs in national media concentration assessments, who conduct their analyses solely on pluralism grounds.[6] However, in that same research, we criticised the effectiveness of such a system, as, except for certain Member States,[7] the NRA's assessment and opinion is mostly non-binding, and easily outweighed by authorities with higher powers. As we will see, the EMFA is unlikely to change this limitation, as neither the NRAs', the Board's, nor the Commission's opinions in these cooperative assessments are legally binding. Notwithstanding, it attempts to harmonise the current situation, as all Member States must establish such a cooperation procedure and conduct their assessments based on given criteria. The EMFA goes far beyond the special requirements for the media merger assessments at the forefront of this chapter. Concisely summarised by Cabrera Blázquez (2022, p. 3), these objectives are:

- "to ensure that media companies can operate in the internal market subject to consistent regulatory standards, including as regards media freedom and pluralism,
- ensure that EU citizens have access to a wide and varied media offering both offline and online,

5 Following this mapping, we propose a typology of measures with various limits, including media ownership restrictions, special assessments of media mergers, and measures restricting capital control and the actors allowed to own media companies. The latter safeguards (as much as is possible) media companies' independence from various forms of capture (i.e., media or state capture) (Dragomir, 2019; Schiffrin, 2021).

6 Involving NRAs alongside NCAs in these assessments creates a decentralised and more holistic cooperative assessment system where the concentrations are reviewed not only on competition grounds, but also on the basis of pluralism.

7 However, even in these Member States, the NRAs rarely oppose NCAs' decisions and make use of their binding power (see the country cases in European Commission et al, 2022a).

- safeguard the editorial independence and independent management of the media, which is a precondition of media freedom and of the integrity of the internal market,
- foster undistorted competition between media companies by ensuring a transparent and fair allocation of state resources".

3. The European Media Freedom Act (EMFA)

The EMFA (The European Parliament and the Council, 2024) – which entered into force on 7 May, 2024[8] – was first announced as an initiative during Commission President Ursula von der Leyen's State of the Union address in 2021.[9] The EMFA proposal builds upon the European Democracy Action Plan presented in December 2020, the latter of which aims to support free and independent media, enhance media resilience, ensure transparency in media ownership across the EU, and create safer working conditions for all media professionals.

The EMFA was born from the need to tackle four main identified problems in the internal market: (i) fragmentation of national rules on media pluralism; (ii) insufficient cooperation and convergence among independent media regulators; (iii) public and private interference in the ownership, management, and operation of media outlets; and (iv) lack of media pluralism safeguards, including those found online (Cabrera Blázquez, 2022). Not only does the EMFA lay down the first-ever EU harmonised rules on media freedom and independence, but it does so in the form of a directly applicable Regulation.

8 While the EMFA entered into forced on 7 May, 2024, it is only applicable from 8 August, 2025 onwards, with some exceptions to Art. 3, Art. 4(1) and (2), Art. 6(3), Arts. 7–13, Arts. 14–17, and Art. 28 applying at various dates before 8 August, 2025, and Art. 20 applying from 8 May, 2027. The difference between the dates of entry and applicability is that, in the first case, the regulation has legal existence, but is not enforceable. This means that, before the date of applicability, obligations or privileges can neither be exercised nor enforced. The in-between period is meant to allow time for parties to, among other actions, prepare their systems, processes, procedures, and documentation for compliance with the new rules.

9 The address also announced the call for evidence for an impact assessment and the Council of the European Union's conclusions on safeguarding a free and pluralistic media system, and on strengthening the promotion of European audiovisual industry.

The EMFA includes 78 recitals, followed by 29 articles structured into 4 chapters.[10] The matters covered include, but are not limited to, the protection of editorial freedom and independence of media service providers, thereby safeguarding journalistic sources and confidential communications against intrusive surveillance (Art. 4); the adequate and stable funding, and independent functioning of, public service media providers (Art. 5); the development of national media ownership databases containing information on media service providers (Art. 6); the protection of online media content produced according to professional standards against unjustified takedowns (Art. 18); the user's right to customise the media offering on devices and interfaces, enabling them to modify the default settings to reflect their own preferences (Art. 20); transparency obligations for providers of audience measurement systems (Art. 24); and the assessment of media market concentrations (Art. 22), on which our chapter focuses.

Upon the EMFA's initial publication, it was accompanied by a non-binding Recommendation establishing several voluntary best practices collected from the sector and geared at promoting editorial independence and greater ownership transparency (European Commission, 2022). Media service providers were encouraged to draw inspiration from the non-exhaustive catalogue of voluntary measures aimed at improving their resilience, and Member States were prompted to take actions to promote media ownership transparency.

3.1 Explaining Section 5 of the EMFA

As highlighted in Recital 63, the EMFA sets out a common framework for assessing media market concentrations across the Union to ensure that media service providers operate in an internal market with reduced obstacles. Moreover, Recital 6 underlines that the insufficient tools for regulatory cooperation between NRAs or bodies could negatively affect this market. To safeguard media pluralism, some Member States have taken regulatory measures, but, in so doing, have contributed to the divergence of approaches. As mentioned in Recital 7, this has increased he risks of endangering

10 Chapter I includes the general provisions (Arts. 1–2), Chapter II incorporates the rights and duties of media service providers and recipients of media services (Arts. 3-6), Chapter III covers the framework for regulatory cooperation and a well-functioning internal market for media services (6 sections comprising Arts. 7–25), and Chapter IV includes the final provisions (Arts. 26–29).

free movement in the internal market. Under this reasoning, Recital 7 highlights the need to harmonise certain aspects of national rules related to media pluralism and editorial standards. According to prior research (Afilipoaie and Ranaivoson, 2022), when NRAs and ministries intervene in media merger assessments, they do so based on media pluralism and often public interest, which are merely mentioned in national laws and rarely explained (Afilipoaie and Ranaivoson, 2022). This lack of definitions and criteria, coupled with various heterogeneous assessment frameworks, results in increased uncertainly for the merging parties. Therefore, Section 5 of the EMFA, titled 'Requirements for well-functioning media market measures and procedures', aims to harmonise these divergent approaches. The section consists of three articles. Art. 21 addresses the justification and proportionality of national measures, and outlines the reasoning behind the Board's and the Commission's interventions. Alongside providing an appeal mechanism, Art. 21 also obliges Member States to set out in advance clear timeframes for the procedures and applications of any legislative, regulatory, or administrative measure, which must be reasoned, transparent, objective, and non-discriminatory. Art. 22 deals with NRAs' assessments of national media market concentrations and the roles and procedures therein. Art. 23 gives the Board and the Commission the power to cast their opinions on media market concentrations in the absence of such assessments when the concentration is likely to affect the functioning of the internal market for media services.

3.2 The EMFA's approach to media pluralism and the link with the Media Plurality Monitor

The EU has long been committed to promoting media pluralism, recognising it as vital for the functioning of democratic societies. It has sought to ensure that media across the continent remains free, independent, and diverse through combining legal frameworks, financial programs and such monitoring tools as the MPM (European Commission, n.d.), the EU's most prominent initiative. The MPM is conducted by the Centre for Media Pluralism and Media Freedom (CMPF) at the European University Institute (EUI), co-financed by the EU. The CMPF publishes yearly reports on the four main areas of risk to media: basic protection of media freedom, market plurality, political independence, and social inclusiveness. More specifically, in this chapter, we use the MPM's market plurality indicators. As with the

evolution of the MPM, the indicators evolve and adapt to the challenges of the digital age.

This risk-based approach of the MPM also informs the EU Rule of Law reports, particularly the chapter on media pluralism and freedom (European University Institute, 2022). This is worth mentioning as 22(d) of the EMFA encourages NRAs to consider the reports' findings in their assessments. Moreover, the MPM's findings are notably cited in Recital 7 of the EMFA. According to Elda Brogi (2020, p. 3), the scientific coordinator of the CMPF:

> The peculiarity of the MPM is that it does not prefer a notion of media pluralism; instead, it builds on the different national and European traditions and definitions to elaborate a set of indicators that tend to cover all possible aspects involved in the definition of media pluralism in a broad European sense [...] It relies on a broad definition of media pluralism that entails legal, economic, and socio-political aspects. It therefore takes a holistic approach that considers all the different nuances of the definition of media pluralism.

Similarly, while the EMFA does not define the term *media pluralism*, it does exemplify through its non-legally binding Recital 64 that media pluralism refers to "the possibility to have access to a variety of media services and media content which reflect diverse opinions, voices and analyses". Recital 29 states that media pluralism can be promoted by "producing a wide range of content that caters to various interests, perspectives and demographics and by offering alternative viewpoints and programming options, which provides a rich and unique offering". Generally speaking, media ownership concentration is perceived as a threat to media pluralism, as it results in the market being controlled by the few, resulting in less competition, which can, in turn, lead to content homogenisation, reduction in the range of viewpoints, and increased political and commercial influence, all of which ultimately influence the formation of public opinion. Art. 22 takes a similar stance, arguing that media concentrations could significantly impact media pluralism and editorial independence.

The harmonisation propositions stipulated in Art. 22(2) lit. (a) to lit. (e) share strong similarities with the MPM's risk indicators related to market plurality. These include sub-indicators concerning the transparency of media ownership, plurality of media providers, plurality in digital markets, media viability, and editorial independence from commercial and owners' influence (European University Institute, 2024). In light of the above, the MPM should be considered a highly useful instrument for more deeply

understanding Art. 22 of the EMFA, especially in terms of the criteria proposed for the pluralism test, as it considers many of the same problems.

3.3 Delving into Art. 22 of the EMFA: assessment of media market concentrations

This chapter focuses on Art. 22, the first section of which (1) highlights the obligation for Member States to lay down (in their national laws) substantive and procedural rules to allow for the assessment of media market concentrations that could significantly impact media pluralism and editorial independence. Thus, it is up to the Member States to decide the significance of this criteria for themselves. Moreover, Art. 22(2) presents an exhaustive list of elements in lit. (a) to lit. (e) which NRAs must include in their assessments. The purpose of these elements is to harmonise the criteria used by the NRAs, colloquially referred to as the "pluralism tests". Art. 22(3) to (6) lays down the roles and procedures of the Board's and Commission's involvement in these assessments. For clarification, we here delve into the occasionally vague and obscure elements of the assessments proposed in Art. 22(2).

The roots of Art. 22 lay in the results of the study on online media plurality and diversity (European Commission et al, 2022a), which highlighted the lack of cooperation systems in media merger assessments across the EU. Building on the above-mentioned study – to which we served as contributors – we identified various cooperation typologies and represented them hierarchically as a power pyramid, with Ministries and NCAs occupying more powerful positions than NRAs, which typically have non-binding advisory competencies in most legislations (Afilipoaie and Ranaivoson, 2022). According to our research, due to NRAs' opinions being generally non-binding, they do not significantly influence the final decisions. Art. 22 does not specify whether the assessment is binding or not, leaving it up to the Member States to decide the powers allocated to NRAs. Nevertheless, this power hierarchy will likely remain.

Art. 22 introduces a requirement for Member States without a cooperative assessment system in place to designate an NRA responsible for, or substantively involved in, the assessment, and to establish substantive and procedural rules in national law. Art. 22(2) harmonises these assessments based on exhaustive criteria, offering some legal certainty to the merging parties, as Art. 22(1)(d) and (e) stipulates that the Member States shall "set

out in advance objective, non-discriminatory and proportionate criteria for notifying such media market concentrations and for assessing the impact on media pluralism and editorial independence […] and specify in advance the timeframes for completing such assessments".

Under the EMFA, these regulatory cooperative assessments of media market concentrations[11] apply if the latter can significantly impact media pluralism and editorial independence. Under the EMFA, a media service provider is an individual or legal entity that professionally engages in providing a media service, with editorial responsibility over the content. This means that they decide what content is included, organised, presented, or distributed within their media services. The EMFA applies to traditional players[12] as well as to digital platforms, such as streaming and on-demand services.[13]

Exactly how the EMFA considers VSPs (e.g., YouTube) could revive a heated debate about their editorial control, or lack thereof. There have been long debates concerning the "neutral" conduct of VSPs across academic circles. While VSPs have consistently declared that they simply host content on their platforms and have no editorial control, academic research has stated otherwise (see, for example, Napoli and Caplan, 2017; Picard and Pickard, 2017; Beckett, 2019; Barwise and Watkins, 2018). Moreover, Mansell (2015, p. 3) argued that online platforms are not "neutral 'conduits' for traffic and hosts for content creators […] [t]hey have the power to influence what ideas citizens are able to find easily and whether the notion of a public sphere for democratic dialogue can be sustained into the future as the media ecology increases in complexity". In 2018, when the AVMSD was last revised, Art. 1(1)(aa) explicitly defined VSPs as having no editorial control over the content uploaded by their users. Besides, more recently, VSPs seemed to have won the debate in judgements by the CJEU. According to Frank Peterson v. Google LLC and Others, and Elsevier Inc. v Cyando AG. (2021) – joined cases concerning the liability of online platforms for

11 Art. 2(15) of the EMFA defines media concentrations as involving at least one media service provider or one online platform providing access to media content.

12 For example, TV and radio broadcasters, such as the BBC or VRT; news media organisations, including their print and digital versions (e.g., *The Guardian* or *Le Monde*); and digital native media, whose online communication is the primary focus, such as Business Insider or Politico.

13 Netflix or Hulu are two examples, both producing or curating such editorial content as documentaries and deciding on the organisation of their catalogues.

copyright infringements carried out by their users – platforms could qualify as "neutral" hosts (Reda and Selinger, 2021).

However, through Recital 11 and the definition of a media market concentration under Art. 2(15), the EMFA combines VSPs and VLOPs[14] (e.g., Facebook) under the definition of a media service provider, thereby giving NRAs the task of reviewing the mergers involving these platforms under the pluralism test. Recital 11 of the EMFA reads that "[i]n the digital media[15] market, video-sharing platform providers or providers of very large online platforms could fall under the definition of media service provider" if they exercise editorial control over a section or sections of their services.[16] Nevertheless, NRAs often face uncertainty over categorising VSPs and VLOPs as media service providers, which can constrain their participation in the assessment.

4. Analysis of Art. 22(2) lit. (a) to lit. (e)

4.1 Art. 22(2)(a)

> […]the expected impact of the media market concentration on media pluralism, including its effects on the formation of public opinion and on the diversity of media services and the media offering on the market, taking into account the online environment and the parties' interests in, links to or activities in other media or non-media businesses.

Art. 22(1) stipulates that NRAs should only conduct the pluralism test (following the elements proposed in Art. 22(2) in media market concentrations that could significantly impact media pluralism and editorial independence. Albeit abstract, lit. (a) proposes that NRAs should follow these specific

14 Art. 33 of the Regulation (EU) 2022/2065 (2022) Digital Services Act (DSA) classifies platforms with over 45 million monthly users in the EU as VLOPs and have to abide by certain obligations. According to the Commission (2024), as of 19 September, 2024, there were 23 designated VLOPs under the DSA.

15 Digital media is any form of media that uses electronic devices for distribution (see Recital 3 of the EMFA).

16 Recital 11 mentions the key role that VSPs and VLOPs play in organising content using automated means or algorithms, but this characteristic does not seem to be explicitly considered a form of editorial control. Yet, through this automated organisational control, such platforms shape the visibility of content and decide on its distribution, thus controlling the actual architecture in which users consume content (Helberger, 2020; van Drunen, 2021). In a platform context, it is clear that editorial control transcends the traditional editorial practices in the editorial rooms.

avenues for their impact assessments, which include references to the online environment. By definition, a concentration arises where there is a change of control on a lasting basis resulting from the merger of two or more previously independent companies or parts of companies. Lit. (a) suggests that some (significant) change of control can impact the formation of public opinion and diversity. By breaking down lit. (a), the pluralism test covers aspects related to two interrelated points: (i) ownership and (ii) diversity and opinion-formation power.

4.1.1 Ownership and beyond

The first point, "the parties' interests in, links to or activities in other media or non-media businesses", includes matters of ownership, links to governmental institutions, interest groups, any capital holdings, and political links and activities. Horizontal,[17] vertical,[18] cross-media,[19] and conglomerate concentrations[20] are different forms of media ownership concentration that describe how the control of media outlets and resources is structured within a market. Different forms of media ownership raise different concerns to media pluralism and competition. For example, the matter of cross-media ownership has long been debated in academia, as this type of ownership can lead to a concentration of power that enables one entity to influence the distribution of information. Accordingly, Harcourt and Picard (2009) argued that limitations to cross-media ownership are necessary to curb excessive power over public opinion. When the media is concentrated in the hands of a few, the risk of content homogenisation increases (Hendrickx and Ranaivoson, 2019), which affects the range of information and perspectives available, and thus ultimately shapes public opinion. However, Evens and Donders (2018, p. 107) noted that "diversification through cross-media ownership allows broadcasters or distributors to reduce risks and benefit from economies of scope", arguing that such restrictions should be kept to a

17 A horizontal merger occurs when a company, such as a newspaper, acquires an outlet of the same type of media, such as another newspaper.

18 A vertical merger occurs when a company controls different stages of the production and distribution process within the same media industry, such as a newspaper that acquires a printing press.

19 A cross-media merger occurs when a company, such as a newspaper, acquires different types of media outlets, such as a television station or a radio channel.

20 A conglomerate media merger occurs when a larger conglomerate that owns businesses in various industries acquires a media company.

minimum, especially considering the challenges posed by online platforms that traditional media must navigate. While cross-media ownership can lead to scale, efficiencies, synergies, and a broader audience reach, it can also raise concerns over the reduced diversity of viewpoints and media concentration, prompting many Member States to regulate it so as to protect media pluralism and democracy at large.

In the virtual sphere, ownership departs from the traditional media landscape and is characterised by unprecedented scale and concentration, data-driven strategies, global reach, platform dominance, decentralised content creation, regulatory challenges, and novel economic models. This means that NRAs must also take those "online environment" characteristics into account when conducting their assessments. To conduct such ownership measurements, cooperation between the merging parties and the national authorities, alongside reporting transparency, is key.

In the online environment, an ownership assessment extends beyond direct ownership (e.g., capital shares) or reach (e.g., market or audience shares) and spans to indirect financial support and technological dependencies, which tend to fall outside of the scope of traditional regulatory tools (Fanta and Dachwitz, 2020). Seipp et al (2023, p. 1558) stated that, considering the platform context and the new tools available with which to reshape audience attention, "ownership is no longer concerned with owning shares or control over cable networks or programme content but is more about ownership or control over data, algorithms, and infrastructures". Afilipoaie, Donders and Ballon (2022) noted that more recent online platform merger assessments consider data, patents, API interoperability, and gatekeeping as signs of power. The MPM's indicators have been fine-tuned to account for the everchanging digital environment, such as by including risk indicators for cross-media concentration online.[21] In this case, concentration metrics focus on revenues (e.g., subscriptions, membership, donations, advertising, public funding) rather than audience shares due to the latter's heterogeneity, lack of methodological transparency, and incomparability across entities and markets.

The MPM also enquires about the financial structure reporting obligations in both the media and digital sectors. However, transparency obligations of financial and ownership structures, especially for digital native news media, are practically inexistent, as these are not captured by existing national laws (Ranaivoson and Rozgonyi, 2023). Moreover, there

21 That does not include aggregators, social networks, and intermediaries.

are no media ownership restrictions in the online media sector, and no transparency obligations in terms of structural and financial disclosures. These aspects thus make it challenging for NRAs to consider the online environment.

4.1.2 Diversity and opinion-formation power

The second and third points, "diversity of media services and the media offering on the market", address internal and external pluralism, focusing on the risks of market concentration affecting public opinion – despite there being no straightforward connection. Media is recognised for its public opinion-forming power, which directly impacts citizens' democratic participation and societal well-being (Harcourt and Picard, 2009). Accordingly, traditional media, such as broadcasting, radio, and newspapers, became highly regulated. However, in the online world, the dangers of influencing people's opinions increase manifold because of the greater risks posed by "knowledge (data) and the tools to command and organize online attention, and the ability to use that data and algorithmic tools for persuasion" (Helberger, 2020, p. 846). Moreover, the speed and reach of (dis)information circulation top those of traditional media. This is why Helberger (2020) described social media platforms as "wielders of considerable opinion power" (p. 843), but lacking the accountability of legacy broadcasters (Moore, 2016).

The shift in media power dynamics (van Dijck, Poell and de Waal, 2018) reduced the role of traditional gatekeepers, such as journalists and editors, who once decided on the content most relevant to the public. Instead, these decisions are in the hands of technology companies that, with the help of data and algorithms, shape user profiles and direct information flows, with implications for how news is produced, distributed, and consumed. Thus, the dynamics of opinion power are shifting in favour of powerful online entities (Dodds et al, 2023; Kristensen, 2023). Simon (2022) added that artificial intelligence (AI) adoption will further increase news organisations' dependence on platforms.

Despite the risks for the diversity of services and offerings, Recital 64 of the EMFA reads that "[a]n important criterion to be taken into account is the reduction of competing views within that market as a result of the media market concentration". This alludes to the fact that NRAs can positively assess media mergers if internal pluralism (i.e., competing views) is maintained, even if external pluralism (i.e., the number of outlets) is reduced.

This aligns with Picard and Zotto (2015, p. 62), who opined that "pluralism is about sustaining representation of different political viewpoints and forms of cultural expression within a society", which is not necessarily dependent on the number of existing outlets. This belief resonates with Barnett (2010b), who, over a decade ago, suggested a switch from a structural regulation (that prevents greater ownership concentration) to a content regulation strategy, which imposes substantial public interest obligations on the content output of media businesses in return for a more relaxed corporate environment. Therefore, to lead to a positive NRA assessment, the merging parties should demonstrate how their internal pluralism (i.e., opinions, voices, and analyses) will be safeguarded post-merger. Although foregrounding internal, over external, pluralism represents a relatively novel approach, the discussion changes when online platforms are added to the equation. With only a few dominant platforms, concerns emerge about their effects on external plurality (i.e., platform market concentration and the sustainability of news media considering platform dominance), internal diversity (content moderation, ranking, and recommendation systems), exposure diversity, and the degree to which users independently make information choices today (Brogi et al, 2021). These factors must be considered in media concentration assessments as they reflect the realities of the online environment.

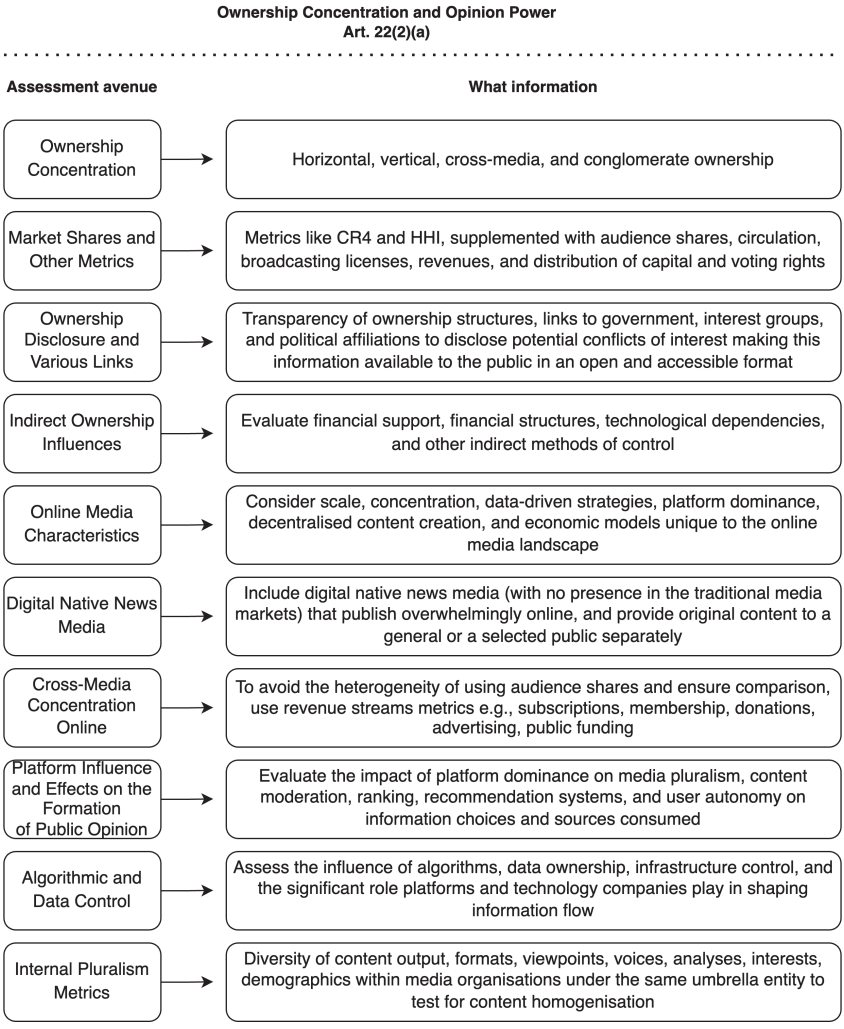

Figure 1. Overview of the necessary information to assess the ownership concentration and opinion power. Source: Authors

4.2 Art. 22(2)(b)

> "the safeguards for editorial independence, including the measures taken by media service providers with a view to guaranteeing the independence of editorial decisions." (Art. 22(2)b EMFA)

4.2.1 Editorial independence

Picard and Zotto (2015) argued that, beyond media ownership, the real concern is interference with democratic and social processes. Journalists play a crucial role in the functioning of a democratic society by informing and influencing public opinion. However, commercial interests and owners' influence can threaten editorial independence, as highlighted in Art. 22(2(b).

Structural ownership does not quite paint the whole picture, with indirect influences, such as financial support, also representing ways to exercise control. The MPM's "transparency of media ownership" indicator underlines that ownership information of news media, including digital native news media, should be publicly accessible so as to more easily expose potential conflicts of interest, political affiliations, and the "ultimate beneficial owners" (UBO)[22] of the media entity. The public has the right to know who has the capacity to influence editorial production and interfere with the journalistic profession, and the right to use this information in the selection of outlets (Reporters Sans Frontiers, 2016). Many Member States have restricted the categories of actors who can own media entities to prevent their politicisation.[23] While regulations and restrictions can safeguard tools for media sectors, editorial independence can also be ensured via self-regulatory measures, such as codes of conduct or ethics, editorial guidelines, and charters, as well as by excluding media owners from the editorial decisions.

22 Directive (EU) 2015/849 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, also referred to as the Anti-Money Laundering directive (AML), introduced UBO registers, which are databases containing information about persons who ultimately own or control the customer and/or the natural person on whose behalf a transaction is being conducted. The UBO is always a natural person.

23 Restrictions often involve public administration personnel, family members, and board members of the public service media (PSM), NCAs, and NRAs (European Commission et al., 2022a). These restrictions are a defensive mechanism against media and state capture (Dragomir, 2019).

Nevertheless, Art. 22(2)(b) gives media service providers a relatively free hand to take the measures they deem appropriate.

4.2.2 Editorial independence in practice

There are various risks to editorial independence. The MPM's risk indicator, "Editorial independence from commercial and owners influence", assesses risks by examining the regulatory safeguards in place in the appointment and dismissal procedures of editors-in-chief, ensuring their independence from the media entity's commercial interests. On this matter, the Recommendation emphasises the role of internal independent bodies in protecting the editors-in-chief's autonomy. The MPM also assesses the risk of commercial interference and considers the safeguards implemented to deter journalists from basing their editorial decisions on commercial interests. This is covered in the Recommendation, which also mentions that editorial content should be separated and clearly distinguishable from advertising and promotional content. The MPM's variables also include the existence and effectiveness of measures separating editorial and journalistic content from marketing, advertising, and other commercial activities inside the same news organisation.

The same MPM risk indicator directly refers to Art. 6(3)(b) of the EMFA on the "duties of media service providers" to enquire whether their owners must disclose any potential conflicts of interest that could affect editorial content. It questions whether owners or other commercial entities abstain from influencing editorial decisions. In the digital sphere, commercial influence includes clickbait content and self-promotion. The Recommendation further include safeguards related to the human, consultation, and participation rights of journalists to allow newsroom workers to be involved in management decisions (among others), all which are part of a toolbox of voluntary measures for media companies to consider. These are linked to Art. 22(2)(e), which allows parties to propose commitments to prevent and address concerns raised by NRAs. However, transparency and effective enforcement are critical.

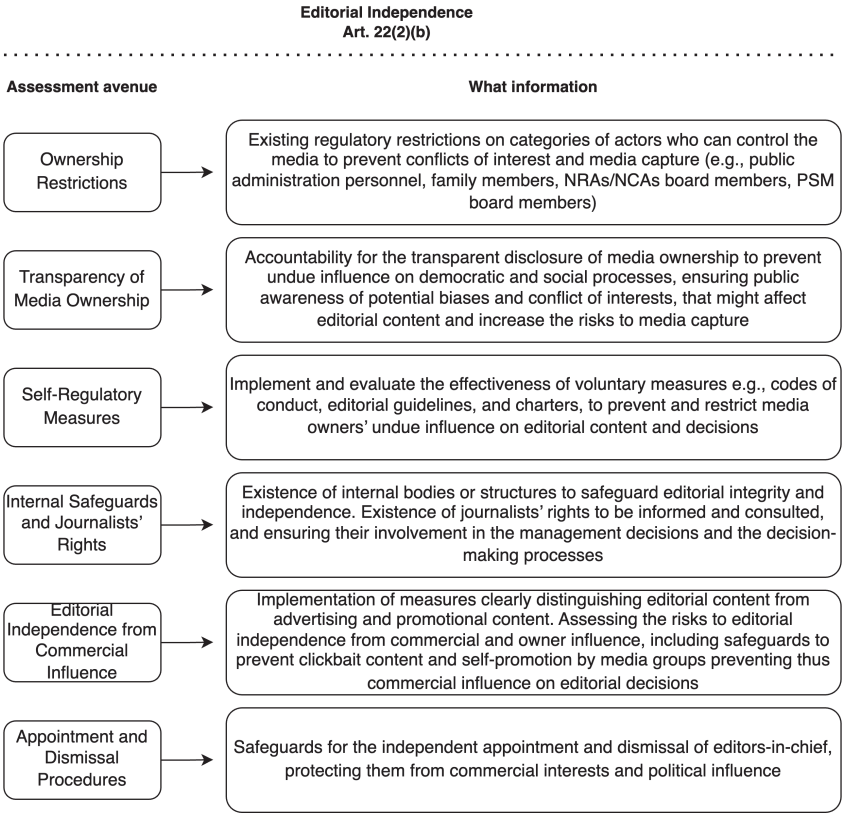

Figure 2. Overview of the necessary information to assess the editorial independence. Source: Authors

4.3 Art. 22(2(c)

> "whether, in the absence of the media market concentration, the parties involved in the media market concentration would remain economically sustainable, and whether there are any possible alternatives to ensure their economic sustainability." (Art. 22(2)c EMFA)

4.3.1 Economic sustainability

Mergers and acquisitions often present the only viable option for survival (Barnett, 2010a; Evens and Donders, 2018). Barnett (2010a) highlighted

that, to protect pluralism and diversity, regulators need to ensure that the structures themselves do not go extinct in the first place. Art. 22(2)(c) alludes to a similar idea, as it is possible that, without the merger, the less economically viable outlet might cease to exist – a risk that NRAs will have to consider in their verdict, which could make them more susceptible to approve it, despite the merger leading to more concentration.

Economic sustainability in the media sector enhances market entry, competition, and supply diversity, which in turn supports demand diversity and democratic principles. The news sector's sustainability depends on its ability to invest, innovate, and monetise data and content. Traditional media's two-sided business models, based on audience and advertising revenues, face pressure from digital platforms. Furthermore, the widespread availability of free online news has decreased consumers' willingness to pay for news content (European Commission, 2023). These structural changes have strained news media's business models, requiring them to find ways to adapt and diversify their income streams for longevity. Yet, the current layoffs and revenue reductions, in both the number of companies and their investments (Kim et al, 2021; Peterson and Dunaway, 2023), suggest that this task is far from easy.

4.3.2 Assessment of economic sustainability

Evaluating the economic sustainability of both the acquirer and acquiree (i.e., the parties to the transaction), can be a challenging process as it depends on a variety of internal and external factors.[24] The MPM considers the sustainability of the news media production as a pre-requisite for media pluralism and diversity. One of the three media viability indicators looks at revenue trends, measuring viability by analysing (among other aspects) advertising, subscriptions, crowdfunding, donations, and State funding trends.[25] Brogi and Sjøvaag (2023) identified contextual advertising[26] as

24 Such factors are dependent on market conditions, future innovation, competition, business models, and short- vs. long-term profitability, among others.

25 The MPM considers these revenue trends separately for the audiovisual, radio, newspaper and press agencies, digital native media, and local media.

26 Contextual advertising involves displaying advertising based on the content of the webpage the user is viewing. Contrary to targeted advertising, the method does not rely on tracking user behaviour, but rather aligns with the context of the content being consumed. Research by the Commission (2023) suggests that such content-based advertising can lead to increased revenue for news media organisations.

an alternative to targeted advertising, the latter being based on users' personal data. The use of alternative revenue sources, such as crowdfunding, paywalls, subscriptions, donations, and philanthropy, suggest that media outlets are hoping to find viable business models. Investment in innovative business models and AI tools for journalism and experimenting with content innovation in the newsrooms[27] are further signs of the sustainability and resilience of media organisations.

The second media viability indicator employed by the MPM addresses the employment and salary trends of journalists, which serves as a proxy for the quality of information supply. Layoffs and salary cuts may indicate a struggling media outlet. A reduced personnel could ultimately become too overburdened to keep pace with the work, which could lead to an output of lower quality.

The third way to assess an entity's viability is by considering the existence of public financial incentives to support media pluralism, correct market failures, and ensure diverse viewpoints.[28] Brogi and Sjøvaag (2023) stated that direct, transparent, objective, and predictable government support tools,[29] alongside indirect support measures,[30] are crucial for the sustainability of news media. All Member States offer some form of direct or indirect support to their news media, and some have started to extend this support to online news media as well (European Commission et al, 2022a). Considering the challenges of online platforms faced by media outlets, Brogi and Sjøvaag (2023) discussed novel, economically oriented

27 Based on the categories proposed by Posetti (2018) for the Oxford Reuters Journalism Innovation Project, innovations could consider experimentation with storytelling and reporting (e.g., reassessing what constitutes a story), audience engagement (e.g., moving beyond clicks and shares to audience participation), new content distribution strategies (e.g., beyond social platforms and search engines), technology and products (e.g., newsroom-borne tools and solutions), people and culture (e.g., skills development and training), organisation and structure, leadership and management (e.g., support from the top that permits innovation), structural innovations (e.g., workflows, reporting lines, interdepartmental collaboration), and other forms of non-business-related innovations. These MPM uses these categories in their yearly questionnaire to identify newsroom innovation.

28 To avoid market distortions, such national public support is closely overseen by the Commission, as stipulated in Art. 107 TFEU, which generally prohibits State aid unless exceptionally justified (Buts and Jegers, 2012).

29 Subsidies or support for distribution are common.

30 Favourable taxation schemes in the forms of reduced VAT and other fiscal incentives, such as targeted tax breaks, are among such indirect support measures.

policy support approaches.[31] To ensure that NRAs are aware of the possible struggles of media outlets, it should ask the merging parties to submit the information pertaining to their economic (in)viability as part of their notification documentation.

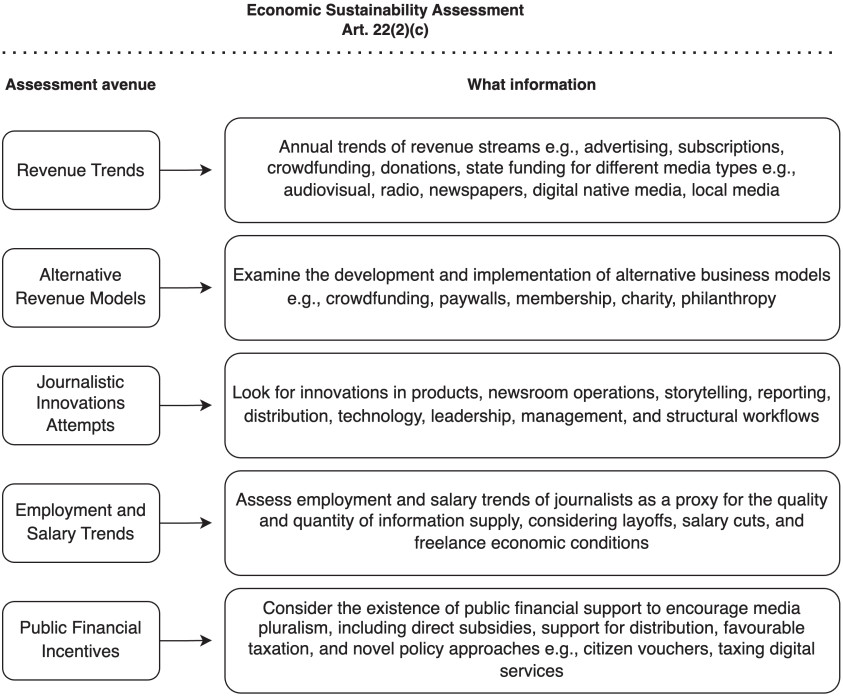

Figure 3. Overview of the necessary information to assess the economic sustainability. Source: Authors

4.4 Art. 22(2)(d)

> "where relevant, the findings of the Commission's annual rule of law report concerning media pluralism and media freedom." (Art. 22(2)d EMFA)

31 Their suggestions include the allocation of vouchers to citizens to support their preferred news media by purchasing subscriptions, allowing them to claim tax benefits for supporting their chosen outlet (this could especially be the case when the outlet has a non-profit status), or taxing digital services to redirect these funds to support public interest journalism.

At the request of the European Parliament, since 2020, the Commission's annual Rule of Law report presents a synthesis of the rule of law situation in the EU, which includes media freedom and pluralism among its four main topics (Directorate-General for Justice and Consumers, 2020). These reports rely on various information sources, and often cite the empirical findings of the MPM country reports. As seen above, the MPM's indicators serve as a baseline for explaining the possible pluralism and independence tests envisaged by lit. (a), (b), and (c), suggesting that the EMFA was built on and informed by the EU's long-standing commitment to monitor, protect, and promote media pluralism.

Initially, the EMFA proposal did not reference the Rule of Law reports as part of the NRAs' pluralism test. However, the European Parliament amended Art. 22(2) in order for NRAs to include, where relevant, its findings. Both the MPM and the Rule of Law reports consider similar risk indicators and the existing media regulatory frameworks[32] implemented by the Member States. The revealed threats are recognised as creating and maintaining vulnerabilities, as well as elevating the risks to media pluralism, editorial independence, and fair competition (Fathaigh, 2020). Both the MPM and the Rule of Law reports contain recommendations for improvements, which are readdressed to inspect the progress in the following country reports.

Despite the value of these reports, EU auditors and lawmakers have voiced their concerns over their lack of transparency and accountability, including their susceptibility to political influence, thus potentially limiting the Rule of Law reports' reliability (Griera, 2024). Additionally, the general nature of these reports may lack the specificity needed for thorough media concentration assessments, making Art. 22(2)(d) more symbolic than substantive. The figure below includes the considerations accounted for in the chapter on media freedom and pluralism of the Rule of Law Reports, which NRAs can consult "where relevant".

32 For an overview of the existing media ownership rules across all the Member States, see Afilipoaie and Ranaivoson (2023).

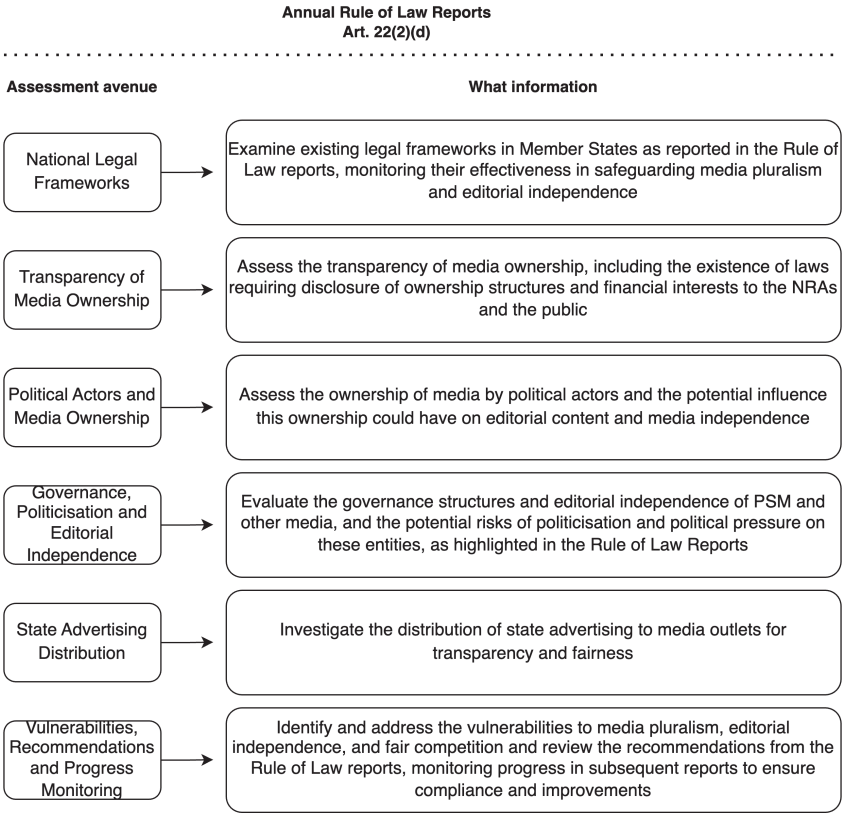

Figure 4. Overview of the Rule of Law Reports' information that could be used "where relevant". Source: Authors

4.5 Art. 22(2)(e)

> "where applicable, the commitments that any of the parties involved in the media market concentration might offer to safeguard media pluralism and editorial independence." (Art. 22(2)e EMFA)

The original EMFA proposal contained no references to possible commitments (also known as remedies) as enshrined in lit. (e). Commitments are essential in competition law cases in both ex-ante and -post[33] reviews. In

33 Ex-post (or, antitrust) assessments are usually made amidst instances of abuse of dominance or evidence of cartels and collusion. These ex-post investigations are usu-

the context of merger assessments, conducted ex-ante, commitments ensure that companies partaking to the merger take certain actions to ensure that the merger will not harm competition. The merging parties can, at their own initiative, offer these remedies, or the authority conducting the assessment can ask for commitments as a precondition for the merger's approval.[34,35] The Commission's (2022) Recommendation lacks guidance on what constitute acceptable commitments.[36] However, as each merger case differs, so will the commitments proposed by the merging entities or required by NRAs.

The analyses of lit. (a) and (b) presented in this chapter allude to potential commitments. For example, in the protection of editorial independence, as seen in the explanation of lit. (b), editorial content is recommended to be separated and clearly distinguishable from advertising and promotional content. The Recommendation encourages media service providers to promote the participation of editorial staff members (or their representative bodies) in the decision-making process.[37] Thus, internal reconfigurations, guidelines, and transparent steps in the decision-making process could be proposed as commitments in the eventuality of NRAs' concerns.

Lit. (a) mentions that, in their analyses, NRAs shall consider the online environment, and the concentration's effects on pluralism, diversity, and the formation of public opinion. The wording of lit. (a), where it speaks of

ally triggered by complaints, whistleblowers, or suspicious behaviour. In these cases, investigations occur after the company's anticompetitive conduct has taken place. Such commitments often accompany fines and the cessation of infringing activities.

34 The notifying parties to a merger must sign a document containing commitments to be respected for an agreed-upon period. Usually, these commitments do not exceed 10 years.

35 For example, in the case of the M.8124 Microsoft/LinkedIn merger, alongside other commitments, Microsoft agreed to not oblige Windows PC original equipment manufacturers (OEM) to install LinkedIn on the PCs for a period of five years. The commitments sufficed to obtain the Commission's approval.

36 For example, the Regulation (EU) 2022/2560 on foreign subsidies distorting the internal market provides a non-exhaustive list of possible commitments in case the Commission finds the subsidy to be possibly distortive.

37 Such involvement is proposed in certain cases and could take the form of information rights (i.e., changes to the composition of the management board, replacing the editor-in-chief, major changes to the legal form or the ownership of the media service provider), consultation rights (i.e., when appointing a new editor-in-chief and agreeing on an applicable consultation procedure), participation rights (i.e., members of the editorial staff being allowed to participate in management by electing representatives in the managing board), or a combination thereof.

"taking into account the online environment", is very broad, yet we make use of the Council of Europe's (2018) Recommendation,[38] which points out that media content is "increasingly managed, edited, curated and/or created by internet intermediaries", meaning that Member States must recognise the varying degrees in which those internet intermediaries impact media pluralism using automated processes and encourage these players to act. These actions points include improving transparency in automated processes and assessing and improving these automated processes to ensure that users are exposed to a broad diversity of media content. Although a Recommendation document at the time, this wishful thinking has now been laid down in EU regulation. Art. 27 of the DSA on recommender systems' transparency, requires all online platforms using such systems to explain, in their terms and conditions, the parameters[39] used in their recommender systems and make available a functionality that allows the service's recipient to select and modify their preferred option.[40] Although only applicable to VLOPs and VLOSEs, this explainability requirement goes hand in hand with the systemic risk assessment stipulated in Art. 34 of the DSA,[41] as these platforms must assess the risks of "any actual or foreseeable negative effects for the exercise of fundamental rights, in particular [...] to freedom of expression and information, including the freedom and pluralism of the media enshrined in art. 11 of the Charter" (Charter of Fundamental Rights of the European Union, 2016) and mitigate such risks.[42]

38 CM/Rec(2018)1 on media pluralism and transparency of media ownership.

39 Under Art. 27(2), these explanations shall include at least: (a) the most significant criteria for determining the information suggested to the recipient of the service; and (b) the reasons for the relative importance of those parameters.

40 This provision aims to help users comprehend how specific information is prioritised for them and how their online behaviour impacts the recommendation of products, services, or content. However, a paradox exists between this transparency goal and the reality, meaning that users often skim or ignore online terms and conditions, which are typically lengthy and complex, thus limiting the efficacy of this notice policy (Obar and Oeldorf-Hirsch, 2020).

41 Art. 34(2) DSA identifies the factors influencing such systemic risk, which are: a) the design of their recommender systems and any other relevant algorithmic system; b) their content moderation systems; c) the applicable terms and conditions and their enforcement; d) systems for selecting and presenting advertisements; and e) data related practices of the provider. For more information on risk assessment in the DSA, see Chapter 4 'The Digital Services Act: Online Risks, Transparency and Data Access' by Marie-Therese Sekwenz and Rita Gsenger.

42 These risk assessments must occur at least every year and in any event prior to deploying functionalities likely to have a critical impact on the risks identified.

These provisions can serve as inspiration for potential commitments attached to concentration notifications, which also target legacy media and smaller online platforms. Nevertheless, effective enforcement mechanisms must be in place to ensure that the commitments are upheld.

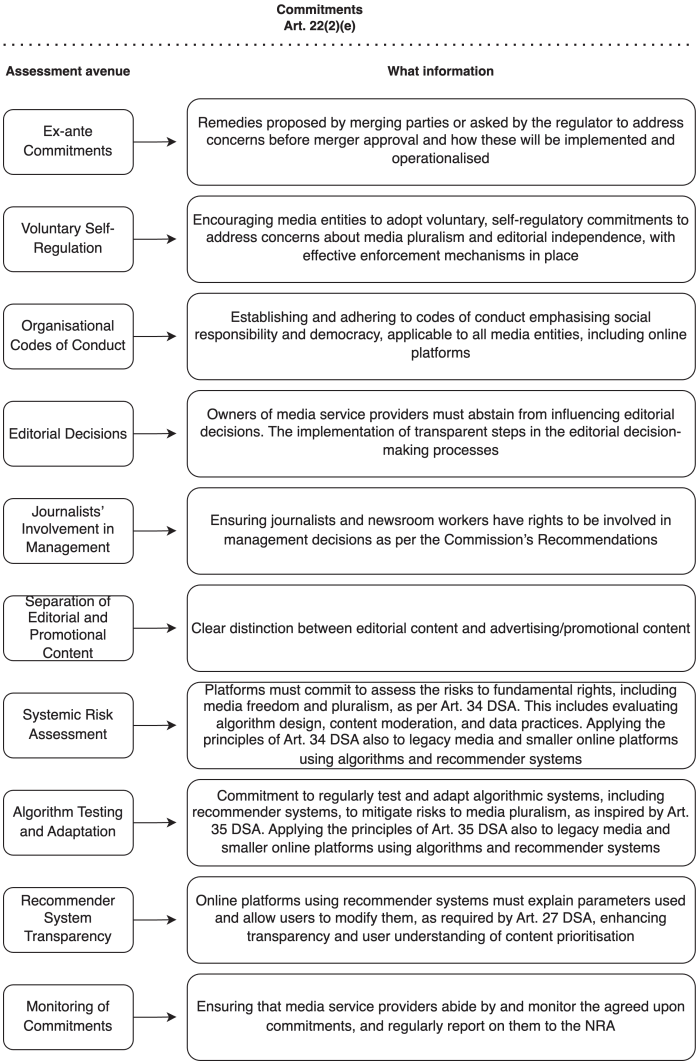

Figure 5. Overview of some of the commitments that could be proposed "where applicable". Source: Authors

5. Conclusion

Art. 1 of the EMFA claims that its main purpose is the proper functioning of the internal market for media services. However, the reality is that the EMFA is the EU's regulatory response to the threats surrounding media freedom and pluralism. Moreover, the Commission needed to use Art. 114 of the TFEU and its internal market argument as a legal basis for its regulatory intervention, thus making these tortured arguments about regulating pluralism for economic reasons. Not only does the EMFA lay down the first-ever EU-harmonised rules on media pluralism and independence, transparency of media ownership, allocation of state advertising to media service providers, and protection of journalistic sources and journalists' rights, but it does so in the form of a directly applicable Regulation. Considering the general and vague elements proposed for consideration by Art. 22(2) lit. (a) to (e), this chapter has explained how these elements of the media pluralism test (under Art. 22) may appear. This has been achieved by building on the MPM's market plurality indicators and the Recommendation accompanying the EMFA.

The EMFA explicitly stresses the essential role played by the NRAs in upholding media pluralism objectives and editorial independence safeguards by providing them with an active participatory role in the assessment of national media mergers; considering the non-binding opinion of the NRAs, the actual impact of the pluralism tests on the final media merger decisions remains to be seen. Effective oversight requires high levels of trust and transparency, and robust monitoring and intervention powers for NRAs. Thus, to exercise their role, NRAs' independence becomes even more paramount. For NRAs to conduct thorough pluralism tests, access to accurate and up-to-date data is crucial. However, NRAs face significant challenges in monitoring (especially online) media pluralism due to legal, technical, and sometimes practical obstacles.[43] These challenges can be mitigated through open communication and trust between NRAs and the merging parties. NRAs can directly ask the media service providers participating in a merger for the required information and track the companies'

43 These include obstacles related to the country-of-origin principle (see Art. 3 Directive 2000/31/EC, shortly the "e-Commerce Directive"), the high cost of qualitative data analysis, and the frequent absence of necessary data. The lack of such data is due to fluctuating audience numbers, a lack of harmonised measurement metrics, unreported data, and data often being held by large private entities.

structural changes through the continuous maintenance of dedicated public repositories.

Although Art. 22 represents a step in the right direction, the light regulatory approach falls short in several areas. Although it aims to harmonise the pluralism test, the elements stipulated in the legislation are left unclear, leaving room for interpretation, which, in turn, could result in a non-unified approach of Member States. The reference to accounting for the online environment remains undefined in the EMFA, leaving NRAs with considerable uncertainties. To add to these, considering current legislation and case law, the possibility to treat VSPs and VLOPs as media service providers can strike one as wishful thinking – at least for now. As per the Recommendations, it seems that, generally speaking, the EMFA is largely reliant on voluntary measures. This reliance, coupled with media service providers' willingness to self-regulate, poses significant challenges. Continuous ex-post monitoring to ensure compliance is resource-intensive, underscoring the necessity for automatic self-reporting mechanisms. Finally, the EMFA fails to address the matter of exposure diversity – a critical aspect of media pluralism also highlighted by the Council of Europe (2018), since merely having diverse media service providers does not guarantee their content reaching, and being consumed by, the audience.

The introduction of a common framework for the media pluralism tests and the involvement of NRAs in media concentration assessments is a positive development, acknowledging the importance of a diverse and independent media for democracy. The willingness to cooperate, voluntary measures, organisational codes of conduct, and a social responsibility to democracy should be at the forefront of all media entities, including online platforms. While the EMFA's measures are less bold than anticipated, they advance the much-needed ownership transparency measures, address the allocation of state advertising, and introduce an additional scrutiny layer to media mergers based on non-economic considerations. In so doing, unwanted practices could be deterred and the accountability of media service providers increased.

References

Afilipoaie, A., Donders, K. and Ballon, P. (2022) 'The European Commission's approach to mergers involving software-based platforms: towards a better understanding of platform power', *Telecommunications Policy*, 46(5) [Online]. Available at: https://doi.org/10.1016/j.telpol.2021.102288.

Afilipoaie, A. and Ranaivoson, H. (2022) 'Assessing media mergers and acquisitions: the power pyramids of regulatory cooperation', *Journal of Digital Media & Policy*, 15(1), pp.7-26.

Afilipoaie, A. and Ranaivoson, H. (2023) 'EU and the complex, nation-dependent web of media ownership regulation in Europe: the role of media ownership rules in limiting market concentration' in Ranaivoson, H., Broughton Micova, S. and Raats, T. (eds.) *European audiovisual policy in transition*. London: Routledge, pp.113–134.

Barnett, S. (2010a) 'Media ownership policy in a recession: redefining the public interest', *Interactions: Studies in Communication & Culture*, 1(2), pp. 217–232.

Barnett, S. (2010b) *What's wrong with media monopolies? A lesson from history and a new approach to media ownership policy*. London School of Economics [Online]. Available at: https://www.lse.ac.uk/media-and-communications/assets/documents/research/working-paper-series/EWP18.pdf (Accessed: 5 February 2023).

Barwise, P. and Watkins, L. (2018) 'The evolution of digital dominance: how and why we got to GAFA' in Moore, M. and Tambini, D. (eds) *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. Oxford: Oxford University Press, pp. 33–54. Available at: https://global.oup.com/academic/product/digital-dominance-9780190845124?cc=be&lang=en&# (Accessed: 5 October 2022).

Beckett, C. (2019) *New powers, new responsibilities. A global survey of journalism and artificial intelligence*. London School of Economics [Online]. Available at: https://blogs.lse.ac.uk/polis/2019/11/18/new-powers-new-responsibilities/ (Accessed: 19 September 2022).

Brogi, E. (2020) 'The Media Pluralism Monitor: conceptualizing media pluralism for the online environment', *Profesional de la Información*, 29(5), pp. 1–7.

Brogi, E., Carlini, R., Nenadić, I., Parcu, P. L. and de Azevedo Cunha, M. V. (2021) 'EU and media policy: conceptualising media pluralism in the era of online platforms. The experience of the Media Pluralism Monitor' in Parcu, P.L. and Brogi, E. (eds.) *Research handbook on EU media law and policy*. Cheltenham: Edward Elgar Publishing, pp. 16–31.

Brogi, E., & Sjøvaag, H. (2023). *Good practices for sustainable news media financing*. Council of Europe [Online]. Available at: https://rm.coe.int/msi-res-2022-08-good-practices-for-sustainable-media-financing-for-sub/1680adf466 (Accessed: 27 September 2024).

Buts, C. and Jegers, M. (2012) 'The effect of "state aid" on market shares: an empirical investigation in an EU Member State', *Journal of Industry, Competition and Trade*, 13(1), pp. 89–100.

Cabrera Blázquez, F.J. (2022) *The proposal for a European Media Freedom Act*. Council of Europe [Online]. Available at: https://rm.coe.int/note-emfa/1680a9af14 (Accessed: 27 September 2024).

'Charter of Fundamental Rights of the European Union' (2016) *Official Journal of the European Union* C202, 7 June, pp. 389-405 [Online]. Available at: http://data.europa.eu/eli/treaty/char_2016/oj (Accessed: 26 January 2025).

Commission of the European Communities (1992) *Pluralism and media concentration in the internal market*. Publications Office of the European Union [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/be71ea95-61ab-44d3-9b14-2d7cb82d8d81/language-en (Accessed: 27 September 2024).

'Commission Recommendation (EU) 2022/1634 of 16 September 2022 on internal safeguards for editorial independence and ownership transparency in the media sector' (2022) *Official Journal of the European Union* L245, 22 September, pp. 56-65. Available at: http://data.europa.eu/eli/reco/2022/1634/oj (Accessed: 27 September 2024).

'Council Directive 89/552/EEC of 3 October 1989 on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the pursuit of television broadcasting activities' (1989) *Official Journal of the European Union* L298, 17 October, pp. 23-30 [Online]. Available at: http://data.europa.eu/eli/dir/1989/552/oj (Accessed: 26 January 2025).

Council of Europe (2018) *Recommendation CM/Rec(2018)11 of the Committee of Ministers to Member States on media pluralism and transparency of media ownership*. Council of Europe [Online]. Available at: https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680790e13%22],%22sort%22:[%22CoEValidationDate%20Descending%22]} (Accessed: 27 September 2024).

'Council Regulation (EC) No 139/2004 of 20 January 2004 on the control of concentrations between undertakings (the EC Merger Regulation)' (2004) *Official Journal of the European Union* L24, 29 January, pp.1-22. Available at: http://data.europa.eu/eli/reg/2004/139/oj (Accessed: 26 January 2025).

'Directive (EU) 2018/1808 of the European Parliament and of the Council of 14 November 2018 amending Directive 2010/13/EU on the coordination of certain provisions laid down by law, regulation or administrative action in Member States concerning the provision of audiovisual media services (Audiovisual Media Services Directive) in view of changing market realities' (2018) *Official Journal of the European Union* L303, 28 November, pp. 69-92. Available at: http://data.europa.eu/eli/dir/2018/1808/oj (Accessed: 26 January 2025)..

Directorate-General for Justice and Consumers (2020) *2020 Rule of law report – communication and country chapters*. European Commission [Online]. Available at: https://commission.europa.eu/publications/2020-rule-law-report-communication-and-country-chapters_en (Accessed: 27 September 2024).

Dodds, T., de Vreese, C., Helberger, N., Resendez, V. and Seipp, T. (2023) 'Popularity-driven metrics: audience analytics and shifting opinion power to digital platforms', *Journalism Studies*, 24(3), pp. 403–421.

Dragomir, M. (2019) *Media capture in Europe*. Media Development Investment Fund [Online]. Available at: https://www.mdif.org/wp-content/uploads/2019/07/MDIF-Report-Media-Capture-in-Europe.pdf (Accessed: 12 August 2022).

Van Drunen, M. (2021) 'Editorial independence in an automated media system', *Internet Policy Review*, 10(3) [Online]. Available at: https://doi.org/10.14763/2021.3.1569 (Accessed: 26 January 2025).

Enli, G., Raats, T., Syvertsen, T. and Donders, K. (2019) 'Media policy for private media in the age of digital platforms', *European Journal of Communication*, 34(4), pp. 395–409.

European Commission (2021) *European Media Freedom Act: commission starts consultations with call for evidence, PRESS RELEASE*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/news/european-media-freedom-act-commission-starts-consultations-call-evidence (Accessed: 27 September 2024).

European Commission (2022b) *Explanatory memorandum of the European Media Freedom Act*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52022PC0457 (Accessed: 27 September 2024).

European Commission et al (2022a) *Study on media plurality and diversity online: final report*. Publications Office of the European Union [Online]. Available at: https://data.europa.eu/doi/10.2759/529019 (Accessed: 9 December 2022).

European Commission et al (2023) *Study on the impact of recent developments in digital advertising on privacy, publishers and advertisers*. Publications Office of the European Union [Online]. Available at: https://data.europa.eu/doi/10.2759/294673 (Accessed: 26 January 2025).

European Commission (2023). *The European media industry outlook*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/european-media-industry-outlook (Accessed: 27 September 2024).

European Commission (2024) *Supervision of the designated very large online platforms and search engines under DSA*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/list-designated-vlops-and-vloses (Accessed: 23 September 2024).

European Commission (no date) *Monitoring media pluralism in the digital era*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/monitoring-media-pluralism (Accessed: 27 September 2024).

European University Institute (2022) *The Media Pluralism Monitor informs the EU Commission's Rule of Law Report*. Centre for Media Pluralism and Media Freedom [Online]. Available at: https://cmpf.eui.eu/rule-of-law-report-eu-commission-mpm2022/ (Accessed: 27 September 2024).

European University Institute (2024) *MPM 2024 Questionnaire*. Centre for Media Pluralism and Media Freedom [Online]. Available at: https://cmpf.eui.eu/wp-content/uploads/2024/07/Questionnaire_MPM2024.pdf?sequence=1&isAllowed=y (Accessed: 27 September 2024).

Evens, T. and Donders, K. (2018) *Platform power and policy in transforming television markets*. Cham: Springer International Publishing.

Fanta, A. and Dachwitz, I. (2020) *Google, the media patron. How the digital giant ensnares journalism*. Otto Brenner Foundation [Online]. Available at: https://www.otto-brenner-stiftung.de/fileadmin/user_data/stiftung/02_Wissenschaftsportal/03_Publikationen/AH103_Google_EN.pdf (Accessed: 27 September 2024).

Fathaigh, R.Ó. (2020) *First annual report on the Rule of Law in the EU, including media pluralism and freedom*, *IRIS legal observations of the European Audiovisual Observatory*. IRIS Merlin [Online]. Available at: https://merlin.obs.coe.int/article/9010 (Accessed: 27 September 2024).

'Frank Peterson v. Google LLC and Others and Elsevier Inc. v. Cyando AG' (2021) Joined Cases C-682/18 and C-683/18. *EUR-Lex* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0682 (Accessed: 27 September 2024).

Griera, M. (2024) *EU Commission's rule of law reporting lacks transparency, auditors say*. Euractiv [Online]. Available at: https://www.euractiv.com/section/politics/news/eu-commissions-rule-of-law-reporting-lacks-transparency-auditors-say/ (Accessed: 27 September 2024).

Haraszti, M. (2011) *Media pluralism and human rights*. Council of Europe [Online]. Available at: https://rm.coe.int/16806da515 (Accessed: 24 September 2024).

Harcourt, A. and Picard, R.G. (2009) Policy, economic, and business challenges of media ownership regulation', *Journal of Media Business Studies*, 6(3), pp. 1–17.

Helberger, N. (2018) Challenging diversity: social media platforms and a new conception of media diversity' in Moore, M. and Tambini, D. (eds) *Digital dominance: the power of Google, Amazon, Facebook, and Apple*. Oxford: Oxford University Press, pp. 162–186.

Helberger, N. (2020) 'The political power of platforms: how current attempts to regulate misinformation amplify opinion power', *Digital Journalism*, 8(6), pp. 842–854.

Helberger, N., Karppinen, K. and D'Acunto, L. (2018) 'Exposure diversity as a design principle for recommender systems', *Information, Communication & Society*, 21(2), pp. 191–207

Hendrickx, J. and Ranaivoson, H. (2019) 'Why and how higher media concentration equals lower news diversity – the Mediahuis case', *Journalism* 22(11) [Online]. Available at: https://doi.org/10.1177/1464884919894138 (Accessed: 26 January 2025).

Karppinen, K. (2013) *Rethinking media pluralism*. New York: Fordham University Press.

Kim, M., Stice, D., Stice, H. and White, R. M.(2021) 'Stop the presses! Or wait, we might need them: firm responses to local newspaper closures and layoffs', *Journal of Corporate Finance*, 69 [Online]. Available at: https://doi.org/10.1016/j.jcorpfin.2021.102035.

Kristensen, L.M. (2023) 'Audience metrics: operationalizing news value for the digital newsroom', *Journalism Practice*, 17(5), pp. 991–1008. Available at: https://doi.org/10.1080/17512786.2021.1954058 (Accessed: 26 January 2025).

Laidlaw, E.B. (2010) 'A framework for identifying Internet information gatekeepers', *International Review of Law, Computers & Technology*, 24(3), pp. 263–276 [Online]. Available at: https://doi.org/10.1080/13600869.2010.522334 (Accessed: 26 January 2025).

Mancini, J. (2018) *Considering non-price effects in merger control – background note by the Secretariat*. OECD [Online]. Available at: www.oecd.org/daf/competition/non-price-effects-of-mergers.htm (Accessed: 7 October 2021).

Mansell, R. (2015) 'Platforms of power', *Intermedia*, 43(1), pp. 20–24 [Online]. Available at: http://eprints.lse.ac.uk/61318/ (Accessed: 5 October 2022).

Moore, M. (2016) *Tech giants and civic power*. CMCP, Policy Institute, King's College London [Online]. Available at: https://doi.org/10.18742/PUB01-027 (Accessed: 26 January 2025).

Muñoz Larroa, A. (2019) 'Industrial organization of online video on demand platforms in North America: between diversity and concentration', *The Political Economy of Communication*, 7(2), pp. 79–104 [Online]. Available at: https://www.polecom.org/index.php/polecom/article/viewFile/113/336 (Accessed: 7 February 2023).

Napoli, P.M. (1997) 'Rethinking program diversity assessment: an audience-centered approach', *Journal of Media Economics*, 10(4), pp. 59–74.

Napoli, P.M. and Caplan, R. (2017) 'Why media companies insist they're not media companies, why they're wrong, and why it matters', *First Monday*, 22(5) [Online]. Available at: https://doi.org/10.5210/FM.V22I5.7051 (Accessed: 26 January 2025).

Obar, J.A. and Oeldorf-Hirsch, A. (2020) 'The biggest lie on the internet: ignoring the privacy policies and terms of service policies of social networking services', *Information, Communication & Society*, 23(1), pp. 128–147.

Peruško, Z. (2010) 'The link that matters: media concentration and diversity of content' in Klimkiewicz, B. (ed.) *Media freedom and pluralism: media policy challenges in the enlarged Europe*. Budapest: Central European University Press, pp. 261–273 [Online]. Available at: https://books.openedition.org/ceup/2184?lang=en (Accessed: 7 October 2021).

Peterson, E. and Dunaway, J. (2023) 'The new news barons: investment ownership reduces newspaper reporting capacity', *Annals of the American Academy of Political and Social Science*, 707(1), pp. 74–89.

Picard, R.G. and Pickard, V. (2017) *Essential principles for contemporary media and communications policymaking*. Reuters Institute for the Study of Journalism [Online]. Available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/research/files/Essential%2520Principles%2520for%2520Contemporary%2520Media%2520and%2520Communications%2520Policymaking.pdf (Accessed: 20 March 2019).

Picard, R.G., and Zotto, C.D. (2015) 'The dimension of ownership and control of media' in Valcke, P. Sükösd, M. and Picard, R.G. (eds) *Media pluralism and diversity*. Palgrave Macmillan UK, pp. 54–66.

Posetti, J. (2018) *Time to step away from the 'bright, shiny things'? Towards a sustainable model of journalism innovation in an era of perpetual change*. Reuters Institute for the Study of Journalism [Online]. Available at: https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2018-11/Posetti_Towards_a_Sustainable_model_of_Journalism_FINAL.pdf (Accessed: 25 September 2024).

Ranaivoson, H. (2019) 'Online platforms and cultural diversity in the audiovisual sectors. A combined look at concentration and algorithms' in Albornoz, L. and García Leiva, M.T. (eds) *Audio-visual industries and diversity*. Liège: Routledge, pp. 100–118.

Ranaivoson, H. and Rozgonyi, K. (2023) 'The Audiovisual Media Services Directive and the effectiveness of media transparency requirements' in Ranaivoson, H., Broughton Micova, S. and Raats, T. (eds) *European audiovisual policy in transition*. Oxford: Routledge, pp. 135–153.

Reda, F. and Selinger, J. (2021) 'YouTube/Cyando – an important ruling for platform liability – Part 1', *Kluwer Copyright Blog* [Online]. Available at: https://copyrightblog.kluweriplaw.com/2021/07/01/youtube-cyando-an-important-ruling-for-platform-liability-part-1/ (Accessed: 25 September 2024).

'Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act) (Text with EEA relevance)' (2022) *Official Journal of the European Union* L277, 27 October, pp.1-102 [Online]. Available at: http://data.europa.eu/eli/reg/2022/2065/oj (Accessed: 26 January 2025).

'Regulation (EU) 2024/1083 of the European Parliament and of the Council of 11 April 2024 establishing a common framework for media services in the internal market and amending Directive 2010/13/EU (European Media Freedom Act) (Text with EEA relevance)' (2024) *Official Journal of the European Union* L series, 17 April, pp. 1-37 [Online]. Available at: http://data.europa.eu/eli/reg/2024/1083/oj (Accessed: 26 January 2025).

Reporters Sans Frontiers (2016) *Contribution to the EU public consultation on media pluralism and democracy*. European Commission [Online]. Available at: https://ec.europa.eu/information_society/newsroom/image/document/2016-44/reporterssansfrontiers_18792.pdf (Accessed: 27 September 2024).

Schiffrin, A. (ed.) (2021). *Media capture*. New York; Chichester: Columbia University Press.

Seipp, T.J., Helberger, N., de Vreese, C. and Ausloos, J. (2023) 'Dealing with opinion power in the platform world: why we really have to rethink media concentration law', *Digital Journalism*, 11(8), pp. 1542–1567.

Simon, F.M. (2022) 'Uneasy bedfellows: AI in the news, platform companies and the issue of journalistic autonomy', *Digital Journalism*, 10(10), pp. 1832–1854.

Trappel, J. and Meier, W.A. (2022) 'Soaring media ownership concentration: comparing the effects of digitalisation on media pluralism and diversity' in Trappel, J. and Tomaz, T. (eds.) *Success and failure in news media performance: comparative analysis in the Media for Democracy Monitor 2021*. Gothenburg: Nordicom, University of Gothenburg, pp. 147–164 [Online]. Available at: https://doi.org/10.48335/9789188855589-7 (Accessed: 26 January 2025).

'Treaty on the Functioning of the European Union' (2012) *Official Journal of the European Union* C326, pp. 47-390 [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2012/oj (Accessed: 26 January 2025).

Valcke, P. (2011) 'Looking for the user in media pluralism regulation: unraveling the traditional diversity chain and recent trends of user empowerment in European media regulation', *Journal of Information Policy*, 1, pp. 287–320.

Van Dijck, J., Poell, T. and de Waal, M. (2018) *The Platform Society*. New York: Oxford University Press.

Venit, J.S. (2013) 'The scope of EU judicial review of commission merger decisions' in Lowe, P. and Marquis, M. (eds.) *European competition law annual 2010: merger control in European and global perspective*. Oxford: Hart Publishing, pp. 113–131 [Online]. Available at: https://cadmus.eui.eu/handle/1814/25916 (Accessed: 30 January 2023).

The Data Governance Act – Is "Trust" the Key for Incentivising Data Sharing?

Lucie Antoine

Abstract

In order to contribute to the overall objective of fostering data sharing in the EU, the Data Governance Act introduces two sets of provisions: first, it provides a standardised procedural mechanism for facilitating the re-use of certain data categories held by public sector bodies; second, it establishes a legal framework for the provision of data intermediation services in general and data altruism organisations in particular. Thereby, the Data Governance Act heavily builds upon the idea of increasing trust. During the last years, the principle of trust has already become a central regulatory objective in EU legislation, in particular as regards the online and platform environment. However, which role can trust play in the data economy for incentivising data sharing? And can the Data Governance Act, following this rationale, fulfil its objectives from both a theoretical and practical perspective?

1. The role of trust for data sharing

Does trust play an essential role in incentivising data sharing? Is increasing trust in data intermediaries the key for fostering the development of respective actors in the European market? And can the establishment of trustworthy data intermediaries contribute significantly to the overall objective of creating a European single market for data by enhancing the availability and reusability of data?

Following the underlying rationale of the Data Governance Act (DGA) (Regulation (EU) 2022/868), these three questions would have to be answered in the affirmative. Trust is the general principle shaping the DGA. Indeed, it seems clear that this holds true for the DGA's provisions defining a mandatory legal framework for *data intermediation services* in general and *data altruism organisations* in particular (see Section 3.0.). Data intermediation services, such as platforms allowing businesses to exchange data,

and data altruism organisations, including initiatives pooling health data in order to make it available for scientific research, should provide their services in a manner that users or data *donors* can be sure that *their* data is only used for the intended purposes, and not, for instance, for the business interests of the provider. Introducing legally binding conditions for offering data intermediation or altruism services thus aims – in a first step – to foster the development of reliable, neutral, and therefore trustworthy data intermediaries in line with *European values*. High hopes have been expressed that – in a second step – data intermediaries can then increase trust in data sharing as such, making data flow more easily in practice.

Moreover, the DGA's second important set of provisions on facilitating the re-use of data held by public sector bodies builds upon the principle of trust equally (see Section 3.0). These provisions address constellations in which public sector bodies (e.g., statistical offices) possess data (e.g., statistical data) intended to be re-used by third parties (e.g., for scientific research). By defining standardised and transparent conditions for requesting access and re-use of data held by the public sector, trust in both the re-use mechanism and the acting institution should be strengthened. This is particularly important as the DGA addresses the re-use of data protected on grounds of commercial or statistic confidentiality, by intellectual property (IP) rights of third parties or as personal data. As such, the DGA introduces instruments that account for the data's sensitivity, e.g., by restricting the transfer of certain data to third countries outside the EU.

Even though, on principle, it is convincing that trust has been identified as a pivotal prerequisite for data sharing (European Commission, 2018, p. 1; Richter and Slowinski, 2019, p. 14), the DGA and its underlying rationale raise manifold questions on the general concept of trust (from a sociological and a legal perspective) and its relation to data sharing requiring more nuanced inquiries, particularly from an interdisciplinary perspective. This ranges from highly fundamental aspects on law and trust over the role of trust as a guiding principle for the European platform economy (see Section2) to the specific question of whether the DGA's provisions, which rely heavily on the principle of trust (see Section 3.), can fulfil their objective from both a theoretical and practical perspective (see Sections 3 and 4.).

2. Law and trust

Trust can be defined as the "firm belief in the reliability, truth, or ability of someone or something" (Oxford English Dictionary, 2024). From a sociological perspective, Luhmann (2014, pp. 27, 39) influentially considered trust as the pre-requisite for reducing (social) complexity. This concerns in particular the complexity arising from the *freedom* of others to behave in a way that might run counter to the trusting party's expectations (Luhmann, 2014, p. 38). Trust goes beyond *information* as it is not possible to predict a counterpart's behaviour with sufficient certainty (Luhmann, 2014, p. 38). However, social – and legal – norms can provide objective reference points for anchoring trust (e.g., through sanctions). Such frameworks have the result that certain (on principle, possible) actions are deemed less probable, which can impact decision making (Luhmann, 2014, pp. 29, 40). Accordingly, trust and law are strongly interconnected (Peukert, 2022, p. 231). Put simply, the law (i.e., legal norms) can contribute to minimising *risk* by reducing uncertainty, and is therefore a factor that can increase *trust*. Legally speaking, trust consequently plays an important role as a theoretical justification for normative intervention in form of laws (cf. Peukert, 2022, p. 232). Trust shall be created *through* the law – however, at the same time, this depends on trust *in* the law (Peukert, 2022, p. 231) and its institutions.

As Luhmann (2014, p. 24) already posited, the more complex systems become, the more trust is required. Along these lines, trust has, in recent years, become a central regulatory objective in EU legislation, particularly in terms of the (highly complex) online and platform environment (Peukert, 2022, p. 237; Cole, 2022). The online environment does not only consist of a multitude of actors that, in part, have assumed genuinely *new* roles in society (most importantly, platforms and intermediaries), it also offers a plethora of possible ways for behaving. This increases complexity and, thus, risk, which could lead to low levels of trust. In particular, the Digital Services Act (DSA), introduced as Europe's "basic law for the platform economy", strongly refers to the principle of trust (see, e.g., Cole, 2022, p. 308; Kaesling, 2022). In order to create a "trusted online environment", inter alia hate speech (Liesching, 2022) and disinformation (Peukert, 2023) have been regulated. *Trusted flaggers* should contribute to identifying *illegal content*, both under the DSA (Kaesling, 2022) and, for copyright infringing content, under the Digital Single Markets Directive (DSM Directive; see Lauber-Rönsberg, 2022). Furthermore, comparably early instruments,

such as the E-Commerce Directive (2000/31/EC) or the Platform to Business Regulation (2019/ 1150), already contain strong references to "trust" and "trustworthiness" (for further examples, see Cole, 2022, p. 320). The European regulation of AI is characterised by a comparable approach aimed at creating and promoting "trustworthy AI" (see AI Act[1], Regulation 2024/1689). However, also on a global level, the vision of a "trusted" digital future (OECD, 2022b) and "fostering data flows with trust" (OECD, 2022a) is shared.

3. Trust in the DGA

3.1 The DGA: background, legal nature, and overview

As a legal instrument, the DGA is tailored to increase trust in actors that have been identified as relevant for allowing data to flow in Europe, thus contributing to the overarching objective to establish a European data economy. In order to unleash the full potential of data-driven innovation in the EU, the European Data Strategy (European Commission, 2020a) follows an approach of openness and access to data. The overall aim is to facilitate data sharing between different actors, and thus establish a European single market for data. The majority of legal instruments implemented in recent years have primarily pursued the objective that data can be accessed, ported, and re-used: the Open Data Directive (ODD), regarding the re-use of certain data held by the public sector (G2B); the Data Act (DA), addressing data access in particular in B2B and B2C relations, as well as access to privately held data by the public sector (B2G); the Digital Markets Act (DMA), providing – inter alia – access and portability rights vis-à-vis gatekeepers; the General Data Protection Regulation (GDPR), covering access to and portability of personal data; and the Digital Content Directive (DCD), enabling consumers to port certain non-personal data (as part of further contractual rights and obligations in relation to digital content).

However, both these mandatory instruments and voluntary data sharing (mostly based on contracts) face a common challenge: *how* can the envisaged data flows be made to effectively work in practice? Not only legal uncertainty – particularly regarding personal data – but also organisational

1 For more information on trustworthy AI in the AI Act, see Chapter 3 'Accountable AI: It Takes Two to Tango' by Jorge Constantino.

(infrastructure) and technical (e.g., standardisation, interoperability) barriers constitute relevant practical obstacles for data sharing (see Leistner and Antoine, 2022, p. 34). To this list, the DGA adds the lack of trust – in processes, in actors, in the ability to maintain control over data, and in data sharing in general.

The DGA therefore repeatedly refers to the principle of trust (Kerber, 2021, p. 2).[2] Strengthening trust in the data economy and in the concept of data sharing as an important means for fostering the data economy requires trust in the involved actors, whether the public sector, businesses, or individuals. The DGA identifies transparency and "trustworthy" data governance structures as the main factors by which to increase trust in the relevant players, accompanied by guaranteeing control over data by the individual data subject or data holder.

However, the DGA does not lay down a general horizontal framework for data governance in the strict sense. Rather, it focuses on more specific areas: *first,* the DGA implements a standardised mechanism for facilitating the re-use of data held by public sector bodies that cannot be made available as open data due to its sensitive character (see Section 3.0); *second*, the DGA provides a legal framework for data intermediation services in general and for data altruism organisations in particular, which have been identified as important enablers for facilitating data sharing in practice (see Section 03.3). These provisions exemplify the DGA's underlying rationale that increasing trust is deemed key for fostering data sharing.

The DGA also contains further provisions on the competent national authorities, the international transfer of non-personal data, and the establishment of a European Data Innovation Board (EDIB); however, this chapter will not address these provisions in detail.

The DGA entered into force on 23 June 2022 and has been applicable since 24 September 2023. As the DGA is a Regulation, its provisions are directly applicable in the Member States without having to be transposed into national law.

2 See Recitals 3, 5, 23, 24, 32, 33, 38, 43, 46, 47, and 52 DGA.

3.2 Re-use of public sector information (Chapter II): trust in the process and in the institutions

With the provisions contained in Arts. 3–9, the DGA introduces a standardised procedural mechanism for facilitating the re-use of certain data categories held by public sector bodies. The term *re-use* is broadly understood as referring to use by natural or legal persons for non-commercial and commercial purposes (Art. 2(2) DGA). In a nutshell, the DGA's provisions in Chapter II aim at making data (subject to the rights of third parties) held by the public sector available for re-use while respecting their sensitive nature at the same time (Kerber, 2021, p.1). The principle that data which has been collected by public sector bodies at the expense of public budgets should benefit society has been part of EU policy for a long time (Recital 6 DGA) and is manifested in, for example, the legal instruments on open data. However, where data of a more sensitive nature is at stake, public sector bodies must also respect that particular character as part of their public task.

The DGA does not address the question as to *whether* data held by the public sector body should be made available for re-use, but rather *how* making data available for re-use should work (Lauber-Rönsberg and Becker, 2023, p. 32). Establishing a basic procedural framework for data re-use requests and laying down conditions for re-use intended to protect the data's sensitive character has the objective to increase transparency. Consequently, citizens can trust public sector bodies that they, on the one hand, do not *retain* data that are valuable for research or innovation purposes, while they, on the other hand, comply with their public task by preserving the data's sensitive nature, even when making them available for re-use.

The DGA has been inspired by the re-use mechanisms that certain Member States already have in place (Richter, 2022, p. 4). The European Commission's (EC) Impact Assessment Report (European Commission, 2020b, p. 13), for instance, refers to the French "Centre d'accès sécurisé aux données" (Centre for secure access to data) established inter alia by the French government and the National School for Statistics, allowing the secure processing of statistical micro-data. It also refers to the establishment of the data permit authority "Findata" in Finland, which provides a one-stop shop solution for data re-use requests as well as to research centres established in Germany for facilitating access to medical reimbursement data for researchers by providing a "secure data research infrastructure".

Bearing these envisaged mechanisms in mind can certainly help to better understand the DGA's provisions in detail.

3.2.1 Scope and covered data categories

According to Art. 3(1), the DGA applies to data held by public sector bodies that are protected on grounds of commercial or statistic confidentiality, by IP rights of third parties or as personal data ("protected data", see European Commission, 2024a, p. 2). Thus, the DGA addresses data that does not fall within the scope of the ODD precisely because of its *sensitivity* (cf. Art. 3(1), Recital 10 DGA; Baloup et al, 2021, p. 17; Richter, 2022, pp. 4, 7). For instance, data that has to be made available to a public sector body based on a legal obligation to disclose certain information may also qualify as trade secrets.

Addressees of the provisions are public sector bodies, i.e., a state, regional or local authorities, or other bodies governed by public law (see definitions in Art. 2(17) and Art. 2(18) DGA).[3] The DGA points at data the public sector body supplies as part of its public task (Recital 12, cf. Art. 3(2) (e) DGA). This means that a public sector body is – from a technical and factual perspective – competent for granting access to data for re-use (Specht-Riemenschneider in Specht-Riemenschneider and Hennemann, 2023, Art. 3 para. 62). In fact, it will often primarily depend on whether a public sector body is – in a first step – competent for collecting and storing respective data (Specht-Riemenschneider in Specht-Riemenschneider and Hennemann, 2023, Art. 3 para. 62). Thus, the addressees of the provisions are public sector bodies competent under national law for granting or refusing access requests for re-use (Art. 5(1) DGA). A rather simple example would be a statistical office that makes certain statistical data available for re-use in research or commercial applications.

The DGA itself neither introduces access rights nor obliges Member States to make the data in scope available for re-use (Recital 11 DGA).[4] Rather, it depends on the Member States' national law whether and which publicly held data will be accessible for re-use, under which conditions, and for which purposes.

3 See exception in Art. 3(2) DGA for data held by public undertakings, public service broadcasters, and cultural or educational institutions, such as museums, libraries, or archives.

4 On the contrary, Art. 3(1) ODD states as a general principle that Member States must ensure that documents falling within the Directive's scope "shall be re-usable".

3.2.2 General conditions for re-use

The DGA solely defines certain basic principles (e.g., Art. 4) as a minimum set of conditions for the re-use by third parties which take into account the sensitivity of the data in scope (Art. 5), the possibility to charge fees (Art. 6), as well as certain procedural guideposts for handling requests for re-use (Arts. 8 and 9). Moreover, Member States must designate a competent body (with technical expertise) to assist public sector bodies in handling re-use requests (Art. 7).

First and foremost, the DGA prohibits exclusive arrangements for the re-use of data in order to avoid an exclusionary competitive advantage. An exclusive right to re-use can only be granted under rather strict conditions (necessary for products or services in the general interest that would otherwise not be possible, Art. 4(2)) and for a limited period of time (12 months, Art. 4(4)). In order to guarantee transparency, the decision to grant an exclusive arrangement has to be made available publicly (Art. 4(6)).

Most importantly, Art. 5(2) obliges public sector bodies to allow the re-use of data falling within the scope of the DGA under non-discriminatory, transparent, proportionate, and objectively justified conditions. Consequently, public sector bodies are, for instance, not allowed to impose conditions on data users which make the re-use unduly or even prohibitively difficult. Public sector bodies are allowed to charge a fee for making data available for re-use (Art. 6). In particular, Art. 6(4) allows for a layered scheme, charging less for small and medium-sized enterprises (SMEs) or research institutions. The charged fee must be based on the costs for making the data available (Art. 6(5)).

3.2.3 Additional safeguards

Since the DGA addresses *protected data*, the public sector body has the general obligation to ensure that the protected nature of data to be made available for re-use is preserved (Art. 5(3)).

In terms of personal data, the competent public sector body must therefore anonymise such data before making them available for re-use (Art. 5(3)(a)(i), Recital 15). In this case, the data no longer qualifies as personal data, meaning the GDPR does not apply. As an additional safeguard, Art. 5(5) DGA prohibits re-identifying natural persons and obliges data re-users to implement technical and organisational measures to prevent such re-identi-

fication. In case anonymised data is not suitable for the needs of the re-user, personal data can only be made available for re-use under additional requirements. In that case, all requirements for the lawful processing of personal data according to the GDPR would have to be met. In particular, the DGA itself does not constitute a legal basis for making personal data available for re-use (cf. Art. 5(6)). Moreover, the re-use of personal data should only occur via a "secure processing environment" provided by the public sector body, either remotely or on premise (see Recital 15, cf. Art. 5(3) (b), (c), (4)). Such secure processing environments are already used on a national and European level, such as by statistical offices.[5]

Art. 5 DGA also lays down further conditions for making confidential data (e.g., data protected as trade secret) or data subject to IP rights of third parties available for re-use. In general, data can be confidential for different reasons, stemming either from public[6] or private law. From the perspective of the latter, the protection of data as trade secrets according to the Trade Secrets Directive (2016/943) is the most relevant. Before making confidential data available for re-use, the public sector body should modify the data in a way that prevents the disclosure of confidential information (Art. 5(3) (a) (ii), Recital 15). As an additional preventive measure, the data re-user should be bound by means of a confidentiality agreement in case confidential information is discovered throughout the re-use despite the implemented safeguards (Art. 5(5)). Where a respective modification of the data is not possible or is not suitable for the intended re-use, confidential data can solely be made available when the right holder agrees ((Art. 5(6), (8)) or where such disclosure is lawful by virtue of EU or national law based on other grounds (Recital 18). In this case, the re-use should again occur via a "secure processing" environment, as mentioned above.

Data as such is not protected by IP rights (see Leistner and Antoine, 2022, p. 46). However, data collections can generally qualify as databases and be protected by copyright (Art. 3 et seqq. Database Directive (96/9/EC)) and/or the database sui-generis right (Art. 7 Database Directive). However, as copyright protection requires an original and creative selection or arrangement of the data, copyright protection will apply solely in rather exceptional cases, such as when a database is characterised by a highly unique structure. While in the case of confidential information already disclosing respective data qualifies as a relevant use act from trade secrets

5 See, for example, Eurostat (no date).

6 See, for example, statistic confidentiality according to Art. 338(2) TFEU.

perspective, IP protection comes into play for the question of whether a protected database can be re-used. If a database qualifies for protection, the DGA leaves the right holder's position arising from copyright or the sui-generis right untouched. Thus, it would have to be assessed under the Database Directive as to whether the use of the database by a re-user is lawful (see Art. 5(7) DGA).

On principle, public sector bodies can also qualify as right holders of the database through the sui-generis right. However, public sector bodies cannot invoke sui-generis protection in order to prevent the re-use of the requested data (see Art. 5(7) DGA); rather they should exercise their right only in a way that facilitates re-use (Recital 17 DGA).

3.2.4 Safeguards for the transfer of non-personal data to third countries

As an additional measure, even non-personal data that is confidential or subject to IP rights can solely be transferred to third countries outside the EU when appropriate safeguards are implemented.[7] These provisions are, to a certain extent, inspired by the GDPR's rules on the transfer of personal data to third countries. First of all, the re-user must inform the public sector body when requesting data for re-use about the intended data transmission to a third country, as well as the purposes of the requested re-use (Art. 5(9) DGA). In order to facilitate international data flows, the EC is empowered to adapt "equivalency decisions" – similar to the adequacy decisions of the GDPR – in order to *certify* that a third country meets similar standards for the protection of trade secrets and IP rights (Art. 5(12) DGA).

Where the requested confidential or IP-protected data should be transmitted to a country for which such decision of the EC does not exist, the re-user must contractually agree to use these data solely in accordance with EU law and to accept the jurisdiction of the courts or tribunals of the EU Member States for any dispute relating to the latter (Art. 5(10) DGA). According to Art. 5(13) DGA, future EU legislation can identify certain particularly sensitive categories of non-personal data which cannot be transmitted to third countries at all. The Regulation on the European

7 In the exceptional case that personal data should be made available for re-use, first and foremost, the requirements set forth in Art. 44 et seqq. GDPR for the transfer of personal data to third countries would have to be met.

Health Data Space (EHDS) already contains a respective provision for health data in its Art. 88.[8]

3.2.5 Transparent and effective framework for re-use requests

In order to practically facilitate the re-use of the data categories covered by the DGA, Member States must establish a "single information point" (SIP) (Art. 8). Aiming at providing a one-stop shop for re-use requests, these SIPs should provide an asset list containing an overview of all available data resources accompanied by relevant information describing the available data (Art. 8(2)). Member States are free to empower one competent body as central "intermediary" that directly handles and grants re-use requests (Art. 7(2)).

The competent public sector bodies must make the conditions for re-use and the procedure for requests available via the SIP (Art. 5 (1)). Based on the provided information, interested data users should then be able to send a request for the re-use of data via the SIP, which is then transmitted to the competent public sector body deciding about granting or refusing the request (Art. 8 (2)). On a European level, the EC has already established the European Single Access Point (ESAP) (Art. 8(4) DGA),[9] which merges the information provided by the national SIPs.

According to Art. 9, public sector bodies have to decide to grant or reject a request within a time frame of two months from the date of receiving the re-use request (Art. 9(1)). An extension of 30 days is possible in cases of exceptionally extensive and complex requests. Art. 9(2) grants the requesting person a right to seek redress, meaning that the decision taken by the public sector body can be challenged before the competent national authority or court.

3.2.6 Summary, guiding principles and perspective

Chapter II of the DGA aims at *unlocking* data held by the public sector that cannot be made available as *open data* under the ODD due to their sensi-

8 For more information about the EHDS, see Chapter 15 'The European Health Data Space: The Next Step in Data Regulation' by Lisa Markschies.

9 The ESAP is integrated to the European Data Portal "data.europa.eu" (European Union, no date). However, for the time being, only datasets from the Dutch and Czech National Single Information Points are available (as of 30 June 2024).

tive nature. By establishing a procedural framework for re-use requests and defining conditions for re-use that protect the data's particular character, the DGA aims to increase transparency. For potential re-users, the DGA's provisions clarify how access to respective data can be obtained and under which conditions, as well as which limitations must be respected during re-use (e.g., from a technical perspective). For actors who might have a legal position in the data at stake, the DGA's framework guarantees that these positions (i.e., in terms of the sensitivity of the data) are respected. From a public interest perspective, the standardised procedural mechanism for re-use requests and the transparent and *fair* conditions for re-use do not only facilitate the re-use of data held by the public sector in practice, but also increase trust in public institutions. Public sector bodies obtaining data as part of their public tasks are responsible for protecting respective data even when making them available to third parties for re-use. Moreover, they should, at the same time, contribute to research and innovation in the general interest by allowing re-use. This aspect is, for instance, materialised in the *research-friendly* approach explicitly followed by the DGA (Recitals 15 and 16). Consequently, in terms of scientific research, data should be *as open as possible, as closed as necessary*. However, practically speaking, it is worth bearing in mind that the DGA does not contain any obligation for making data available for re-use. Rather, the Member States have ample discretion in deciding which data categories should be accessible for re-use under national law and under which conditions.

3.3 Data intermediaries: the emerge of neutral and trustworthy players?

The second set of provisions contained in the DGA does not address public institutions, but rather aims to establish reliable and trustworthy data intermediaries in the markets that contribute to facilitating data flows between individuals and businesses, as well as in relation to the public sector. Enhancing data access and fostering data sharing faces a number of legal, organisational, and technical challenges – particularly in terms of making the desired data flows work in practice. Consequently, data intermediaries have been identified as (potential) key enablers for facilitating data access and data sharing (Recital 27). High hopes have been placed on these actors, with a real "data intermediary hype" (Richter, 2023, p. 458) having been observed in recent years.

In order to foster the development of data intermediaries in the European single market, the DGA introduces a mandatory legal framework for providing data intermediation services in general and data altruism organisations in particular. The underlying idea is that implementing a set of rules to which providers of respective services must comply will increase trust in these players. Natural and legal persons should thereby be encouraged to make use of data intermediaries offering a trusted and secure environment for data exchange and sharing (Hennemann and von Ditfurth, 2022, p. 1907). In particular, the European data intermediaries are meant to form a counterpart to the internationally dominating platforms with their immense market and data power (Recital 32 DGA; European Commission, 2020b, p. 16; Richter, 2023, p. 462). By introducing public registers and a *certification* scheme with labels and logos, compliance with DGA-defined rules should be clearly signalled.

3.3.1 Data intermediation services (Chapter III)

Chapter III of the DGA addresses data intermediation services. As an umbrella term, data intermediation service describes a very heterogenous concept. Diverse studies and research papers on a possible categorisation and classification of different data intermediaries have been published in recent years, taking into account various perspectives and disciplines (see Richter and Slowinski, 2019, p. 10; OECD, 2019, p. 36; Wernick, Olk and von Grafenstein, 2020, p. 67; Simon et al., 2020, p. 20; Micheli et al., 2023; Schneider, 2023, 2024).

However, all data intermediaries share two basic features in common: first, their role as neutral, independent third parties; and, second, their function to bring together a person having data and a person interested in this data, as well as to facilitate the respective data flow between these two parties (cf. Recital 27 DGA; Richter and Slowinski, 2019, p. 13; Richter, 2023, p. 459). Notwithstanding, the realisation and organisation of an intermediation service can vary widely (see Recital 27 DGA). As such, the DGA's definition of data intermediation service covers a broad range of services with different purposes and very different forms of organisation.

In line with the overall objective to create neutral and trustworthy data intermediation services, the DGA introduces a notification process and defines specific conditions under which respective services have to be provided.

3.3.2 Definition of data intermediation service

Following these two main characteristics that data intermediaries share, the DGA's definition of "data intermediation service" (Art. 2(11) DGA) adds two additional and, at the same time, limiting features (Richter, 2023, p. 462): first, the purpose of establishing a commercial relationship between data holder and data user; and, second, the open nature of the service ("undetermined number of data holders and users"). Thus, neither services establishing non-commercial relationships between data holders and users (e.g., open access repositories for research data, see Recital 29 DGA), nor closed networks qualify as data intermediation services in the sense of the DGA. Possible examples of data intermediation services are, for instance, data marketplaces or platforms, data pools open to all interested parties, and providers of "data sharing ecosystems", such as the envisaged common European data spaces (Recital 28 DGA). This has particular relevance, as providers of common European data spaces might therefore have to fulfil – in particular circumstances – the obligations outlined in Arts. 11 and 12 of the DGA.

Data intermediation services can cover both personal and non-personal data (European Commission, 2020b, p. 5). Therefore, services particularly tailored to personal data – often called Personal Information Management Systems (PIMS) – that provide, for instance, tools for managing consent to the processing of personal data and for exercising the data subject's right, as foreseen in the GDPR (Recital 30 DGA), also qualify as data intermediation services. However, in terms of processing personal data, the GDPR always fully applies.

The provision of mere technical means for data sharing (e.g., in the form of cloud storage, software tools) does not qualify as a data intermediation service. Moreover, services that aggregate, enrich, or transform data for the purpose of adding substantial value, intermediation services for copyright-protected content (i.e., online content-sharing service pursuant to the DSM Directive), and data sharing services offered by the public sector which are not aimed at establishing commercial relationships[10] do not constitute data intermediation services either (see Art. 2(11) DGA).

10 On principle, public sector bodies can also act as intermediation services (Recital 27 DGA); however, only when aiming at the establishment of commercial relationships do they fall under the definition in Art. 2(11). Public sector bodies making data

3.3.3 Notification process and public register

Before beginning their activities, providers of a data intermediation service have to submit a notification to the national competent authority (Art. 11(1), (4) DGA), designated by Member States (Arts. 13, 14 DGA). According to Art. 10, the notification process is mandatory for (a) providers of platforms or comparable infrastructure services allowing bilateral or multilateral connections and data exchanges between data holders and potential data users (e.g., data sharing platforms or marketplaces where businesses can exchange data); (b) PIMS allowing data subjects to make personal data available and to exercise their rights contained in the GDPR (e.g., PIMS or data wallets, which allow individuals to control their personal data); and (c) data cooperatives,[11] where users are proper members of the structure (such as health data cooperatives, where patients can share their health data for research purposes).

The notification has to contain basic information, such as the name, legal status, form, ownership structure, relevant subsidiaries, number of national registers, address of the main establishment or the legal representative, public website, contact details of a competent contact person, and the description of the offered services (Art. 11(6) DGA). Data intermediation service providers in this sense must comply with the obligations set out in Art. 11 by 24 September 2025 (Art. 37 DGA). After having received the notification, the competent authority issues a declaration, confirming that the data intermediation services provider has submitted a notification containing all relevant information pursuant to Art. 11(6) (Art. 11(8)). In addition, the data intermediation service can request the competent authority to confirm its compliance with all obligations defined in Arts. 11 and 12 (Art. 11(9)). The national competent authorities report any notification to the EU, which, in turn, provides a public register of recognised data intermediaries (Art. 11(10)).[12] Where the competent authority issues a respective confirmation, the data intermediation service is further allowed to use the label "data intermediation services provider recognised in the Union" and the following logo:

available for re-use pursuant to Chapter II do not qualify as intermediation service in this sense (Recital 28).

11 See the definition in Art. 2(15) with Recital 31, and, on data cooperatives, Zingales (2022, p. 8).

12 The register is available at European Commission (2024).

Figure 1: Common logo as adopted through Commission Implementing Regulation (EU) 2023/1622 of 9 August 2023 on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union

3.3.4 Conditions for providing data intermediation services

In order to guarantee the envisaged role of a data intermediation service as a neutral and trustworthy third party, Art. 12 DGA defines mandatory conditions under which data intermediation services have to be provided.

Due to the strict neutrality principle (see also Recital 33; Spindler, 2021, p. 107; Baloup et al, 2021, p. 31), the DGA, first and foremost, mandates that data intermediation services have to be provided as structurally separate from other services, meaning by a separate legal person (Art. 12 (a)). According to Recital 32, "data intermediation services providers should offer a novel, 'European' way of data governance, by providing a separation in the data economy between data provision, intermediation and use". Notwithstanding, such structural separation, i.e., in the form of a separate legal person (Rec. 33), has a far-reaching economic impact that might even disincentivise the development of data intermediation services (see Richter, 2023, p. 465; Hartl and Ludin, 2021, p. 537).

Second, Art. 12 DGA additionally limits the purposes for which intermediation services can use data. Most importantly, providers are obliged to not use data for purposes other than the provision of a data intermediation service (Art. 12 (a)). Moreover, they may not use data stemming from users' activities for other purposes than the development of the intermediation service (Art. 12 (c)), and not change the data format unless this is requested by the user or necessary for enhancing interoperability or mandated by law (Art. 12 (d)). Additional tools and services can only be offered for the specific purpose of facilitating the exchange of data (Art. 12 (e), Recital 32). Indeed, accepting such an offer would require an explicit request or approval of the data subject or data holder. In sum, the purpose limitations seek to prevent conflicts of interest and to *unbundle* services (Richter, 2022, p. 463) in the interest of the user.

Third, Art. 12 further specifies the conditions under which the data intermediation service has to be offered. According to Art. 12 (b), the intermediation service (including the pricing) must not be tied to other services. Furthermore, access to the data intermediation service has to be granted under fair, transparent, and non-discriminatory conditions for both data holders, data subjects, and users. Even in the case of insolvency, data intermediation service providers have to ensure that data holders and users are able to access and retrieve their data (Art. 12 (h)).

Fourth, providers of data intermediation services are obliged to implement technical and organisational measures for preventing fraudulent or abusive practices (Art. 12 (g)), safeguard a reasonable continuity of service in case of insolvency (Art. 12 (h)), and prevent unlawful access to non-personal data (Art. 12 (j)). They have to inform data holders in case of unauthorised data access (Art. 12 (k)), comply with IT-security standards for storage, processing and transmission of data (Art. 12 (l)), and maintain log records of the data intermediation activity (Art. 12 (o)). Moreover, data intermediation services should explicitly contribute to enhancing interoperability, also in terms of other intermediation services (Art. 12 (d), (i)).

As regards personal data, Art. 12 (m) adds an additional layer of responsibility for data intermediation service providers: they must act in data subjects' best interests, inter alia by informing and, where appropriate, advising data subjects in a concise, transparent, intelligible, and easily accessible manner. According to Recital 30, this could include advising data subjects on the possible use of data, conducting due diligence checks on data users before allowing access to personal data, or offering a technical solution for in-situ access to personal data instead of transferring it to third parties. Thus, Art. 12 (m) does not contain a clear-cut set of measures that data intermediation services must implement for this purpose. This leaves providers with a wide discretion on the one hand, but also carries significant legal uncertainty on the other. In particular, the abstract obligation to act in the data subjects' best interest is – pursuant to Recital 33 – understood as an intermediation service's "fiduciary duty" towards the individual. Consequently, Art. 12 (m) imposes a far-reaching responsibility on personal data-related intermediation services far exceeding the strict neutrality principle (less critical e.g., Specht-Riemenschneider in Specht-Riemenschneider & Hennemann, 2023, Art. 12 para. 98 arguing that the structural imbalance of power to the detriment of data subjects justifies such fiduciary duty).

3.3.5 Summary, guiding principles, and perspective

The obligations contained in Chapter III aim to safeguard the strict neutrality of data intermediation services. Most importantly, respective services have to be provided as structurally separate from other services. In addition, providers must not use the data "consigned" to them for their own purposes and additional services can only be offered to the user under certain circumstances. All of these obligations form the prerequisites for distinguishing the *European way* of data intermediation services (Recital 32) from data leeches. The framework outlined for the provision of data intermediation services is thus, on principle, suitable for increasing trust in the respective services as potential users do not have to fear that "their" data is being used for the provider's own interests. As such, the strict conditions under which data intermediation services can be provided could, on principle, incentivise data holders and potential data users to make use of these respective services.

However, it remains to be seen whether there are sufficient incentives for data intermediation services to generate their respective business models. The obligations to which data intermediation services providers must comply under the DGA are quite far-reaching. Offering data intermediation services in accordance with the DGA's framework has a cost side. Even already existing intermediaries are still in their "infancy" (Gellert and Graef, 2021, p. 11), or in a "rather nascent phase" (Richter, 2023, p. 460). In this context, it has also to be kept in mind that no ex-ante examination by the competent authority is conducted on a substantive level. Thus, data intermediation services must assess their compliance on their own account, but at the same time face ex-post supervision by the national competent authority. Although this mechanism has been introduced with the idea to limit both the regulatory burden and the service providers' costs (Gellert and Graef, 2021, p. 9), it may result in a model that tends to be rather unattractive for the relevant players (Hartl and Ludin, 2021, p. 537). On principle, being able to use the label of recognised data intermediation service could set certain incentives for providers as it signals their compliance with the DGA to the market, and thus their nature as a neutral and trustworthy third party. However, this would require that potential users of data intermediation services sufficiently value the trustworthiness of such a service when taking decisions and that increased trust can really incentivise data sharing via respective services (further discussed in Section 4.). Therefore, it remains to be seen whether the framework provided by

the DGA helps data intermediation services scale up, or rather stifles the development of respective business models. However, at least eight data intermediation services from Finland, France, and Hungary are currently registered in the EU (European Commission, 2024b).

3.3.6 Data altruism organisations (Chapter IV)

For the particular category of data altruism organisations – put simply, data intermediaries acting not-for-profit and for the social good – Art. 16 et seqq. DGA provide specific provisions. As mentioned above, the obligations for data intermediation services do not explicitly apply to data altruism organisations (Art. 15).

As can data intermediation services, data altruism organisations can appear in multiple forms. The basic constellation the DGA seems to have in mind are data altruism organisations that, in a first step, pool data for a particular purpose of general interest, and, in a second step, allow access to this data (e.g., for research purposes). An illustrative – and often-quoted – example here is Germany's "Corona Data Donation App" (Corona Datenspende, 2024). During the COVID-19 pandemic, users were able to share such data as resting pulse, daily activity, and sleep duration via a smartphone app. Over half a million people in Germany decided to support the project and donated their data. The data was then used for scientific research on the long-term effects of the COVID-19 virus. However, the DGA also seems to cover constellations in which data altruism organisations primarily provide tools allowing data subjects or data holders to easily give consent (personal data) or permission (non-personal data) to the data processing of third parties (cf. Art. 21(6)). Thus, data wallets or consent management tools can also qualify as data altruism organisations, at least as far as they pursue objectives of general interest or act for the social good.

When organisations conduct data altruism activities, they can apply for registration in the public register what requires to fulfil further pre-requisites when providing their service. This also entails the obligation to introduce tools allowing the donating data subject or data holder to manage consent and permission.

3.3.7 Definition of data altruism

The definition of data altruism contained in Art. 2(16) of the DGA is characterised by three main features: (1) data subjects or data holders deliberately share "their" data with a data altruism organisation by means of giving consent or permission to the use of the respective data; (2) data altruism organisations have to work on a not-for-profit basis and are only allowed to seek compensation for covering the costs incurred from making their data available; and (3) data is made available for the social good, i.e., for objectives of general interest. Regarding objectives of general interest, Recital 35 lists possible examples, such as "healthcare, combating climate change, improving mobility, facilitating the development, production and dissemination of official statistics, improving the provision of public services, or public policy making".

3.3.8 Registration process and public register

Compared to data intermediation services, which are subject to a mandatory *notification* process, data altruism organisations can be *registered* voluntarily with the competent national authority. In this regard, data altruism organisations need to apply for registration (Art. 19(4) DGA) and, as a prerequisite, must meet the requirements set forth in Art. 18. The competent authority only registers a data altruism organisation if it complies with the respective obligations (Art. 19(5)). Thus, the competent authority not only examines the application for registration formally, but also substantively. Moreover, the competent authorities – which the Member States have to designate (Art. 23) – monitor and supervise the compliance of data altruism organisations after registration (Art. 24).

Art. 18 defines the requirements for registration. This provision both specifies the notion of data altruism organisation and adds further criteria to be fulfilled in order to qualify for registration. Comparable to the provisions on data intermediation services in general, these requirements aim at guaranteeing the neutrality of data altruism organisations. However, the criteria set forth for data altruism organisations are even stricter in this regard. This reflects the particular altruistic character of respective organisations, distinguishing them from "normal" data intermediaries. As such, apart from making their data available for objectives of general interest, data altruism organisations must also be structured as an (independent)

legal person. Further, a data altruism organisation does not only have to operate on a not-for-profit basis, but it has to be legally independent from any entity operating on a for-profit basis. Moreover, data altruism activities must be conducted through a structure that is functionally separate from other activities.

In addition, data altruism organisations must comply with the rulebook developed by the EC according to Art. 22 DGA. However, so far, this rulebook does not exist. Once registered, a data altruism organisation is allowed to use the label data altruism organisation recognised in the Union as well as the respective logo:

Figure 2: Common logo as adopted through Commission Implementing Regulation (EU) 2023/1622 of 9 August 2023 on the design of common logos to identify data intermediation services providers and data altruism organisations recognised in the Union

The Member States must establish a national register of recognised data altruism organisations (RDAOs); the latter of which must then be reported to the EC, who will then compile the information in the EU register of RDAOs (Art. 17 DGA; see European Commission, 2024c). Currently, only one data altruism organisation is registered,[13] the "Associació Dades pel Benestar Planetari (DATALOG)" from Spain. DATALOG operates in Barcelona and was developed from a project conducted by the Universitat Pompeu Fabra. DATALOG provides a platform where citizens can upload their invoices for consumption of public services, such as water, gas, and electricity. For the individual user, the platform not only allows a centralised management of respective invoices, but also an analysis of the individual consumption, thereby allowing for its further optimisation in a responsible and sustainable manner. As regards the city of Barcelona, consumption data can be mapped and aggregated on a large scale. Data analysis can then show tendencies, patterns, and correlations regarding

13 As of 2 July 2024.

citizens' consumption, thereby enabling smarter and more sustainable decisions for the city's further development.

3.3.9 Further obligations for recognised data altruism organisations

The DGA does not stop at defining registration requirements, but also outlines certain transparency duties (Art. 20) and conditions under which the RDAOs must conduct their activities (Art. 21).

In order to make the work of data altruism organisations transparent, RDAOs are obliged to keep full and accurate records on which natural or legal persons were given the possibility to process data held by the RDAO, when or for how long such processing took place, what the purpose of processing was, and whether a fee was paid (Art. 20(1)). Furthermore, RDAOs have to submit an annual activity report to the competent authority (Art. 20(2)).

Regarding the data-sharing process, the RDAO must inform the data subject or holder before sharing any data, in a clear and easily comprehensible manner, for which objectives of general interest the RDAO will conduct data processing activities (Art. 21(1) (a)). Where personal data is concerned, the information needs to be more specific, demonstrating a "specified, explicit and legitimate purpose" for which personal data is processed. RDAOs must not use the data provided to them for other purposes than the objectives of general interest (Art. 21(2)). Where data processing activities are conducted in third countries outside the EU or where data might be made available in such countries, the RDAO has to provide further information (Art. 21(1) (b), (6)).

Regarding the data processing activities, the RDAO must ensure an appropriate level of security for data storage and processing (Art. 21(4)) – also with regard to non-personal data – and to inform data holders of any unauthorised transfer, access, or use of non-personal data (Art. 21(5)). Where (also) personal data is at stake, the provisions of the GDPR take precedence.

3.3.10 Consent and permission

In order to facilitate data sharing for the social good in practice, RDAOs should provide tools for easily providing and withdrawing consent (person-

al data) and permission (non-personal data) (Art. 21(3) DGA). However, this is no easy task. Obtaining valid consent for the processing of personal data under the GDPR (Art. 6(1) (a) GDPR) is subject to certain requirements that, particularly where the purpose of the processing is not clear from the outset, are difficult to fulfil. This is also the case when data is collected and made available for altruistic grounds by RDAOs (cf. Recital 50 DGA; Specht-Riemenschneider, 2023, p. 658; von Hagen and Völzmann, 2022, p. 177). Thus, obtaining consent pursuant to Art. 6(1) (a) GDPR and – for very sensitive data, such as health data – and under the even stricter requirements of Art. 9(1) (a) GDPR, has been identified as a major obstacle and challenge to data altruism activities and scientific research in general (cf. Steinrötter, 2021, p. 61). In order to *help* data altruism organisations deal with this issue, the EC will, according to Art. 25 DGA, develop a European data altruism consent form. However, this has yet to be adopted. In addition, it still remains to be seen how helpful the final consent form will be (see Schreiber, Pommerening and Schoel, para. 88). First, the European Data Protection Board has been consistently hesitant to approve a model consent form as fulfilling the requirements set forth in the GDPR, arguing that it depends on the particular circumstances of any single case. Hence, it is unlikely that a consent form will be adopted which could be used straightforwardly (Rachut, 2024, p.252). Second, a technical solution for obtaining (and withdrawing) consent in line with the GDPR would be most favourable for making data wallets, consent management tools, and other data sharing platforms work in practice (European Commission, 2020b, p. 14). Whether guidelines on how such technical implementation could look like will (and can) be developed is currently an open question.

An additional layer of complexity is introduced by the unclear legal nature of the permission a data holder has to give for the processing of non-personal data. As far as non-personal data is not a trade secret and a data collection is not protected by IP rights, no exclusive position in relation to non-personal data exists. Consequently, a permission to use non-personal data would actually not be necessary. Most likely, the required permission has to be interpreted as the very basic (implicit) agreement between the RDAO and the data holder sharing non-personal data on the provision of the data altruism service. Notwithstanding, the wording of Art. 25 DGA suggests that the European Consent Form will also contain a template for giving permission to the processing of non-personal data.

3.3.11 Summary, guiding principles, and perspective

In principle, the provisions on data altruism organisations rightly address three main obstacles to data sharing for the social good which have been identified in recent years: no established players in the markets, a lack of trust, and legal uncertainty (particularly regarding the processing of personal data).

However, the requirements that data altruism organisations have to meet in order to be registered are high. From the very outset, the need to be established as a legal person excludes all kinds of projects and studies which are, however, the most common form of organisation in scientific research (Spindler, 2021, p. 105). As data altruism organisations must operate on a not-for-profit basis and be legally independent from any entity operating on a for-profit basis, they will need financial resources to be able to run their services (in terms of research data repositories, see OECD, 2017, p. 20). Moreover, they must provide their service as functionally separate from any other service; this requires building an independent organisational and technical infrastructure which goes hand in hand with significant costs. Whether sufficient data altruism organisations fulfilling these requirements will appear must be awaited. Pessimistically speaking, the mere number of only *one* registered data altruism organisation throughout 27 Member States raises certain doubts in this regard.

In terms of the second point, trust, the DGA's strict requirements are suitable for safeguarding the envisaged role of RDAOs as not only neutral, but also altruistic players. Due to the particular character of RDAOs acting for the social good, it is convincing to define even stricter requirements than for other types of data intermediaries. Potential data donors should be sure that "their" data is only used for the purposes in the general interest they wished them to be used for, such as for health research. Thus, also in terms of data altruism organisations, the DGA can contribute to increased trust in respective players. Apart from the question of whether data altruism organisations will emerge in the EU despite the strict requirements set out in the DGA, the question also arises as to whether the trustworthiness of RDAOs is sufficient to incentivise data subjects and data holders to donate data for objectives of general interest. Whether potential data donors can be prompted to share data by offering additional incentives, such as by providing small rewards to persons who donate their data, remains open. Recital 45 DGA solely states that "data subjects should be able to receive

compensation related only to the costs they incur when making their data available".

Notwithstanding, if, third, the existing legal uncertainty on how to obtain valid consent for pooling and making personal data available for altruistic purposes in line with the GDPR cannot be reduced, it may be difficult in practice to make these initiatives fly.

From a practical point of view, the EHDS[14] may significantly impact the role of data altruism organisations. So far, data cooperatives and comparable projects for data donation have primarily existed in the health sector. With the new rules on the secondary use of health data, the relevance of data altruism organisations in the health sector might decrease. As the example of Spain's DATALOG shows, sustainability and green development might currently be the most promising sector for the development of data altruism organisations.

4. The role of trust in business and consumer decisions?

As the analysis has shown, the DGA is heavily reliant on the principle of trust. This concerns both the set of rules on a standardised mechanism for facilitating the re-use of data held by public sector bodies that cannot be made available as open data due to their sensitivity and the provisions on data intermediaries. As shown above (see Section 2), from a theoretical point of view, legal norms can reduce complexity, as the uncertainty over a counterpart's behaviour is perceived as being narrowed down from a multitude of possible options to fewer probable – lawful – options. This reduces risk and, thus, can increase trust. Hence, the DGA's provisions on G2B data sharing and data intermediaries are well suited to the theoretical concept of trust, both from a sociological and a legal perspective. However, the follow-up question arises as to whether this concept works in practice and, in particular, whether the relevant market players really value trust when taking business and consumer decisions.

Through establishing a minimum set of rules for facilitating data re-use requests and defining conditions for re-use that aim to protect the data's sensitive character, the DGA pursues the objective of increasing transparency. A higher degree of transparency can increase citizens' trust in public

14 For more information on the EHDS, see Chapter 15 'The European Health Data Space: The Next Step in Data Regulation' by Lisa Markschies.

sector bodies. On the one hand, public sector bodies should not be able to retain data that are valuable for scientific research or innovative business models, while, on the other hand, they are bound to their public task of preserving the data's sensitive nature, even when making them available for re-use. Hence, this framework can contribute to a more transparent mechanism that might favour trust in the acting institutions (i.e., public sector bodies). Notwithstanding, the success of the framework for G2B data flows beyond open data will heavily depend on whether data access and re-use requests are handled efficiently in practice and – most importantly – which data the Member States decide to make available. Thus, the concept of trust plays an important role in this context, but is, on its own, not decisive for the success of the DGA's objectives and the envisaged decisions of the involved actors. When looking at the provisions on data intermediaries, trust, however, serves as the central reference point. In the DGA, the European legislator follows the assumption that a lack of trust has, thus far, prevented data intermediaries from emerging. However, no empirical evidence exists in this regard (Hennemann and von Ditfurth, 2022, p. 1910; Kerber, 2021, p. 3).

First, the question arises whether a mandatory legal framework for data intermediaries as provided by the DGA can – as such – increase trust in these players. Taking into account the findings presented above, from a theoretical point of view, such a legal framework is indeed suitable for reducing the (perception of) risk that data intermediaries might opt to act in such a way as to serve their own business interests – as the big platforms mostly do. Consequently, the framework introduced by the DGA indeed has the potential to increase users' trust in data intermediaries. Increased trust might therefore impact users' choices.

Second, users would not only have to trust these players, but also have confidence in the business model of trustworthy intermediaries as such. In short, users would have to be willing to use data intermediary services for managing or sharing data. Third, even if that were the case, users, would have to sufficiently value *trust* when taking (privacy-related) decisions (Kerber, 2021, p. 4; Waldman, 2018, p. 47). From a theoretical point of view, trust seems to be the main *topos* for deciding with whom data should be shared. This is all the more true for the case of data, since data holders and data subjects, to a certain extent, lose *control* over data when having made them available to a third party for the first time. Notwithstanding, what drives user's privacy decisions has not for nothing been a highly debated question for decades – particularly from the perspective of behavioural economics, respectively law

and economics (see inter alia (influentially) Acquisti and Grossklags, 2005); for a recent empirical study, see Sprigman and Tontrup, 2024, p. 11, with comprehensive references on previous research). Consumer and business decisions are based on multiple factors and complex relations. For instance, the DGA also introduces logos and labels that should clearly signal compliance with the rules defined therein in order to provide transparent and easily accessible information. However, ultimately, consumer and business choices might not be rational, even when it comes down to trust. In addition, the price, certain network effects, and the straightforwardness of a service seem to be decisive factors for driving user decisions – being a *data leech* or recognised *data intermediary* that receives the data (Gellert and Graef, 2021, p. 8; Sprigman and Tontrup, 2024, p. 7).

Thus, although the objectives followed by the DGA theoretically align with the academic concept of trust, from a practical point of view, it seems questionable whether trust sufficiently influences business or consumer decisions, particularly in the data and platform economy. However (and more positively), from interdisciplinary perspective, this offers a plethora of anchoring points for further empirical research which would be necessary for answering these questions comprehensively.

5. Concluding remarks

The DGA is built on the assumption that increased trust can significantly influence user choices, thereby contributing to the overall objective to foster and facilitate data sharing in the EU. The idea that a clear legal framework, being for G2B data flows and for the provision of intermediation services, has the potential to strengthen trust in the respective actors and institutions and can thus impact users' decisions fits perfectly into the theoretical concept of trust. However, practically speaking, the question remains whether trust, on its own, can assume the envisaged essential role for consumer or business decisions in this regard.

All in all, therefore, it seems particularly doubtful that data intermediaries can fulfil the immense expectations that have been projected on them. In principle, data intermediaries could indeed assume an important role in the data economy, such as by facilitating voluntary data sharing and exchange, providing the infrastructure for making mandatory access regimes work in practice or offering tools for enforcing data subject's rights and managing consent for the processing of personal data in line with the

GDPR (Specht-Riemenschneider and Kerber, 2022, p. 24). However, the requirements are rather high and, for the time being, it seems questionable whether sufficient intermediaries fulfilling the respective standards will appear in the markets. This is, first, due to the cost side of the measures the DGA implements. Second, incentives for generating respective data intermediation services seem to be lacking, as it remains unclear whether users will turn to data intermediation services as expected.

Whether the DGA will positively impact the re-use of data held by public sector bodies does not solely depend on trust. Rather, which data the Member States decide to make available, and under which conditions, will be decisive. Hence, although the concept of trust also shapes the DGA's provisions on the re-use of public sector bodies, trust, on its own, is not decisive for the success of the DGA's objectives and the envisaged decisions of the involved actors.

Considering the broader picture, the EU is following a strong regulatory approach in trying to promote innovation in line with such democratic values as freedom of choice and digital sovereignty, safety and security, participation, and sustainability. In so doing, the EU is seeking to promote *regulation* as a unique selling point on a global level. This rationale underlies many of the recent EU legislative acts on data and the digital environment, and also shapes the DGA's provisions on data intermediaries. The DGA once more is an expression of a strongly *mission-based* legal intervention – a phenomenon which characterises European data-related legislation significantly and aims at shaping markets. Whether the relevant players will follow this approach remains to be seen.

References

Acquisti, A. and Grossklags, J. (2005) 'Privacy and rationality in individual decision making', *IEEE Security & Privacy*, 3(1), pp. 26–33.

Baloup, J., Bayamlioğlu, E., Benmayor, A et al (2021) 'White paper on the data governance act'. *SSRN* [Online]. Available at: https://ssrn.com/abstract=3872703 (Accessed: 27 January 2025).

Cole, M. (2022) 'Vertrauenswürdigkeit des Online-Umfelds', *UFITA*, pp. 305 – 327.

Corona Datenspende (2024) [Online]. Available at: https://corona-datenspende.github.io/en/ (Accessed: 27 January 2025).

'Directive 2000/31/EC of the European Parliament and of the Council of 8 June 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market ('Directive on electronic commerce')' (2000) *Official Journal* L 178, 17 July, pp. 1–16 [Online]. Available at: http://data.europa.eu/eli/dir/2000/31/oj (Accessed: 19 January 2025).

'Directive (EU) 2016/943 of the European Parliament and of the Council of 8 June 2016 on the protection of undisclosed know-how and business information (trade secrets) against their unlawful acquisition, use and disclosure' (2016) *Official Journal* L 157, 15 June, pp. 1–18 [Online]. Available at: http://data.europa.eu/eli/dir/2016/943/oj (Accessed: 27 January 2025).

'Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases' (1996) *Official Journal* L 77, 27 March, pp. 20–28 [Online]. Available at: http://data.europa.eu/eli/dir/1996/9/oj (Accessed: 27 January 2025).

European Commission (2018) *Commission staff working document guidance on sharing private sector data in the European data economy*. COM(2018) 232 final [Online]. Available at: https://digital-strategy.ec.europa.eu/en/news/staff-working-document-guidance-sharing-private-sector-data-european-data-economy (Accessed: 27 January 2025).

European Commission (2020a) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions – a European strategy for data*. COM(2020) 66 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066 (Accessed: 27 January 2025).

European Commission (2020b) *Commission staff working document, impact assessment report, accompanying the document proposal for a Regulation of the European Parliament and of the Council on European data governance (Data Governance Act).* SWD(2020) 295 final [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020SC0295 (Accessed: 27 January 2025).

European Commission (2024a), *Implementing the Data Governance Act – guidance document* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/new-practical-guide-data-governance-act (Accessed: 29 January 2025).

European Commission (2024b) *EU register of data intermediation services* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-intermediary-services (Accessed: 27 January 2025).

European Commission (2024c) *EU register of recognised data altruism organisations* [Online]. Available at: https://digital-strategy.ec.europa.eu/en/policies/data-altruism-organisations (Accessed: 29 January 2025).

European Union (no date) *European data* [Online]. Available at: https://data.europa.eu/data/datasets?superCatalog=erpd&locale=en (Accessed: 27 January 2025).

Eurostat (no date) *Microdata.* [Online]. Available at: https://ec.europa.eu/eurostat/web/microdata (Accessed: 27 January 2025).

Gellert, R. and Graef, I. (2021) 'The European Commission's proposed Data Governance Act: some initial reflections on the increasingly complex EU regulatory puzzle of stimulating data sharing' *TILEC Discussion Paper No. DP2021-006. SSRN* [Online]. Available at: https://ssrn.com/abstract=3814721 (Accessed: 27 January 2025).

Hartl, A. and Ludin, A. (2021) 'Recht der Datenzugänge', *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung*, pp. 534–538.

Hennemann, M. and von Ditfurth, L. (2022) 'Datenintermediäre und Data Governance Act', *Neue Juristische Wochenschrift*, pp. 1905–1910.

Kaesling, K. (2022) 'Vertrauen als Topos der Regulierung vertrauenswürdiger Hinweisgeber im Digital Services Act', *UFITA*, pp. 328–351.

Kerber, W. (2021) *DGA – einige Bemerkungen aus ökonomischer Sicht*. University of Marburg [Online]. Available at: https://www.uni-marburg.de/de/fb02/professuren/vwl/wipol/pdf-dateien/kerber_dga_einige-bemerkungen_21012021.pdf (Accessed: 27 January 2025).

Lauber-Rönsberg (2022) '"Vertrauenswürdige Rechtsinhaber" im Kontext des Urheberrechts', *UFITA*, pp. 265–276.

Lauber-Rönsberg, A. and Becker, P. (2023) 'Auswirkungen des Data Governance Act auf Forschungseinrichtungen und Repositorien', *Recht und Zugang*, pp. 30–47.

Leistner, M. and Antoine, L. (2022) *IPR and the use of open data and data sharing initiatives by public and private actors*. European Parliament [Online]. Available at: https://www.europarl.europa.eu/thinktank/en/document/IPOL_STU(2022)732266 (Accessed: 27 January 2025).

Liesching, M. (2022) 'Hassrede und NetzDG – Vertrauenskonzepte im Beschwerde-Management', *UFITA*, pp. 252–264.

Luhmann, N. (2014) *Vertrauen*. 5th ed. Constance & Munich: UVK Verlagsgesellschaft mbH.

Micheli, M. et al. (2023) *Mapping the landscape of data intermediaries*. Publications Office of the European Union [Online]. Available at: https://publications.jrc.ec.europa.eu/repository/handle/JRC133988 (Accessed: 27 January 2025).

OECD (2017) 'Business models for sustainable research data repositories', *OECD Science, Technology and Industry Policy Papers* 47 [Online]. Available at: https://doi.org/10.1787/302b12bb-en (Accessed: 27 January 2025).

OECD (2019) *Enhancing access to and sharing of data: reconciling risks and benefits for data re-use across societies*. OECD Publishing [Online]. Available at: https://doi.org/10.1787/276aaca8-en (Accessed: 27 January 2025).

OECD (2022a) 'Fostering cross-border data flows with trust', *OECD Digital Economy Papers, No. 343* [Online]. Available at: https://doi.org/10.1787/139b32ad-en (Accessed: 27 January 2025).

OECD (2022b) *Declaration on a trusted, sustainable and inclusive digital future*. OECD Legal Instruments [Online]. Available at: https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0488 (Accessed: 27 January 2025).

Oxford English Dictionary (2024) '*trust*' (*n.*). Oxford: Oxford University Press [Online]. Available at: https://doi.org/10.1093/OED/5777528687 (Accessed: 27 January 2025).

Peukert, A. (2022) 'Vertrauen als Topos der Plattformregulierung', *UFITA*, 8, pp. 230–251.

Peukert, A. (2023) 'The regulation of disinformation in the EU – overview and open questions' *SSRN* [Online]. Available at: https://ssrn.com/abstract=4496691 (Accessed: 27 January 2025).

Rachut, S. (2024) 'Datenaltruismus unter dem Data Governance Act. Verpasste Chance beim Zusammenspiel von DGA und DS-GVO', *Zeitschrift für Datenschutz*, 14(5), pp. 248–253.

'Regulation (EU) 2019/1150 of the European Parliament and of the Council of 20 June 2019 on promoting fairness and transparency for business users of online intermediation services.' *Official Journal* L 186, 11 July pp. 57–79 [Online]. Available at: http://data.europa.eu/eli/reg/2019/1150/oj (Accessed: 27 January 2025).

'Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)' (2022) *Official Journal* L 152, 3 June, pp. 1–44, [Online]. Available at: http://data.europa.eu/eli/reg/2022/868/oj (Accessed: 27 January 2025).

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L, 2024/1689, 12 July [Online]. Available at: http://data.europa.eu/eli/reg/2024/1689/oj (Accessed: 27 January 2025).

'Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847' (2025) *Official Journal* L, 2025/327, 5 March 2025 [Online]. Available at: http://data.europa.eu/eli/reg/2025/327/oj (Accessed: 7 March 2025).

Richter, H. (2022) 'Ankunft im Post-Open-Data-Zeitalter', *Zeitschrift für Datenschutz,* 12(1), pp. 3–8.

Richter, H. (2023) 'Looking at the Data Governance Act and beyond: how to better integrate data intermediaries in the market order for data sharing', *GRUR International Journal of European and International IP Law*, 72(5), pp. 458–470.

Richter, H. and Slowinski, P. (2019) 'The data sharing economy: on the emergence of new intermediaries', *International Review of Intellectual Property and Competition Law*, 50, pp. 4–29.

Schneider, I. (2023) 'Digital sovereignty and governance in the data economy: data trusteeship instead of property rights on data' in Godt, C. and Lamping, M. (eds.) *A critical mind*. Berlin: Springer, pp. 369–406.

Schneider, I. (2024) 'Data stewardship by data trusts: a promising model for the governance of the data economy?' in Padovani, C. et al. (eds.) *Global communication governance at the crossroads*. Cham: Springer Nature Switzerland, pp. 333–349.

Schreiber, K., Pommerening, P. and Schoel, P. (2023) *Das neue Recht der Daten-Governance*. Baden-Baden: Nomos.

Simon, N., Markopoulos, I., Gindl, S. et al (2020) *Definition and analysis of the EU and worldwide data market trends and industrial needs for growth*. Trusts [Online]. Available at: https://www.trusts-data.eu/wp-content/uploads/2021/07/D2.1-Definition-and-analysis-of-the-EU-and-worldwide-data-market-trends-....pdf (Accessed: 27 January 2025).

Specht-Riemenschneider, L. (2023) 'Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und DSGVO', *Zeitschrift für europäisches Privatrecht*, pp. 638–672.

Specht-Riemenschneider, L. and Hennemann, M. (2023) *Data Governance Act.* Baden-Baden: Nomos.

Specht-Riemenschneider, L. and Kerber, W. (2022) *Designing data trustees – a purpose-based approach*. Konrad Adenauer Stiftung [Online]. Available at: https://www.kas.de/documents/252038/16166715/Designing+Data+Trustees+-+A+Purpose-Based+Approach.pdf/ffadcb36-1377-4511-6e3c-0e32fc727a4d (Accessed: 27 January 2025).

Spindler, G. (2021) 'Schritte zur europaweiten Datenwirtschaft – der Vorschlag einer Verordnung zur europäischen Data Governance', *Computer und Recht*, pp. 98–108.

Sprigman, C. and Tontrup, S (2024) 'Privacy decision-making and the effects of privacy choice architecture: experiments toward the design of behaviorally-aware privacy regulation', *Journal of Empirical Legal Studies*, 21(2), pp. 1–55.

Steinrötter, B. (2021) 'Datenaltruismus', *Zeitschrift für Datenschutz*, pp. 61–62.

Von Hagen, P. and Völzmann, L. (2022) 'Datenaltruismus aus datenschutzrechtlicher Perspektive', *MMR – Zeitschrift für IT-Recht und Recht der Digitalisierung*, pp. 176–181.

Waldman, A. (2018) *Privacy as trust – information privacy for an information age.* Cambridge: Cambridge University Press.

Wernick, A., Olk, C. and von Grafenstein, M (2020) 'Defining data intermediaries – a clearer view through the lens of intellectual property governance', *Technology and Regulation,* pp. 65–77.

Zingales, N. (2022) 'Data collaboratives, competition law and the governance of EU data spaces' in Kokkoris, I. and Lemus, C. (eds.) *Research handbook on the law and economics of competition enforcement*. Cheltenham/Northampton: Edward Elgar, pp. 8–49.

The Open Data Directive: Potential and Pitfalls for the Social Sciences

Nik Roeingh & David Wagner

Abstract

The Open Data Directive (ODD) constitutes a key element of European digital policy, designed to promote the reuse of public sector data. It aims to enhance government transparency, public participation, and economic growth by regulating conditions for public data reuse. While the ODD does not establish a general right to data access, it strengthens the reuse of publicly available datasets and introduces High Value Datasets (HVDs), which must be made available free of charge and with minimal restrictions.

For the (social) sciences, the ODD creates a dual role: As users, (social) scientists benefit from access to public sector data, particularly HVDs encompassing geospatial, environmental, and statistical data. Simultaneously, the directive imposes obligations on (social) scientists conducting publicly funded research. Under the ODD, publicly funded research data must be reusable for commercial and non-commercial purposes when deposited in institutional or subject-based repositories. Notably, the directive distinguishes between research data and scientific publications, explicitly excluding the latter from its scope. By facilitating access to valuable datasets while promoting open science, the ODD presents an opportunity for the social sciences. It aligns with broader trends toward open data and transparent governance, making research results more accessible and reusable. However, implementation depends on national policies, and limitations – such as restrictions on access to public undertakings' data or dynamic datasets – persist. Despite these constraints, the directive marks a significant step toward greater openness in research and public sector information.

1. Introduction

For over two decades, Western societies have embraced "open government data" as a central credo of digital policy. Previously, the principle of official secrecy – long prevalent in continental Europe, and legally and culturally

ingrained in state bureaucracies – restricted access to government information (Ramge and Mayer-Schönberger, 2020, p. 169).

The groundwork for a shift towards *openness* was established over 50 years ago, as the 1970s brought a new understanding of the state–citizen relationship.[1] At the time, the perception emerged that government accountability requires transparency, which would enable citizens to participate more fully (Henninger, 2013, p. 81). This was the starting point of the open government debate in its transparent and participatory form (Lederer, 2015, p. 56). With the advancing digitalisation of the 1980s, the discourse expanded. Beyond the democratic and participatory goals, the commercial potential of information became evident as it became easier to exchange, analyse, and leverage machine-readable data (Aichholzer and Burkert, 2004, pp. 3–4; Stieglitz, Orszag and Orszag, 2000, 53 et seq.).

Finally, in 2009, US President Barack Obama gave a significant international boost to the principle of openness. His administration's "Memorandum on transparency and open government" (Obama, 2009b) and the "Open government directive" (Obama, 2009a) emphasised a commitment to transparent, participatory, and collaborative governance, promoting the proactive release of government data. This commitment had a global impact, raising awareness about transparent administration and the value of open government data.

Back in 2000 – when Obama had only just missed out on a seat in Congress – the European Union was already considering opening up government data, due primarily to the potential economic and societal benefits of re-using government information (European Commission, 2000, 26 et seq.). The first EU-wide standardisation occurred in 2003 with the Directive on Public Sector Information (PSI) (Directive 2003/98/EC). Following multiple revisions, the PSI Directive was updated and replaced in 2019 by the Open Data Directive (ODD) (Directive (EU) 2019/1024), marking a significant milestone in the EU's legal approach to openness. It is this milestone that is at the centre of this investigation, which we shall consider from a scientific perspective.

As government-funded science both relies on and generates data, it has consistently been part of the openness debate, now reinforced by the ODD. Science is expected not only to benefit from open data, but also to contribute to it, specifically through open science data. This expectation spans

1 For a comprehensive and well-founded examination of the genealogy of the term "open data", see Gray (2014).

all disciplines, including such traditional fields as medicine and natural sciences, and is increasingly extending to the social sciences. This study aims to assess how the social sciences can benefit from the ODD and the extent to which they are obligated to contribute within its framework.

Section 2 offers a comprehensive and coherent account of the concept of open government data. It begins by providing a concise overview of the rationale behind open government data (2.1) and then proceeds to examine it through the lens of the state of data (2.2). In order to gain further insights, we then analyse its components and their general implications (2.3), which lay the groundwork for examining the ODD as an extension of the broader concept of open government in Section 3. This section begins by exploring the historical foundations of the ODD (3.1) and then addresses the core question of the level of data openness it ensures, grounded in the concept of "openness" (3.2).

Section 4 focuses specifically on the role of the social sciences within the ODD, exploring the extent to which social scientists can benefit from the Directive when their research relies on government data (4.1), as well as to what extent they must also contribute data themselves when their research is government funded (4.2).

Methodologically, this chapter employs the full range of legal interpretative approaches for its jurisprudential sections. Using grammatical, systematic, historical, and teleological methods, it examines the varying degrees of openness mandated by the ODD and the associated rights and obligations for (social) sciences. The analysis also incorporates European methodology, acknowledging the unique linguistic considerations of European law due to the multilingual nature of legal texts and recitals.

2. Open (government) data – a spectral concept

2.1 Understanding open government data through its rationale

The rationale behind open government data cannot be distilled into a single line of reasoning, but has several legitimisation approaches. The objectives can be grouped into three main categories: first, enhancing transparency in government and administration, as aligned with the principle of freedom of information (Kitchin, 2014, p. 56; Mayernik, 2017, p. 2); second, strengthening participation and collaboration (Filippi and Maurel, 2015,

p. 2; Kitchin, 2014, p. 55); and third, fostering innovation and economic growth (Kitchin, 2014, p. 55; Richter, 2021, p. 43). While transparency and participation were the initial focus, attention has gradually shifted towards ensuring that open government data serves as a valuable resource for industry and academia, enabling the creation of new scientific knowledge and economic value (Borgesius, van Eechoud and Gray, 2015, p. 2083; Stieglitz, Orszag and Orszag, 2000, 53 et seq.). Consequently, the public sector is encouraged to make as much of its data as available as possible, ensuring that everyone – the scientific community included – can access and re-use them for new purposes at no cost (Geiger and von Lucke, 2012, 268 et seq.).[2]

2.2 Understanding open government data as a data state

Apart from its underlying rationale, open government data can also be viewed simply as a description of a data state (Open Data Institute, 2020). Data are considered "open" if they can be freely used, modified, and shared by anyone for any purpose (Open Definition, no date). Adding "government" specifies the source of such data. In this sense, "open data" contrasts with "closed data", which are accessible and usable only within an organisation, with third-party access restricted. These terms – open and closed – define opposite ends of a data accessibility spectrum. Between these poles lie "shared data", which are also available to third parties, but under certain restrictive conditions (Fia, 2021, p. 189).

2 In 2007, a working group in Sebastopol, California, established the "8 principles of open government data", which have since become the standard for assessing openness in government records. These principles outline open government data as public data that are complete, primary, timely, accessible, machine-processable, non-discriminatory, non-proprietary, and license-free, with compliance that is reviewable. For more details, see The Annotated 8 Principles of Open Government Data (no date).

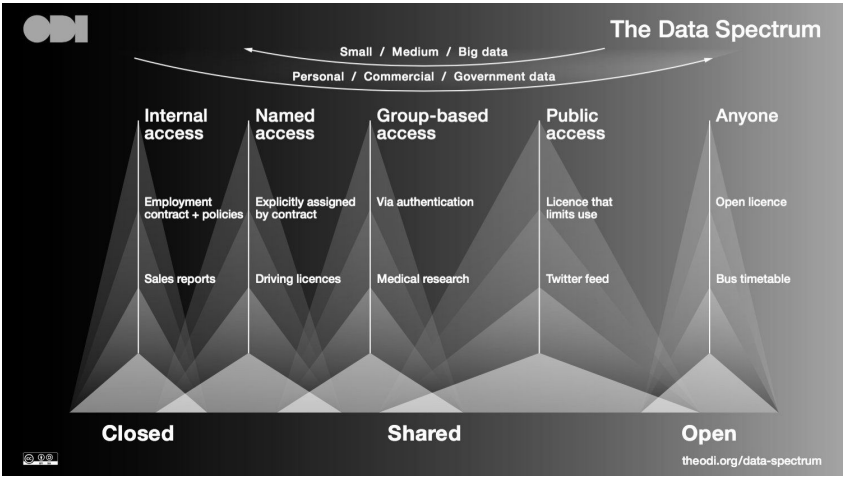

Figure 1: The data spectrum (Source: ODI, 2020)

Viewing open data as a state of data provides the advantage of defining it clearly and removing ideological undertones. However, this perspective should not mask the fact that distributing data as "open" is often driven by specific motives, which may not align with those stated publicly. For instance, a government may release mobility data to justify a new traffic management system, implying transparency. Yet, it may withhold other data that could have suggested alternative decisions.[3] For data users, these motives might be secondary if the data's source and quality are transparent, as their interest may not necessarily lie in scrutinising government actions.

2.3 Open – government – data: a fully-fledged definition?

A more detailed definition of open (government) data requires analysing each element of the term. However, these elements cannot be viewed in isolation, as their meanings become interdependent when combined into the concept of open data.

3 This problem is part of the wider issue that data are not neutral representations of the physical world, but that there is a certain distance between representation and object, as is repeatedly emphasised in science and technology studies. Supposedly neutral images are referred to as "view from nowhere" in order to emphasise the impossibility of a neutral perspective, which is inherent in every representation (Helmreich, 2011, p. 1229).

2.3.1 Openness

A closer examination of the criterion of "openness" reveals that earlier definitions encompass only the universally agreed-upon core elements among all stakeholders. Over time, additional criteria have been introduced to designate data as "open". The first widely recognised proclamation of open data stipulated, among other requirements, that data be machine-readable (Fia, 2021, p. 190).[4] Subsequent frameworks have not only heightened the technical standards for openness, but have also incorporated the underlying motivations for providing the data directly into the definition.[5]

The concept of "openness" is inherently gradual rather than binary, allowing for the addition of various requirements. This nuance is reflected in Tim Berners-Lee's "5-star open data model" (W3C, 2013).[6] Technical specifications for data openness are crucial for findability and reusability, and should not be underestimated. However, from a legal perspective, data are considered "open" if they are free from terms of use that impose restrictions beyond what the law requires. Additionally, it is important to recognise that, in light of citizens' fundamental rights, not all data should be publicly accessible. For example, making personal data (e.g., health information) openly available could expose individuals to significant risks.

2.3.2 Data

The term "data" serves as the object that the adjective "open" more precisely describes. Despite being central to the *datafication* movement since the 1990s,[7] its fundamental meaning remains unclear. Generations of scientists have attempted to define it. For the purposes of this chapter, it suffices to understand data as "information encoded in a way that can be processed

4 The ODD defines a machine-readable format as a "file format structured so that software applications can easily identify, recognize and extract specific data, including individual statements of fact, and their internal structure" (Art. 2(13)).

5 The Open Data Charter incorporated the potential of Open Data to foster transparency and citizen engagement, as well as to spur inclusive economic development (see ODC, no date).

6 Tim Berners-Lee is not only a strong voice in data policy, but also set out the basic structure of the World Wide Web as we know it with his paper "Information management: a proposal" (Berners-Lee 1989, 1990).

7 Datafication refers to the ongoing process of collecting, storing, and analysing digital data in all areas of society.

by machines" (Zech, 2015, p. 193). This rather axiomatic definition, which heavily emphasises the term's digital and semantic aspects, is justified by the fact that data are typically shared for their content and can only be truly open if at least shared in digital form.[8]

2.3.3 Government

Finally, at first glance, the term "government" seems clear. However, this is only true if "government" is equated with all state actors who are allowed to exercise sovereign powers to interfere with the rights of citizens.[9] Besides that, states are nowadays frequently active in service administration: they build infrastructure and support people in need with social systems. Moreover, states can even act commercially, setting up companies under private law that do not exercise any sovereign power. In light of the diversification of state activities, actors turned the demand for the state to open its data through the catchy slogan "public money, public data" (Kitchin, 2014, p. 48). As the history of the ODD shows, this demand has increasingly made its way into binding legislation through the various iterations of the directive. Still, to date, not all public sector organisations are obliged to make data openly available.

3. Openness in the Open Data Directive

Although access and re-use of data are two sides of the same coin (Augsberg, 2016, p. 46), the ODD primarily regulates the re-use of data that are already accessible, without creating an obligation to provide access.[10] This seemingly odd separation between access and re-use arises from the division of legislative powers between the EU and its Member States: access to government data has traditionally been recognised as an inherent legislative

8 This is because the transfer of analogue data would be accompanied by significantly higher marginal costs, which would prevent them from being given away free of charge. More time and effort are also required to use analogue data for new purposes, because transferring them requires manual work.

9 In a state governed by the rule of law, this authorisation is typically only granted to state actors.

10 In this respect, the new rules on high value data are the exception to that rule.

power of the Member States, as it touches upon the core of sovereignty.[11] In contrast, the re-use of data can be grounded in the EU's competence to ensure the functioning of the internal market (Article 114 of the Treaty on the Functioning of the European Union (TFEU); Recital 7 of the ODD).

3.1 A brief history of internal market regulation for open public sector data

For several decades, European initiatives have aimed to establish a unified information market. At around the turn of the millennium, the EU began discussing the general re-use of government information from the standpoint of economic value creation and societal benefits (European Commission, 2000, pp. 26 et seq.). Gradually, there has been a growing recognition that public sector information should be viewed not only as a means of promoting transparency, but also as an economic asset capable of adding value.[12] Technological advancements – particularly the rise of digitalisation – have fuelled political aspirations to open up state information resources (Richter, 2021, pp. 49 et seq.).

These efforts culminated in the 2003 PSI Directive, which pursued three primary objectives. First, it aimed to contribute to the creation of a single market for public sector information and to harmonise laws at a minimal level, thereby addressing the divergent provisions and procedures among Member States regarding the use of public sector information sources (Recital 6, PSI Directive). Second, it sought to prevent distortions of competition in the internal information market by ensuring fair, reasonable, and non-discriminatory conditions for re-use (Recitals 1, 8, 25, PSI Directive). Finally, it intended to promote economic growth by facilitating the cross-border use of public sector information. The European legislator recognised this information as an essential raw material for products and services with digital content (Recital 5, PSI Directive).

In 2013, the PSI Directive underwent its first amendment following an evaluation by the European Commission (EC) (Directive 2013/37/EU). The primary reasons for these changes were that, despite earlier progress,

11 Exceptions can only exist where normative requirements on the provision of data fall within a special legislative competence of the European legislator, such as in the environmental sector.

12 While there is a plethora of studies, which argue for economic benefits from opening up government data, there is a lack of hard data supporting these claims (see van Eechoud, 2016, p. 39; Richter, 2021, p. 44).

the internal information market remained both practically and legally fragmented (Wirtz, 2014, pp. 389 et seq.). Additionally, open data policies advocated for the active promotion of open data to enhance the availability and re-use of public sector information with minimal restrictions (Recital 3, PSI Directive 2013). The focus shifted towards an enhanced exploitation of the economic and social opportunities arising from the re-use of information (Recital 5, PSI Directive 2013). This amendment, which also addressed the technically outdated aspects of the PSI Directive, was intended to accelerate this transformation.

In the six years following the last amendment, technological advancements further widened the gap between law and reality. Consequently, the PSI Directive was thoroughly revised in 2019 and has since been referred to as the ODD. This technological progress is notably encapsulated in the term "data-based society" (Richter, 2023d, Recital 30).[13] Accordingly, the promotion of artificial intelligence (AI) was incorporated into the Directive's objectives during the legislative process. The main changes in the new iteration involve expanding the material scope to include public undertakings and research data. Prior to this revision, educational and research institutions were explicitly excluded from the Directive's scope. Since 2013, the EU has taken measures to promote open data, including policies for open access to EU-funded research data (Gobbato, 2020, p. 151; Richter, 2018, p. 53). In light of this, the ODD now also addresses research data.

Moreover, the legislator has revised the compensation rules by establishing the principle of free provision, tightening exclusivity regulations, and promoting real-time access to dynamic data (Recital 4 ODD). Additionally, the ODD now authorises the EC to define a list of High Value Datasets (HVDs) that public authorities and public undertakings in Member States are required to provide in accordance with open data principles, under conditions to be specified in implementing acts.

The ODD pursues three primary objectives. First, it seeks to harmonise laws to create a single market and prevent distortions of competition within it (Recitals 3, 12 ODD). Second, it aims to promote digital innovation by

13 Recitals 10, 11 ODD. Although the focus of the ODD has evolved over the years, its central regulatory object remains the same: it employs the outdated concept of "documents". This term is defined as "any content whatever its medium (paper or electronic form or as a sound, visual or audiovisual recording)" and "any part of such content" (Art. 2 para. 6). Due to the explicit emphasis on content and the medium's independence, data are addressed as a specific type of document.

considering public sector information as essential raw material for products and services that benefit both consumers and companies. The Directive emphasises fostering innovation, particularly regarding AI applications, which it views as transformative for all sectors of the economy (Recitals 3, 9, 13 ODD). Third, it now aims to ensure that the re-use of data contributes to social purposes, such as accountability and transparency, ultimately enabling the public sector to improve the fulfilment of its tasks (Recitals 13, 14 ODD). This addition introduces an original open data aspect to the already-established competition and industrial policy objectives in the new version, although it is more complementary than fundamentally transformative. As an EU directive, it addresses Member States, which then transpose its provisions into national legislation.

3.2 Categories of openness in the Open Data Directive

The ODD's inherent commitment to openness is reflected in its fundamental principle regarding the re-use of documents (Art. 3 para. 1). It mandates that Member States make all existing documents within the Directive's scope re-usable for commercial or non-commercial purposes. For instance, data collected by a municipal transport company could be repurposed to develop a mobility app offering real-time updates, dynamic route planning, and alternative connection suggestions. However, Art. 3, para. 1 of the ODD applies only if a document is accessible. This limitation weakens the Directive's effectiveness through not barring Member States from restricting or excluding access to documents under their national laws (Martini, Haußecker and Wagner, 2022, pp. 7 et seq.; Recital 23 ODD).

As with any guiding principle, the concept of unrestricted re-use is a goal to be pursued to the greatest possible extent. It should thus be regarded as an optimisation requirement that can be satisfied to varying degrees depending on specific parameters. These parameters are manifested in various categories of openness, notably: the absence of access barriers, non-discriminatory access, the level of usage costs, the design of terms of use, machine interpretability, data completeness, and the use of open formats and standards, among others (Beyer-Katzenberger, 2014, pp. 144 et seqq.). The ODD stipulates a range of different specifications concerning these aspects.

3.2.1 Standard licences (Art. 8 ODD)

The first limitation to the general principle of re-use is that data providers may attach conditions to re-use through licenses (Art. 8 ODD).[14] However, these conditions must remain within the Directive's normative framework; they must be "objective, proportionate, non-discriminatory, and justified on grounds of a public interest objective" (Art. 8 para. 1 ODD). Furthermore, they should "not unnecessarily restrict possibilities for re-use and shall not be used to restrict competition" (Art. 8 para. 1 ODD). The legislator imposes substantive legal requirements that any restrictions on re-use must meet. If these are not satisfied, the conditions are unlawful.[15]

The European legislator recommends that Member States use open standard licenses (Art. 8 para. 2 ODD).[16] Currently, a variety of licensing practices exist at the Member State level. In addition to the Creative Commons (CC) and Open Data Commons (ODC) licenses, there are also country-specific licensing models, such as "Data License Germany 2.0" in Germany, "Licence Ouverte" in France, and the "Licentie modellicentie" in Belgium.[17] Furthermore, the use of data is often subject to such conditions as attribution requirements (Recital 44 ODD), protections against alteration, liability limitations, and considerations regarding the use of personal data.[18]

3.2.2 Available formats (Art. 5 ODD)

Another crucial factor that determines the degree of data openness is the format in which the data are available. Data formats are pivotal for the

14 Licensing presents significant challenges for open data as a whole. Essentially, if a user wishes to create a derivative work using two or more datasets, they must assess the license compatibility of all the datasets involved. Conceptually, this assessment yields only two outcomes: either the licenses are compatible or they are not. Therefore, considerations of license compatibility can become a substantial barrier to the re-use of multiple datasets made available under different licenses. In this sense, the need for compatibility assessments hinders the achievement of the EU's open data policy objectives (Graux, 2023, p. 5).

15 Failure to comply with these requirements has no tangible consequences for the licensor.

16 The Commission provides guidance on standard licensing (European Commission, 2014, 2 et seq.).

17 Graux (2023, 7 et seq.) gives a short empirical assessment of the state of play.

18 For individual licenses, see Richter (2023b, Recital 197 et seqq.).

usability *of* the data and shape the economic potential that can be derived *from* them (Richter, 2021, p. 159).

Since the data economy cannot process analogue information, it focuses on digitally structured, semantically meaningful data. Only such data can be processed en masse by machines. For example, environmental information in paper form is far less useful for the market entry of digital weather services than the provision of structured datasets. Indeed, the ODD grants users the right to receive information in any pre-existing format precisely because of the high innovation potential of machine-readable information (Art. 5 para. 1 ODD). Furthermore, it requires the conversion of data into an open, machine-readable, accessible, findable, and re-usable format, insofar as this is "possible and appropriate".

Dynamic data – that is, data updated frequently or in real time, such as sensor-generated weather data (Art. 2 para. 8 ODD) – are subject to specific rules. The ODD establishes that public sector bodies should make dynamic data available for re-use immediately upon collection, providing access through suitable application programming interfaces (APIs) and, where relevant, as bulk downloads (Art. 5 para. 5 ODD).[19]

To prevent undue financial strain on the public sector, the legislator limits both the obligation for public sector bodies to create or modify documents and the requirements for dynamic data (Art. 5 para. 3, Art. 6 ODD).

3.2.3 Charging (Art. 6 ODD)

Open data thrives on free data. Fees can prevent both transparency and data's role as a competitive asset. Thus, the ODD emphasises what Richter (2021, p. 160) has termed a "core competitive parameter", namely the price.

The challenge with fees is that their regulation impacts both data distribution and the potential for data generation (Drexl, 2014, pp. 1 et seq.; Podszun, 2016, pp. 335 et seq.). In the ODD, the legislator has determined that the re-use of documents should generally be free of charge (Art. 6

19 See the European Commission's (2018a, p. 23) findings that "with the growing importance of dynamic data, the insufficient use of APIs is regularly recognized as one of the main barriers for data re-use".

para. 1 ODD).[20] This aligns with the fact that the public sector must, in any case, create large volumes of data so as to fulfil its public duties.

As with any principle, that of cost-free access has exceptions. These are limited to the recovery of marginal costs incurred (Art. 6 para. 1 ODD). The marginal cost approach covers the costs associated with "the reproduction, provision, and dissemination of documents". Accordingly, public sector bodies can charge fees that cover only the marginal costs involved in re-use activities, such as anonymising personal data and protecting commercially confidential information. However, data providers cannot pass on data-generation costs to users and are not permitted to charge a profit (European Commission, 2014, p. 6). In cases where no measures are needed to protect personal or commercial rights, marginal costs are typically close to zero.[21]

3.2.4 Non-discrimination (Art. 11 ODD)

The ODD establishes the general principle of non-discrimination (Art. 11 ODD). Under this principle, any applicable conditions for the re-use of documents must be non-discriminatory for comparable categories of re-use, including cross-border. Any discrimination in re-use conditions therefore requires justification, which can be based on the comparability of the re-use categories (Lundqvist et al., 2015, pp. 100 et seq.). For instance, it is inadmissible to link different re-use conditions to the re-user's personal characteristics. However, differentiating conditions based on the type of use – such as commercial versus non-commercial – is allowed.[22]

20 The principle of free-of-charge access is, to a large extent, the cornerstone of developing open data for public sector information. This journey began in 2003 with the cost recovery principle, which was replaced in 2013 by the binding marginal cost principle. This shift towards reduced costs has consistently been accompanied by concerns about whether a marginal cost regime can ensure high-quality data if public bodies must bear the investment costs themselves.

21 In this case, the Commission recommends that no charges be levied (European Commission, 2014, p. 7). In practice, the marginal cost or free-of-charge policy has led to higher levels of demand satisfaction. However, reliable empirical conclusions on the effectiveness of the charging rules remain elusive, and implementation varies significantly across Member States (European Commission, 2018a, p. 37). Consequently, the effectiveness of the PSI Directive is not readily measurable (Deloitte and European Commission, 2018, pp. 174 et seqq., 250).

22 For more details, see Richter (2023c, Recital 8) and, for a contrary view, Wiebe and Ahnefeld (2015, p. 207).

3.2.5 Exclusivity arrangements (Art. 12 ODD)

A specific application of the principle of non-discrimination is the prohibition of exclusive agreements. This principle mandates that the re-use of documents must be accessible to all potential market participants, even if one or more actors already exploit value-added products based on those documents (Art. 12 para. 1 ODD).[23]

The Regulation seeks to minimise exclusivity agreements by public bodies, ensuring public sector information is available to all market participants under equal terms. This aims to dismantle existing information monopolies and prevent the formation of new ones, thereby opening the market and reducing competition distortions.

Under Art. 12 para. 1 ODD, exclusive rights may be exceptionally justified if necessary for providing a service in the public interest (para. 2), with the standard modelled on Art. 106 para. 2 TFEU. Assessing necessity requires an economic analysis (Richter, 2021, p. 168). Without justification, exclusivity agreements are deemed null and void, and, due to shifting market dynamics, such exclusive rights require periodic review.

The updated ODD also acknowledges de facto exclusivity, where exclusivity occurs without formal agreements or legal privileges. While para. 4 does not prohibit such exclusivity, it requires that any legal or practical arrangements restricting further re-use by third parties be published online two months prior to implementation and reviewed regularly. This inclusion reflects the growth of the digital economy and emerging business models that impact market dynamics, such as cases where a company provides data analysis to a public body in exchange for data access. Additionally, it addresses circumvention strategies where data access may not be exclusive to one company, but limited to a select group of particularly cooperative firms.

23 The inadmissibility of agreements between public bodies and third parties that grant exclusive rights is, in a sense, a natural extension of the prohibition of discrimination. Such agreements would require public bodies, at minimum upon request, to allow the same re-use conditions for all parties rather than excluding others entirely (Richter, 2021, p. 167). However, a legally binding exclusivity agreement de jure prevents the public body from adhering to the principle of equal treatment. The core regulatory content of Art. 12 lies in its significant legal impact: it declares exclusivity agreements invalid or requires them to expire (Art. 12 para. 5). Notably, the timeline for the expiry of these agreements now extends from 19 to 25 years into the future.

4. Social sciences: beneficiary and recipient of the Open Data Directive

The social sciences occupy a dual position within the framework of the ODD. On one hand, they benefit significantly from the EU's new data policy, as data gathered by public sector bodies and enterprises offer immense research potential. These data are critical for addressing research questions, testing hypotheses, and often ensure completeness and high data quality. On the other hand, the ODD represents a double-edged sword for the social sciences, in that they are typically state-funded and therefore fall under the open data regulations applicable to the public sector. Consequently, the social sciences can act both as beneficiaries and as obligated parties under the Directive.

4.1 Social sciences as a beneficiary

When social scientists seek to use data under the ODD, they tend to encounter varying degrees of data openness. The Directive does not always fully achieve its open data mandate; rather, it categorises data types and assigns each a different level of openness. Generally, the degree of openness correlates with the conditions under which the data are generated. Public bodies, which typically do not participate in market competition, are held to stricter openness requirements than public undertakings. However, the legislator mandates a particularly high level of openness for data with significant socio-economic potential.

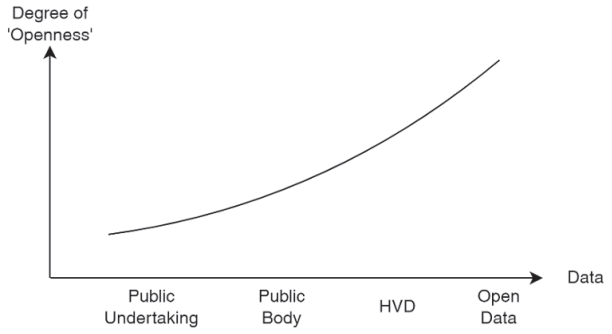

Figure 2: Degrees of "openness" in the ODD (Source: Authors)

4.1.1 High value datasets

The EU legislator has recognised that certain datasets hold greater socio-economic potential than others. These HVDs are governed by a more progressive utilisation framework than other data, with the aim of fostering innovation and enabling a level playing field for developing AI systems that address societal challenges (Bruns et al, 2020, pp. 9 et seq.). HVDs are made available for re-use with minimal legal and technical restrictions, and are free of charge.

According to the legislator, an HVD is a collection of "documents the re-use of which is associated with important benefits for society, the environment and the economy, in particular because of their suitability for the creation of value-added services, applications and new, high-quality and decent jobs, and of the number of potential beneficiaries of the value-added services and applications based on those datasets" (Art. 2(10) ODD). The core thematic categories in which these data are intended to create socio-economic added value are currently geospatial, Earth observation and environment, meteorological, statistics, companies/company ownership and mobility (Deloitte and European Commission, 2020, p. 7 et seq.). Nevertheless, the ODD also empowers the EC to introduce new thematic categories of HVDs in order to reflect technological and market developments (Art. 13 para. 2 ODD). In addition, the legislator delegates to the EC the authority to manage the use of HVDs through delegated acts (Art. 13 para. 2 and Art. 14 para. 1 ODD).

The Commission exercised this authority in 2022 through Implementing Regulation (EU) 2023/138, which entered into effect on June 9 2024. This regulation specifies HVDs and includes an annex listing the datasets held by public authorities, along with guidelines for their publication and use (e.g., data and metadata format requirements). Unlike regular datasets, HVDs must be made available for further use by public authorities in a documented, EU-wide, or internationally recognised, open, machine-readable format via the latest APIs[24] and as bulk downloads, accompanied by comprehensive metadata. These datasets are made available under the Creative Commons BY 4.0 license or an equivalent or less restrictive open license. However, HVDs owned by public undertakings are excluded from the Regulation's scope (Recital 7 S. 2 Implementing Regulation (EU)

24 An API refers to a set of functions, procedures, definitions, and protocols for machine-to-machine communication and the seamless exchange of data (Art. 2(6) Implementing Regulation (EU) 2023/138).

2023/138). Unlike the ODD, which required transposition into national law in each EU Member State, the Implementing Regulation applies directly across all EU Member States.

However, even for HVDs, one of the core parameters of openness – the cost of a dataset – faces certain restrictions. While HVDs are generally required to be available free of charge, the ODD specifies exceptions (Art. 14 paras. 3, 4, 5 ODD). Libraries (including university libraries), museums, and archives are exempt from this requirement (Art. 14 para. 4 ODD). Additionally, public sector bodies that need to generate revenue to cover a substantial portion of their costs in fulfilling their public service mission – and for whom free provision would significantly impact their budget – may also be exempted. Member States are allowed to waive the requirement for these bodies to provide HVDs free of charge for up to two years after the relevant implementing act takes effect (Art. 14 para. 5 ODD). Nonetheless, only a small number of public bodies are expected to meet these conditions, as most are funded by tax revenues rather than their own income.

4.1.2 Public sector bodies' data

The degree of openness decreases rapidly in the case of data from public sector bodies that do not qualify as HVDs. This is evident from the fact that certain data falls outside the ODD's scope: if data provision does not align with a public sector body's legally defined tasks, it is excluded from the Directive's application (Art. 2 para. 2 lit. a ODD). This provision reflects the EU legislator's intent to avoid imposing regulatory restrictions on data produced by public sector bodies under market conditions. Thus, if public bodies create data competitively and with the aim of profit – responding solely to demand and third-party purchasing power – the ODD does not apply.

Dynamic data also face openness limitations, as they must be made available as bulk downloads after collection only to the extent that doing so does not exceed the financial and technical capacities of the public body, thereby avoiding disproportionate effort (Art. 5 para. 6 ODD).

The principle of open data is further limited regarding fees. Although the ODD generally mandates that re-use of documents be free of charge (Art. 6 para. 1 ODD), it allows exceptions if a public sector body must generate revenue to cover substantial costs incurred in fulfilling its public mission (Art. 6 para. 2 lit. a ODD). However, in light of the general mandate for free re-use, this exemption is intended to be interpreted narrowly.

Although not primarily aimed at ensuring a high degree of openness, the ODD includes a ban on cross-subsidisation to protect fair competition.[25] If public sector bodies use data as source material for business activities outside their public mandate, the same fees, charges, and other conditions must apply to the provision of documents for these activities as for other users (Art. 11 para. 2 ODD). This provision aims to prevent public bodies, as providers of data products or services, from directly or indirectly pushing private companies out of the market. Such a risk would arise if public bodies could re-use their raw data (originally created to fulfil public tasks) free of charge or at preferential rates compared to third parties. Thus, while the cross-subsidisation ban primarily addresses competition concerns, it also ensures that public bodies do not monopolise their data, thereby making more data available for re-use.

4.1.3 Public undertakings' data

The data of public undertakings diverges even further from the open data ideal. The ODD does not apply to data from public undertakings that is not generated as part of providing services of general interest (Art. 1 para. 2 lit. b lit. i ODD) or that relates to activities directly exposed to competition (Art. 1 para. 2 lit. b lit. ii ODD). This provision effectively excludes companies that operate entirely within free market mechanisms from the Directive's scope.

If the data of public undertakings falls within the ODD's scope, the principle of unrestricted data use does not apply unconditionally (Art. 3 para. 2 ODD). Instead, it depends on the degree to which Member States permit this in their implementing legislation. For example, in Germany, public undertakings can independently decide whether to authorise data re-use. However, if they do permit re-use, the ODD's provisions apply. It is generally reasonable to interpret the publication of data as a re-use authorisation, provided that the data are not accompanied by a license restricting further use. Public undertakings, nonetheless, may charge fees for their data (Art. 6 para. 2 lit. c ODD), with total costs calculated based on

25 The term "cross-subsidisation" refers to "the full or partial transfer of costs incurred in one geographic or product market to another geographic or product market within a company or between parent companies and subsidiaries", as defined by the EC (1998) in its Notice on the application of competition rules to the postal sector and on the assessment of certain State measures relating to postal services.

objective, transparent, and verifiable criteria set by Member States (Art. 6 para. 4 ODD). Additionally, public undertakings are exempt from the prohibition on cross-subsidisation, considering their position in the market.

4.2 Social sciences as a recipient

While the social sciences greatly benefit from the ODD, it is important to remember that their data is often publicly funded. The EU legislator addresses this through a specific regime for research data, of which social scientists should take note. Since 2019, the ODD has included publicly funded research data in its scope through Art. 10 ODD, setting conditions for its re-use – though it does not regulate access to the data itself. The goal is to make the rapidly expanding volume of research data accessible across sectors and disciplines, enabling it to be pooled, re-used, and applied to efficiently and holistically address societal challenges (Recital 27 ODD).

4.2.1 Dividing lines within Art. 10 ODD

The central regulation on research data comprises two distinct regulatory mechanisms. First, Art. 10 ODD introduces a general, non-enforceable political obligation for Member States. They shall support the availability of research data by adopting national policies and relevant actions aimed at making publicly funded research data openly available (i.e., open access policies). These policies should adhere to the principle of "open by default" and align with the FAIR principles (Art. 10 para. 1 ODD).[26]

In contrast, Art. 10 para. 2 ODD establishes specific, substantive conditions for the re-use of publicly funded research data, which Member States are required to implement (Klünker and Richter, 2022, p. 10). According to this provision, research data "shall be re-usable for commercial or non-commercial purposes […], insofar as they are publicly funded and

26 FAIR is an acronym representing principles for research data, which should be *findable*, *accessible*, *interoperable*, and *re-usable*. These principles were proposed in 2016 by a group of stakeholders from academia, scientific publishers, funding organisations, and industry (Wilkinson et al, 2016, pp. 1 et seqq.). Additionally, the principle of "as open as possible, as closed as necessary" applies, where data "closeness" addresses considerations related to intellectual property rights, personal data protection, confidentiality, security, and legitimate business interests. This creates a tension with open data principles, which advocate unrestricted openness.

researchers, research performing organisations or research funding organisations have already made them publicly available through an institutional or subject-based repository".

4.2.2 Research data

The ODD specifically addresses research data rather than scientific publications, defining the former as "documents in a digital form, other than scientific publications, which are collected or produced in the course of scientific research activities and are used as evidence in the research process, or are commonly accepted in the research community as necessary to validate research findings and results" (Art. 2(9) ODD). Examples include statistics, test results, measurements, field observations, survey data, interview records, and images, as well as metadata, specifications, and other digital objects (Recital 27 ODD).

4.2.3 Covered data

It is worth re-emphasising that the ODD only governs the re-use of accessible data – access and proactive allocation are primarily determined by the practices of research institutions and research funders.[27] For re-use to apply, the data must already be publicly available in an institutional or subject-based repository (Art. 10 para. 2 ODD).[28] Repositories are document servers on which files can be archived and generally made accessible free of charge. Researchers' choice of repository for publishing datasets often depends on discipline-specific publishing norms and the publication requirements of leading journals (Zimmermann, 2021, p. 87).[29] One of the best known in social sciences is the SSRN (Social Science Research Network).

27 As long as the EU is not involved in funding research, it cannot give Member States any binding guidelines for their policies. The EU's most important document is therefore only a non-binding recommendation: Commission Recommendation (EU) 2018/790; Richter, 2023a, Recital 169).

28 The basis on which this is done, whether voluntary, contractual, or statutory, is irrelevant. Public access for a fee or access after registration is also covered.

29 The ODD also allows Member States to extend the scope of application to research data that have been made publicly accessible in other ways (Recital 28) (see Gobbato, 2020, p. 152).

The data – not the researcher or institution – must be publicly funded for the ODD to apply (Art. 10 para. 2 ODD). As long as the research data are publicly funded, it is irrelevant who produces them. Consequently, Art. 10 ODD also applies, by exception, to entities that are not public bodies or public undertakings, including private companies. The policy aim behind this is to return the economic potential of publicly funded research data to the public (Zimmermann, 2021, pp. 87-88).[30]

Given the broad definition of research data, a wide array of social science data may fall under the ODD's provisions. This includes both quantitative data (e.g., survey results, comparative studies, or longitudinal surveys) and qualitative data (e.g., interview transcripts, observation notes, or field diaries), provided that they are in digital form. However, the Directive's primary focus is likely on quantitative data, as it is typically organised and highly structured within a data matrix.[31]

In the social sciences, which focus on empirical and theoretical research into social behaviour – examining the conditions, processes, and consequences of human interactions – data often include personal information. If not anonymised, such data falls outside the ODD's scope (Art. 1 para. 2 lit. h, Art. 1 para. 4 ODD).

The scientific context in which data are generated is also critical. Scientific research is typically conducted in both applied and basic research settings, including universities, non-university research institutions, academies of science, departmental research within Member States, and companies (Zimmermann, 2021, p. 87).

Moreover, the data must serve an evidentiary role within the research process and assist in validating the research findings and results. The research community is responsible for defining the criteria here, enabling the ODD to create a flexible, transdisciplinary framework. The evidentiary function arises from the research design and chosen methodology in relation to the research subject, as the data directly contribute to the research process. The validation function focuses not on successful validation, but

30 While the directive defines "research data", it does not attempt to clarify the term "research" itself. Similarly, there is no standardised concept of research or science in other EU law. Although the freedom of science is protected under Art. 13 of the EU Charter of Fundamental Rights, the European Court of Justice has yet to provide any interpretation or guidance on this term.

31 It should also be noted that the term "document" does not extend to computer programs. However, Member States may extend the scope of this Directive to such programs (Recital 30 ODD).

rather on the established practices of the relevant research community. The key is whether, objectively speaking, the data are generally seen as necessary to validate the research findings. In essence, the data must generally serve a validation purpose.

4.2.4 Exclusion: scientific publications

The key distinction between research data under the ODD and other data lies in whether they constitute a scientific publication. The Directive explicitly excludes scientific publications from its definition of research data, distinguishing research data from "scientific articles reporting and commenting on findings resulting from their scientific research" (Recital 27 ODD). Research data has a preparatory and supporting role, meaning that scientific full-text articles, especially those in academic journals, are outside the Directive's scope (Gobbato, 2020, p. 152).

This exclusion primarily serves to ensure flexibility and preserve "individual research measures" (European Commission, 2018b, p. 38 et seq.; Klünker and Richter, 2022, p. 12). It allows researchers to retain flexibility over their publications, reflecting the fundamental right of academic freedom (Richter, 2018, p. 56). Scientific publications are also excluded due to copyright; such publications are works where third parties, such as publishers, may hold copyrights (Klünker and Richter, 2022, p. 12).[32] However, this exclusion does not address researchers' own intellectual property rights.[33]

5. Overall assessment of the Open Data Directive

The history of the ODD reflects a steady trend in European legislation towards greater openness of government data. The latest iteration has addressed key gaps in government data openness by updating normative requirements to align with technological advancements and expanding its scope to cover public undertakings and research data. Yet, the Directive's primary structural limitation persists: data re-use is only possible when access has already been granted.

To date, the European legislator has only managed to close this gap with regard to HVDs, for which it not only stipulates a particularly user-friend-

32 "Third party" refers to any natural or legal person other than a public sector body or a public undertaking that holds the data (Art. 2(17) ODD).

33 Argumentum e contrario Art. 1 para. 2 lit. c ODD.

ly regime for its re-use, but these datasets must also be made available independently of any national access restrictions. However, to ensure that high-value data genuinely contribute to greater openness, additional implementing acts by the Commission are essential.

From the perspective of social science, the new Directive proves to be more of an opportunity than a burden. Like any data-based science, social science benefits from the wider availability of high-quality data in order to establish a vital scientific system. The Directive aligns with the spirit of Open Science, a growing movement advocating for the broad sharing of research evidence and results without financial barriers. This vision rests on the principles proposed by Robert Merton, who championed this concept of "scientific communism" in the mid-20th century (1985, p. 86).

The hope remains that this spirit will also find its way into the offices and management floors of public companies. Progress in government data openness would be far swifter if driven by intrinsic commitment rather than regulatory obligation.

References

Aichholzer, G. and Burkert, H. (eds.) (2004) *Public sector information in the digital age*. Cheltenham: Edward Elgar.

Augsberg, I. (2016) 'Informationszugang und -weiterverwendung als gesellschaftliche Grundprinzipien' in Dreier, T. et al. (eds.) *Informationen der öffentlichen Hand - Zugang und Nutzung*. Baden-Baden: Nomos, pp. 37–58.

Berners-Lee, T. (1989, 1990) Information Management: A Proposal [Online]. Available at: https://cds.cern.ch/record/369245/files/dd-89-001.pdf (Accessed: 30 January 2025).

Beyer-Katzenberger, M. (2014) 'Rechtsfragen des "Open Government Data": Aktuelle Entwicklungen und Rechtsprechung zur Weiterverwendung von Informationen des Staates', *DÖV*, (4), pp. 144–151.

Borgesius, F.Z., van Eechoud, M. and Gray, J. (2015) 'Open data, privacy, and fair information principles: towards a balancing framework', *Berkeley Technology Law Journal*, 30(3), pp. 2073–2131.

Bruns, L., Mack, L., Klessmann, J. et al (2020) *Hochwertige Datensätze in Deutschland: Studie im Auftrag des Bundesministeriums für Wirtschaft und Energie*. Berlin.

'Commission Recommendation (EU) 2018/790 of 25 April 2018 on access to and preservation of scientific information C/2018/2375' (2018) *Official Journal* L 134, 31 May, pp. 12–18 [Online]. Available at: http://data.europa.eu/eli/reco/2018/790/oj (Accessed: 10 February 2025).

Deloitte and European Commission (2018) *Study to support the review of Directive 2003/98/EC on the re-use of public sector information*. Luxembourg.

Deloitte and European Commission (2020) *Impact assessment study on the list of high value datasets to be made available by the Member States under the Open Data Directive*. Luxembourg.

'Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information' (2003) *Official Journal* L 345, 31 December, pp. 90-96 [Online]. Available at: http://data.europa.eu/eli/dir/2003/98/oj (Accessed: 29 January 2025).

'Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information Text with EEA relevance' (2013) *Official Journal* L 175, 27 June, pp. 1–8 [Online]. Available at: http://data.europa.eu/eli/dir/2013/37/oj (Accessed: 30 January 2025).

'Directive (EU) 2019/1024 of the European Parliament and of the Council of 20 June 2019 on Open Data and the re-use of public sector information (recast) PE/28/2019/REV/1' (2019) *Official Journal* L 172, 26 June, pp. 56-83 [Online]. Available at: http://data.europa.eu/eli/dir/2019/1024/oj (Accessed: 29 January 2025).

Drexl, J. (2014) 'The competition dimension of the European Regulation of Public Sector Information and the concept of an undertaking'. *SSRN* [Online]. Available at: https://ssrn.com/abstract=2397018 (Accessed: 30 January 2025). Etalab (no date) *Licence Ouverte / Open Licence* [Online]. Available at: https://etalab.gouv.fr/licence-ouverte-open-licence/ (Accessed: 30 January 2025).

European Commission (2000) *eEurope 2002 – an information society for all*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2000:0330:FIN:EN:PDF (Accessed: 30 January 2025).

European Commission (2014) *Commission notice - Guidelines on recommended standard licences, datasets and charging for the reuse of documents*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014XC0724%2801%29 (Accessed: 30 January 2025).

European Commission (2018a) *Proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=SWD%3A2018%3A145%3AFIN (Accessed: 30 January 2025).

European Commission (2018b) *Commission staff working document impact assessment, proposal for a Directive of the European Parliament and of the Council on the re-use of public sector information*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52018SC0117 (Accessed: 30 January 2025).

Fia, T. (2021) 'An alternative to data ownership: managing access to non-personal data through the commons', *GJ*, 21(1), pp. 181–210.

Filippi, P. de and Maurel, L. (2015) 'The paradoxes of open data and how to get rid of it? Analysing the interplay between open data and Sui-Generis rights on databases', *International Journal of Law and Information Technology*, 23(1), pp. 1–22.

Geiger, C.P. and Von Lucke, J. (2012) 'Open government and (linked) (open) (government) (data)', *JeDEM - EJournal of EDemocracy and Open Government*, 4(2), pp. 265–278.

Gobbato, S. (2020) 'Open science and the reuse of publicly funded research data in the new Directive (EU) 2019/1024', *JELT*, 2(2), pp. 145–161.

GovData (2016) *Datenlizenz Deutschland* [Online] Available at: https://www.govdata.de/informationen/lizenzen (Accessed: 30 January 2025).

Graux, H. (2023) *Licence compatibility in Europe: a winding road to creative commons: a short exploration of legal issues, current trends and the practical reality for data providers and re-users in Europe*. Luxemburg: Publications Office of the European Union.

Gray, J. (2014) *Towards a genealogy of open data: General Conference of the European Consortium for Political Research in Glasgow, 3-6th September 2014*. London.

Helmreich, S. (2011) 'From spaceship earth to google ocean: planetary icons, indexes, and infrastructures', *Social Research*, 78(4), pp. 1211–1242.

Henninger, M. (2013) 'The value and challenges of public sector information', *Cosmopolitan Civil Societies Journal*, 5(3), pp. 75–95.

'Commission Implementing Regulation (EU) 2023/138 of 21 December 2022 laying down a list of specific high-value datasets and the arrangements for their publication and re-use (Text with EEA relevance)' (2023) *Official Journal* L 19, 20 January, pp. 43–75 [Online] Available at: http://data.europa.eu/eli/reg_impl/2023/138/oj (Accessed: 30 January 2025)

Kitchin, R. (2014) *The data revolution*. Thousand Oaks: Sage Publications Ltd.

Klünker, I. and Richter, H. (2022) 'Digital sequence information between benefit-sharing and open data', *Journal of Law and the Biosciences*, 9(2), pp. 1–29.

Lederer, B. (2015) *Open data: Informationsöffentlichkeit unter dem Grundgesetz*. Berlin: Duncker & Humblot.

Lundqvist, B., Forsberg, Y., de Vries, M. and Maggiolino, M. (2015) 'Open data and competition law some issues regarding access and pricing of raw data', *Masaryk University Journal of Law and Technology*, 9(2), pp. 95–120.

Martini, M., Haußecker, D. and Wagner, D. (2022) 'Das Datennutzungsgesetz als digitalpolitischer Ordnungsrahmen für die Monetarisierung kommunaler Daten', *NVwZ-Extra*, 41(11), pp. 1–12.

Mayernik, M.S. (2017) 'Open data: accountability and transparency', *Big Data & Society*, 4(2), pp. 1–5.

Merton, R.K. (1985) 'Die normative Struktur der Wissenschaft. Aufsätze zur Wissenschaftssoziologie' in Merton, R.K. (ed.) *Entwicklung und Wandel von Forschungsinteressen: Aufsätze zur Wissenschaftssoziologie: Mit einer Einleitung von Nico Stehr*. Frankfurt am Main: Suhrkamp, pp. 86–99.

Obama, B. (2009a) *Open government directive: memorandum for the heads of executive departments and agencies*. National Archives [Online]. Available at: https://obamawhitehouse.archives.gov/open/documents/open-government-directive (Accessed: 31 October 2024).

Obama, B. (2009b) *Transparency and open government: memorandum for the heads of executive departments and agencies*. National Archives [Online]. Available at: https://obamawhitehouse.archives.gov/the-press-office/transparency-and-open-government (Accessed: 31 October 2024).

ODC (no date) ODC Principles [Online]. Available at: https://opendatacharter.org/principles/ (Accessed: 30 January 2025).

Open Data Institute (2020) *Tool. The Data Spectrum* [Online] Available at: https://theodi.org/insights/tools/the-data-spectrum/ (Accessed: 30 Jnauary 2025).

Podszun, R. (2016) 'Die Marktordnung für Public Sector Information: Plädoyer für eine wettbewerbsorientierte Auslegung der Richtlinie' in Dreier, T. et al. (eds.) *Informationen der öffentlichen Hand - Zugang und Nutzung.* Baden-Baden: Nomos, pp. 335–360.

Ramge, T. and Mayer-Schönberger, V. (2020) *Machtmaschinen: Warum Datenmonopole unsere Zukunft gefährden und wie wir sie brechen*. Hamburg: Murmann.

Richter, H. (2018) 'Open science and public sector information – reconsidering the exemption for educational and research establishments under the Directive on Re-use of Public Sector Information', *JIPITEC*, 9(1), pp. 51–74.

Richter, H. (2021) *Information als Infrastruktur*. Tübingen: Mohr Siebeck.

Richter, H. (2023a) '§ 2 DNG' in Richter, H. (ed.) *DNG: Datennutzungsgesetz.* München: C.H. Beck.

Richter, H. (2023b) '§ 4 DNG' in Richter, H. (ed.) *DNG: Datennutzungsgesetz.* München: C.H. Beck.

Richter, H. (2023c) '§ 5 DNG' in Richter, H. (ed.) *DNG: Datennutzungsgesetz.* München: C.H. Beck.

Richter, H. (2023d) 'Einl.' in Richter, H. (ed.) *DNG: Datennutzungsgesetz.* München: C.H. Beck.

Stieglitz, J.E., Orszag, P.R. and Orszag, J.M. (2000) *The role of government in a digital age*. Washington D. C.

'Treaty on the Functioning of the European Union' (2012) *Official Journal of the European Union* C326, pp. 47-390 [Online]. Available at: http://data.europa.eu/eli/treaty/tfeu_2012/oj (Accessed: 30 January 2025).

The Annotated 8 Principles of Open Government Data (no data) [Online] Available at: https://opengovdata.org/ (Accessed: 30 January 2025).

Vlaanderen (no date) *Licentie modellicentie-gratis-hergebruik/v1.0* [Online] Available at: https://data.vlaanderen.be/doc/licentie/modellicentie-gratis-hergebruik/v1.0 (Accessed: 30 January 2025).

Van Eechoud, M. (2016) 'Open data values: calculating and monitoring the benefits of public sector information re-use' in Dreier, T. et al. (eds.) *Informationen der öffentlichen Hand – Zugang und Nutzung.* Baden-Baden: Nomos, pp. 107–142.

Wiebe, A. and Ahnefeld, E. (2015) 'Zugang zu und Verwertung von Informationen der öffentlichen Hand – Teil II', *CR*, 31(3), pp. 199–208.

Wilkinson, M.D., Dumontier, M., Aalbersberg, I. J. J. et al (2016) 'The FAIR Guiding Principles for scientific data management and stewardship', *Scientific Data*, 3, pp. 1–9.

W3C (2013) *5 Star Linked Data* [Online]. Available at: https://www.w3.org/2011/gld/wiki/5_Star_Linked_Data (Accessed: 30 January 2025).

Wirtz, H. (2014) 'Die Änderung der PSI-Richtlinie: Fort- oder Rückschritt?' *DuD*, 38(6), pp. 389–393.

Zech, H. (2015) 'Information as property', *JIPITEC*, 6, p. 192.

Zimmermann, J. (2021) 'Zum Potenzial des europäischen Weiterverwendungsrechts für die Erforschung der Biodiversität', *ZUR*, 32(2), pp. 84–92.

Internet of Things Data within the Context of the Data Act: Between Opportunities and Obstacles

Prisca von Hagen

Abstract

Chapter 2 of the Data Act regulates access to data generated during the use of Internet of Things products. It is the first major legislative push to regulate broad data access rights. This article provides an overview of the regulatory structure of data access under the Data Act, as well as an analysis of some of the essential issues. The Data Act establishes a three-party constellation between the "user", the "data holder", and third parties as "data recipients". The article describes the relationship between them and explains the rights and obligations of each party. The Data Act also interacts with other data regulation, such as the GDPR, which is discussed below. The European Commission aims to enable users to make a self-determined decision about access to the data they generate. This decision should lead to more data being made accessible. However, there are difficulties that need to be taken into account. These include, for instance, informing users about the modalities of their data access. Past discussions about the possible need for data ownership had been halted prior to the Data Act. With the new legislation, questions about its role in creating ownership-like position through the back door picked up this topic again. Therefore, this article outlines the discussion on whether the provisions in the Data Act possibly enable such a position and how the control over the data is actually distributed.

1. Introduction

The Data Act (DA, Regulation 2023/2854) came into force in January 2024 after a 2-year legislative process. Following a transition period, it will take effect in September 2025. Among other regulatory areas, it details data access rights that are aimed at enabling users of Internet of Things (IoT) products (i.e. products that are connected to the internet and work together as a network) to access the data they generate more easily. This marks the

first introduction of such broad data access rights. The access is intended to enable more extensive data usage. However, the DA's regulations also create obstacles that may undermine its goals. The purpose of this chapter is to present the regulatory content of the final draft and to summarise the most important points of discussion, which could also hinder the effectiveness of the DA.

2. The concept of the DA

European legislators are confronted with the issue of data not being fully used within the European internal market. According to the European Commission (2022a), 80% of industrial data remain unexploited. The lack of data use is a complex problem for many reasons and one that has multi-dimensional effects. Therefore, it requires a range of solutions to tackle the problem, of which the DA is one part.

2.1 Reasons for the lack of data sharing

Thus far, individual large companies have generally had de facto control over data. Manufacturers of IoT products, for instance, can design them so that only they can access the data (Kerber, 2022, p. 4; Eckard and Kerber, 2024, p. 120). There has also been a lack of relevant regulation that would incentivise or oblige companies to share data. Although there are, at least, regulations governing the requirements for processing personal data, this has not thus far been the case for non-personal data (Eckard and Kerber, 2024, p. 115).

The European Commission (2020) has also identified various reasons for the lack of data sharing. Competitive pressure between companies incentivises competitors not to cede any economic advantages (European Commission, 2020, p. 8). In addition, there is uncertainty as to whether the contractual partner who gets access to the data will use it in accordance with the contract (European Commission, 2020, pp. 8–9).

2.2 Effects of the lack of data sharing

The problems caused by the lack of sharing of IoT data can be divided into two categories (Kerber, 2022, p. 4). First, the users of IoT products cannot,

themselves, utilize the data, which raises a question of fairness. Although the users generate the data by using their IoT products (recital 6 DA), the manufacturers benefit from the users' data through data-driven business models (Podszun and Pfeifer, 2022, p. 953). However, the user may have an economic interest in offering the data on the data market themselves, or at least in participating in the profits generated by their data (Podszun and Pfeifer, 2022, p. 953).

Second, the lack of data sharing prevents third parties from using the data. This hinders the emergence of secondary markets, such as repair services (Kerber, 2022, p. 5; Podszun and Pfeifer, 2022, p. 953). Meanwhile, being the sole party that holds the data, puts individual market participants in a much better position (European Commission, 2020, p. 9): They can unilaterally determine the conditions of data transfer, and have an innovation advantage (European Commission, 2020, p. 8). Overall, this means that potential value-creation opportunities are missed (Kerber, 2022, p. 5).

2.3 Approaches of the European legislator

The European Commission (2020) has recognised these issues and tackled them with the development of the European Data Strategy. The European Data Strategy is intended to supplement measures such as the introduction of the General Data Protection Regulation (GDPR, Regulation 2016/679)[1] to establish a trusting and functioning European data space. Building on the Data Strategy, the European legislator first introduced the Data Governance Act (DGA, Regulation 2022/868)[2], which regulates the infrastructure required to share data. The introduction of the DGA was subsequently followed by the DA.

2.3.1 The European Data Strategy

The European Data Strategy aims to make personal and non-personal data more usable (European Commission, 2020, pp. 4–5). The strategy is intended to secure economic and social welfare within the European Union

1 For more information on the GDPR, see Chapter 14 'EU data protection law in action: introducing the GDPR' by Julia Krämer.

2 For more information on the DGA, see Chapter 11 'The Data Governance Act – Is "trust" the key for incentivising data sharing?' by Lucie Antoine.

(European Commission, 2020, p. 4). In addition to economic considerations, the European Commission (2020, p. 3) has also focused on using the data for general welfare purposes, such as tackling climate change.

According to the European Commission (2020, p. 4), standardised data regulations are important to the creation of a single market for data.

The European Data Strategy contains four pillars outlining specific measures (European Commission, 2020, p. 11). The first and the third pillars of the strategy form the basis for the regulation of IoT data. In the first pillar, the European Commission (2020) has stated that they would like to develop a horizontal legal framework, covering all sectors, for the use of and access to data. They also announced that they want to regulate data governance (European Commission, 2020, pp. 8–9), which was implemented shortly afterwards through the DGA and the regulations on data intermediation services introduced therein. Data intermediation services can be helpful in ensuring the use of data, for example by establishing contact between parties and helping to anonymize the data (cf. recital 26 DA). In this pillar, the European Commission (2020, pp. 7–8) has also anchored the idea of adopting a Data Act that promotes the sharing of data in business-to-government (B2G) and business-to-business (B2B) relationships. The measures of the third pillar furthermore aim to strengthen individuals' control over their data in the future (European Commission, 2020, pp. 20 ff.). The European Commission (2020, p. 20) notes in the first pillar that increased control can be achieved through the DA.

In addition to the horizontal regulations that apply across all sectors, within the fourth pillar, vertical regulations that focus on access to data directly in relation to nine sectors already identified (e.g. the health data space or the mobility data space) are also considered (European Commission, 2020, pp. 21 ff.).

2.3.2 Basic idea of the DA with regard to IoT data

The second chapter of the DA aims to ensure that more data generated by IoT products are made accessible. The users of IoT products, who can be both natural persons and legal entities such as companies, are granted sovereignty over the data generated by their use (recital 15, 18 DA; Kerber, 2022, p. 5). The DA enables users to access the data, use it for lawful purposes (recital 30 DA) and permits third parties to use it at the user's request. The DA is the first legislation to regulate non-personal data (Eckard and Kerber, 2024, p. 114). The European Commission (cf. 2017, p. 13) has

already considered the question of whether those involved in the generation of the data should also decide what happens to it. It is based on the idea that it is only fair if those who are actively involved in the production have access to and can use the data (recital 6 DA; Kerber, 2022, p. 5).

This general allocation of access rights to IoT data is intended to make more data available and stimulate the data economy (recital 6 DA). It is assumed that users have "data literacy", which enables them to assess the value of their data and thus motivates them to make it available to third parties as well (recital 19 DA; Kerber, 2022, p. 5). The DA aims to further promote this data expertise (recital 19 DA). The granting of usage options to third parties includes support for secondary services (e.g. repairs and maintenance) and the development of innovative business models (cf. recital 19 DA).

It is noteworthy that the European legislator is not merely aiming to compensate for a market failure but to completely restructure the data market (Metzger and Schweizer, 2023, pp. 49 ff.; Hennemann and Steinrötter, 2024, p. 6). The regulation intends to break up larger companies' "gatekeeper" position (cf. recital 40 DA; Metzger and Schweizer, 2023, pp. 47, 49) and plans to redesign the market by offering incentives to users (Hennemann and Steinrötter, 2024, p. 6).

The regulations regarding IoT data will be added by an unfairness test for data usage agreements and other contracts related to data between two enterprises in Article 13 DA.

In addition to chapter 2, the DA includes other areas, such as data access in the G2B relationship in chapter 5, and requirements for the interoperability of data processing services, such as cloud providers in chapter 8.

3. The design of the IoT data access

3.1 Scope of application: what data are covered?

The right of access relates to personal and non-personal data from IoT products, which include smart household appliances (e.g. a networked refrigerator) as well as "smart agricultural and industrial machinery" (cf. recital 14 DA).

According to Articles 3 (1) and 4 (1) DA, the right to access includes the product data, the associated service data and the metadata required for its use. The term product data refers to information generated by using the IoT

product (recital 15, Art. 2 No. 16 DA). Data generation during use means that data are generated directly while the product is being actively used. Data access includes data generated indirectly through use (e.g. data related to the environment; recital 15 DA). Data that are merely a consequence of use are also expressly included (recital 15 DA). For example, the access claim also relates to data automatically generated by sensors and recorded in the background (recital 15 DA). In this respect, it is irrelevant if the data are generated when the product is inactive, for instance, while in stand-by mode (recital 15 DA).

The access rights also relate to connected service data (Art. 2 No. 6 DA). Connected service data are generated during the provision of a digital service, such as software (cf. Art. 2 No. 6 DA) necessary for the operation of the product connected to the IoT product (recital 15 DA). Furthermore, the data do not necessarily have to be modified to be covered by the scope of the DA, meaning that raw data are also included (recital 15 DA).

Metadata as additional data is important for understanding and using the generated data. Examples of metadata include timestamps, which are required to place the data in correct relation to one another (recital 15 DA).

However, if the data holder makes significant investments in analysing the data to gain further insights, this derived information is no longer part of the scope of application (recital 15 DA).

3.2 Relevant actors

The DA constructs a three-party constellation between the "user", the "data holder", and third parties as "data recipients".

As noted above, the user can be a natural person or a legal entity, such as a company (Art. 2 No. 12 DA). The decisive factor is the user's ownership of the corresponding product or at least the right for temporary use (Art. 2 No. 12 DA). Included are, for example, farmers who lease smart tractors that they need for work (Specht-Riemenschneider, 2022b, p. 813).

Data holders, who most often are the manufacturers of smart products (Specht-Riemenschneider, 2022b, p. 813), are obliged to share the data (cf. recital 5 DA). The key factor is their de facto control over the data generated (Specht-Riemenschneider, 2022b, p. 813). Data holders are obliged to retain the data for a reasonable period (recital 24, DA), and as soon as they delete the data, they lose their status as data holders. (Bomhard and Merkle, 2022, pp. 173–174).

Finally, data recipients are companies or natural persons to whom the data are made available by the data holders, despite the fact that they are not product users (Art. 2 No. 14 DA). For example, companies needing the data to repair a product are considered to be data recipients (cf. recital 32 DA).

3.3 Data access of the various actors

Whereas in the past only the data holders had de facto control over (non-personal) data, a concept has now been introduced that gives the user access to the data. However, through contractual agreements with the user, the data holders can also continue to use the data (Art. 4 (13), (14) DA). The data holder is obliged to make the data available to third parties at the request of the user (Art. 5 (1) DA).

3.3.1 Data access of the user

Users should be given the power to make decisions regarding their data (cf. Podszun and Pfeifer, 2022, p. 956). Without a contractual agreement between the two parties, access to the data, in the past, depended on who had de facto access to it prior to the DA (Etzkorn, 2024, p. 118).

According to the DA (Art. 2 (2), (3) DA), the data holder must provide the user with the information necessary to gain access to their data before concluding the purchase, rental or lease agreement for the IoT product. For example, information should be provided regarding what data are generated through use, in what format they can be retrieved and how the user can gain access. It is also important that the information can be recalled not only prior to the conclusion of the contract but also later (recital 24 DA).

Data holders should consider the direct accessibility of the data already during the design process (Art. 3 (1) DA). Accessibility can be ensured, for example, via a user interface (Specht-Riemenschneider, 2022b, p. 815). If this "accessibility by design" is not possible, the user has the right under Article 4 (1) DA to have the data made accessible to them in another. It is unclear whether a so-called in situ right, which would permit the user to view the data only on the data holders' server, is sufficient (cf. Specht-Riemenschneider, 2022b, p. 816; Kerber, 2022, p. 9; Hennemann and Steinrötter, 2024, p. 3). Regardless of the form of provision, the data holder must grant access to the data free of charge (Art. 3 (1), 4 (1) DA).

Only microenterprises or small enterprises are exempt from this obligation (Art. 7 (1) DA), as the effort involved would be unreasonably high (cf. recital 41). However, the data may contain trade secrets. In this case, the user must take appropriate measures to ensure their protection (Art. 4 (6) DA).

Subsequently, the user can "use the data for any lawful purpose" (recital 30 DA), which includes commercial use (Efroni et al., 2022, p. 10; Etzkorn, 2024, pp. 120–121). However, the user is prohibited from using the data to develop a competing product (Art. 4 (10) DA).

If the product is used by multiple users (e.g. in the case of several owners) all must be given access to the generated data (recital 21 DA). In practice, this can be realised by providing the option of setting up several user accounts through which each user can access the data (recital 21 DA). If the product is resold, the data holder must provide an option for each user to delete the previously generated data (recital 21 DA).

3.3.2 Data access for data recipients

The user can decide whether the data should be shared with third parties. According to Article 5 (1) DA, the data holder must provide the data to the data recipient at the user's request in the "same quality as it is available to" them. Microenterprises or small enterprises are also excluded from this obligation under Article 7 (1) DA. The data recipient may only use the data for the purposes to which it has contractually agreed with the user. Moreover, they must adhere to further conditions, such as the protection of the data holder's trade secrets (Art. 6 (1), (2) DA). These additional conditions are intended to take into account the conflicting interests of data holders and data recipients (Etzkorn, 2024, p. 121).

Data intermediation services that can support the appropriate fulfilment of data access requests are also explicitly envisaged as potential data recipients (recital 26 DA). The consideration of intermediaries creates a close link with the DGA, which is intended to establish the appropriate infrastructure.

In contrast to the user's free access, the data recipient has a duty to compensate the data holder for the use of the data (Art. 9 (1) DA). The compensation must be "reasonable" and should ensure that data holders are incentivised to generate data (Podszun and Pfeifer, 2022, p. 957). However, it is difficult to determine when a compensation payment is reasonable (Podszun and Pfeifer, 2022, p. 957). It must be determined in each individual case whether the conditions fulfil these requirements. If the

data recipient is a small or medium enterprise or a not-for-profit research organisation, the compensation under Article 9 (4), (2) (a) DA is limited to the costs of provision.

Moreover, gatekeepers within the meaning of Article 5 (3) DA are expressly excluded from data access, as the power of gatekeepers is explicitly intended to be undermined and not manifested through further data access (cf. recital 40 DA).

3.3.3 Restrictions for the use by the data holder

Although data holders maintain de facto access to the data, they are only permitted to use it under Article 4 (13) DA if they have contractually agreed to this with the user. In practice, however, an agreement on the use of the data by the data holder will be made a condition for the purchase, rental or lease agreement (Bomhard and Merkle, 2022, p. 174; Kerber, 2022, pp. 22–23).

It is unclear whether this contract between the data holder and the user can also include a general agreement on the commercial use on the part of the data holder by passing it on to third parties (Hennemann and Steinrötter, 2024, p. 7). In any case, it is only possible within the meaning of Article 4 (14) DA if the commercial disclosure of non-personal data is for "the fulfilment of their contract with the user" (cf. Hennemann and Steinrötter, 2024, p. 7). This stipulation indicates that disclosure to third parties is subject to the narrow limits of the contract signed with the user (Hennemann and Steinrötter, 2024, p. 7). Meanwhile, the processing of personal data continues to be subject to the requirements of the GDPR. According to this, the explicit purpose of the data processing must be clear (Art. 5 (1) (b) GDPR).

4. Problematic aspects

The DA has generated significant interest both in legal studies and practice. It has raised many open questions as well as points of friction, of which the following are among the most important. This presentation, however, is not exhaustive.

4.1 Relationship of the DA to other legal regulations

A central topic of contention throughout the legislative process was the relationship with other legal regimes. For example, as the DA also regulates personal data already governed by data protection law, there are questions of demarcation with the GDPR. As manufacturers, in particular, are obliged to provide access, and the data may allow conclusions to be drawn about the functionality of products (Macher and Graf Ballestrem, 2023, p. 661), the protection of trade secrets plays a significant role. Not least, the DA complements existing digital legislation, such as the GDPR and the DGA.

4.1.1 Relationship to data protection law

The DA refers to personal and non-personal data generated during the use of IoT products. The term personal data refers to data that relate to a natural person and make it possible to identify that person (Art. 4 No. 1 GDPR). The use of IoT products easily leads to the generation of personal data, for example, when using a connected car (Steinrötter, 2023, p. 219). Data holders have an obligation to verify whether the data are personal before granting an access request (Heinzke, 2023, p. 205). In general, it is difficult for controllers to determine when the data can be used to establish a link to an individual from which their identity can be inferred. Data holders will also have problems, especially with large data sets, in drawing the line between personal and non-personal data (recital 34 DA; Bomhard and Merkle, 2022, pp. 172, 174–175; Heinzke, 2023, p. 205).

If the datasets contain personal data, the DA and GDPR apply in parallel in accordance with Article 1 (5) DA (cf. Specht-Riemenschneider, 2022b, p. 810). In case of conflicts between the legal provisions, the GDPR takes precedence pursuant to Article 1 (5) DA. According to Schmidt-Kessel (2024a), collisions should only occur rarely, as the two legal norms have different subject matters. Whereas the GDPR deals, in particular, with the right to use data, the DA contains contract law provisions (Schmidt-Kessel, 2024a, p. 127).

Nonetheless, in certain situations, the access claim causes problems that particularly concern the relationship between the GDPR and the DA (cf. Specht-Riemenschneider, 2023, pp. 664 ff.; Steinrötter, 2023, pp. 220 ff.). In addition, implementing the data access request might create data protection conflicts in some cases.

Legal Basis for Data Processing

According to the GDPR, the processing of personal data requires a legal basis, such as the data subject's consent. If the data are processed without such a legal basis, the data controller faces fines.

If the user requesting the data is the data subject within the meaning of the GDPR, the request for access to the data constitutes implied consent to data processing (Bomhard and Merkle, 2022, pp. 174–175; Specht-Riemenschneider, 2022b, p. 810).

A problem arises when the user and the data subject are not identical and the user requests access to the data for themselves or a third party (Steinrötter, 2023, p. 223; Specht-Riemenschneider, 2023, p. 665). This problem can occur, for example, if a farmer's tractor is operated by a subcontractor (cf. Zech, 2015a, p. 137). Concerning the first version of the DA, it has been discussed whether legal bases for data processing could arise from the DA itself in these cases (Specht-Riemenschneider, 2023, pp. 664 ff.; Steinrötter, 2023, p. 223). This would indicate that the data subject's consent is not required. This would benefit data holders, in particular, who would thereby make the personal data accessible on a legal basis and avoid claims for fines (Steinrötter, 2023, p. 223). However, this is rejected in the final version of the DA in recital 7 DA, which states, "[W]here the user is not the data subject, this Regulation does not create a legal basis for providing access to personal data or for making personal data available to a third party […]".

Relationship between the right to data portability and Article 4 (1) and Article 5 (1) DA

Since the introduction of the GDPR, data subjects have the right to receive their personal data in accordance with Article 20 (1) GDPR or to have them transmitted to others under Article 20 (2) GDPR. They also have the right to obtain a copy of the data processed by the controller in accordance with Article 15 (3) GDPR. Therefore, these provisions are similar to Article 4 (1) and Article 5 (1) DA, which provide the user and third parties with access to IoT data. The claims under the DA indeed have narrower provisions, such as that access must be "without undue delay" and "free of charge". In contrast, under the GDPR, the controller is given an extendable 1-month period within the meaning of Article 12 (2) GDPR and can demand a fee if the data subject exercises their right in an unreasonably excessive manner

(cf. Richter, 2022, p. 307; Steinrötter, 2023, p. 221). However, Article 1 (5) DA expressly stipulates that Articles 4, 5 DA "complement" Articles 15 and 20 GDPR. Therefore, it is positive that Article 4 (1) and Article 5 (1) DA include not only personal data but also non-personal data (cf. Steinrötter, 2023, p. 221).

Criticism of the creation of user accounts

There are data protection concerns, in particular, related to accessing data via user accounts. As described above, this procedure is intended to enable users to assert claims to data access (cf. recital 21 DA). This is important for verifying status as a user (Steinrötter, 2023, p. 222). The problem here, however, is that this creates a link between data and users, which can create a personal reference, even with data that were initially non-personal (Specht-Riemenschneider, 2023, pp. 663–664; Steinrötter, 2023, p. 222). Anonymous data access would probably have been possible, but this approach was not pursued further (Podszun and Pfeifer, 2022, p. 952).

4.1.2 Relationship to trade secret protection

The relationship between the DA and the protection of trade secrets was discussed extensively during the legislative period (cf. Hennemann and Steinrötter, 2024, pp. 3–4). The German Trade Secrets Protection Act (GeschGehG, 2019) protects trade secrets from unauthorised use, acquisition or disclosure in accordance with § 1 (1) GeschGehG. It is based on the Trade Secrets Directive. According to § 2 (1) GeschGehG, a trade secret is information that is not in public domain and that has economic value. In addition, the GeschGehG indicates that the person who knows the information must take steps to maintain secrecy.

Companies are concerned that their trade secrets will be jeopardised by the DA's access to data (Macher and Graf Ballestrem, 2023, p. 661). If information is made public, it is no longer secret, and it therefore loses its trade-secret characteristic (cf. Metzger and Schweizer, 2023, pp. 74–75). However, the data holders could use the trade secret protection argument to (unjustifiably) deny access to the data. (Macher and Graf Ballestrem, 2023, p. 661).

Data as trade secret

However, it is difficult to determine whether data are trade secrets at all (Heinzke, 2023, pp. 205–206; Grapentin, 2023, p. 174). Data must have semantic information value to be categorised as information within the meaning of the GeschGehG (cf. Zech, 2015b, p. 1156; Wiebe, 2023, p. 232; Heinzke, 2023, pp. 205–206). Therefore, there are discussions regarding the trade-secret characteristic of raw data, in particular. In part, raw data do not qualify as a trade secret because they contain no substantive information (European Commission, 2022b, p. 89). This view disregards the fact that raw data, in connection with other data, can have substantive value and can thus be protected as a trade secret (Grapentin, 2023, p. 174; Lorenzen, 2022, p. 253; Wiebe, 2023, p. 232). If, for example, raw data from CT or MRI devices (e.g. temperature and coil rotations of the machine) are linked, significant insights into the functioning of the machine can be derived (Grapentin, 2023, pp. 174–175). In addition, the commercial value, which may be very low for the individual raw data points, increases when linking these with other data (Zech, 2015b, p. 1156; Lorenzen, 2022, p. 253).

Ultimately, courts must decide whether raw data constitutes a trade secret (Metzger and Schweizer, 2023, p. 75). In the event that court proceedings are protracted, data holders could withhold the data for the duration of the proceedings (cf. Kerber, 2022, p. 12).

Approaches of the DA with regard to trade secrets

The protection of trade secrets was extensively revised between the first draft and final version of the DA (cf. Hennemann and Steinrötter 2024, pp. 3–4). Whereas trade secrets were initially only disclosed via data access in accordance with Article 4 (1) DA if the necessary measures were taken to ensure confidentiality, the hurdles for refusal are higher in the final version. Article 4 (8) DA now requires that the data holder prove that they would suffer serious economic damage if the data were to be disclosed. Accordingly, the data holder can only refuse access in individual cases. They must inform the user, in writing, of the refusal and the reasoning for it, and they must notify the competent authority. Even if the conditions for refusing access to data are now stricter, the data holder is still able to use trade secret protection against the user's claim (cf. Hennemann and Steinrötter, 2024, p. 4).

4.1.3 Relationship to database protection

Finally, the relationship between the existing database protection and the provisions of the DA is unclear. Under the Database Directive (Directive 96/9/EC), the extraction or re-utilisation of databases can be prohibited in accordance with Article 7 (1). Database protection is intended to guard the essential investments necessary to create the database (recital 40 Database Directive).

However, Article 7 of the Database Directive does not apply to the data access claims of Articles 4 (1) and 5 (1) DA, according to Article 43 DA. This indicates that the data holder is not entitled to refuse access to the data on the grounds of database rights (cf. Kim, 2024, pp. 87–88; Hennemann and Steinrötter, 2024, p. 6). Nevertheless, there is a controversy regarding the scope of application of the two legal regimes (cf. Kim, 2024, pp. 89–90). According to the DA, data should be prepared in a usable manner (recital 15 DA). If the data are the "outcome of additional investments", they are excluded from the scope of the DA (recital 15 DA). However, creating a database requires a substantial investment in accordance with Article 7 of the Database Directive. The standard is therefore in need of clarification (Kim, 2024).

4.1.4 Relationship to other existing legal instruments

The Digital Markets Act (DMA, Regulation 2022/1925) and the DGA are supplemented by the DA (cf. Specht-Riemenschneider, 2022b, p. 811). The DMA and DA, in particular, jointly pursue the goal of breaking up the accumulation of power by gatekeepers (recital 40 DA).

As noted above, the DGA establishes an infrastructure that intends to realise fairer data distribution, for example through registered or certified data intermediaries. Although the original draft focussed primarily on the promotion of secondary services (e.g. maintenance and repairs; cf. Efroni et al., 2022, p. 14), data intermediation services were included in the final version at various points and recognised as a central element in the distribution of data (cf. Art. 2 No. 10; recital 30 DA).

The European Health Data Space is currently in the legislative process and represents the first vertical regulation on access to data from the healthcare sector.

4.2 Independent decision by the user?

Another point of discussion is the extent to which the user can make independent decisions and whether the possibility of requesting access results in better data distribution. Alongside the data holder, the user is at the centre of the regulations on IoT products (Podszun and Pfeifer, 2022, p. 960). The users' decision to release the data for themselves or third parties should lead to a fairer distribution and thus to more innovation (Krämer, 2022, p. 5). This decision requires the user to be informed (Podszun and Pfeifer, 2022, pp. 960–961), as otherwise, the allocation of data value may be asymmetrical (Eckard and Kerber, 2024, pp. 128–129). However, there is a lack of information among users, particularly in B2C relationships (Kerber, 2022, p. 22). Consumers are, for instance, unaware of the value their data might generate (cf. Krämer, 2022, p. 20).

The DA introduces obligations to inform users that are intended to counteract the information asymmetry between users and data holders (cf. recital 24 DA). In addition, the contract with the data holder pursuant to Article 4 (13) DA, which is necessary for the data holder to be able to use the data, may provide users with further information such as the "envisaged uses by the IoT provider" (Leistner and Antoine, 2022, p. 92).

However, in the case of personal data, experience has already shown that data protection declarations are not read and understood in the majority of cases (Specht-Riemenschneider, 2022a, p. 139; Kerber, 2022, p. 22; Krämer, 2022, p. 9), due to the length and complexity of these texts, among other reasons (cf. Rakoff, 1983, p. 1226; Ben-Shahar, 2009, pp. 13–14). This is in keeping with observations made regarding contractual clauses (cf. Ben-Shahar, 2009, p. 1; Bakos, Marotta-Wurgler and Trossen, 2014, p. 1). For various reasons (e.g. rationality considerations), it may make sense not to read the conditions (Ben-Shahar, 2009, p. 14), when, for example, the cost of reading exceeds the expected benefits (Hillman and Rachlinski, 2002, p. 446).

The information problem is exacerbated by the fact that personal and non-personal data in datasets generated by IoT products are, as noted above, difficult to distinguish from one another (cf. Richter, 2022, p. 304; Bomhard and Merkle, 2022, p. 172). Therefore, it is to be expected that data holders will apply information requirements cumulatively to avoid legal consequences (Steinrötter, 2023, p. 219). In addition, the data holder may be required to comply with further information requirements, for example, under consumer contract law (Rammos and Wilken, 2022, p. 1243).

Therefore, the effectiveness of the information obligation is highly questionable, especially with regard to the B2C sector (cf. Heinzke, 2023, p. 208). In any case, it is closer to the assumption that the user does not perceive the information in this case, either, and that they conclude contracts with the data holders without dealing with the content (Hennemann and Steinrötter, 2022, p. 1483; Podszun and Pfeifer, 2022, pp. 960–961).

4.3 "Property right" of the user versus technical–factual control of the data holder

A much-discussed question throughout the legislative process was to whom the DA assigns rights and what the effects are on the power relations.

The extent to which "ownership" of data, in the form of a transferable exclusive right that protects the data in particular from unauthorised use, makes sense and can promote the data economy has already been discussed (cf. Dorner, 2014; Zech, 2015a; Drexl, 2017). The exclusive right of ownership means that the right holder has a legal defence against anyone (cf. Zech, 2015a, p. 140) – that is to say they also have the right to determine who uses the data, and they can assert claims in the event of unauthorised use. However, to whom this transferable, exclusive right should be assigned, given the multitude of parties involved, (e.g. manufacturers or users), is challenging (cf. Wiebe, 2016, p. 883; Drexl, 2017, p. 277). Data can contain information at the semantic level. An exclusive right of use can therefore prevent access to information and even lead to a monopolisation of information (Wiebe, 2016, pp. 881–882). Due to existing problems, the discussion was settled, and the focus has now shifted to data access rights (cf. Wiebe, 2023, p. 1569; Specht-Riemenschneider, 2022b, p. 810; Hennemann and Steinrötter, 2022, p. 148).

The implementation of exclusive rights to data was explicitly avoided when the DA was introduced (cf. recital 6 DA). However, whether the design of the DA results either in exclusive rights for the user (cf. Bomhard and Merkle, 2022, p. 175; Hennemann and Steinrötter, 2022, p. 148) or, conversely, establishes an exclusive position for data holders by strengthening their de facto control (cf. Kerber, 2022, pp. 15 ff.; Specht-Riemenschneider, 2022b, p. 818) is now being discussed.

4.3.1 "Ownership-like" position of the user?

According to the first approach, Article 4 (13) DA in particular, according to which the data holder may only use non-personal data on the basis of a contract concluded with the user, establishes an ownership-like position (cf. Bomhard and Merkle, 2022, p. 175). According to this argument, excluding the data holder if the user does not agree to a contract with them creates an exclusive position of the user that is akin to an absolute right (Bomhard and Merkle, 2022, p. 175; Hennemann and Steinrötter, 2022, p. 1483).

This is countered by the argument that the DA is only a reaction to the de facto control of data holders and does not aim to introduce a right similar to ownership, but merely to distribute data more fairly (cf. Metzger and Schweitzer, 2023, p. 50). The data are not directly assigned to the user. Rather, the user only has access to the data if they actively make use of their access rights (Specht-Riemenschneider, 2022b, p. 815).

The DA expressly prefers simple access rights to the granting of exclusive access and usage rights (recital 6 DA). In addition, the trilogue procedure of the European legislator included Article 4 (14) DA, which stipulates that third parties who obtain data from the data holders must be contractually obliged not to share it. However, this would not be necessary if an exclusive right of use had been established as a right similar to ownership (Schmidt-Kessel, 2024b, p. 78).

4.3.2 (Exclusive) de facto position of the data holder?

The previous argument against the establishment of users' ownership-like rights is also the argument for the contrary approach, which posits that the DA would result in (exclusive) de facto rule by the data holders (cf. Kerber, 2022, pp. 15 ff.; Specht-Riemenschneider, 2022b, p. 818). Whereas de facto control over the data was previously purely factual, the DA regards this as a given (Martens, 2023, p. 19). According to some scholars, this is even seen as a legal position equivalent to the holder of an IP right (cf. Eckard and Kerber, 2024, pp. 123–124; Kerber, 2022, p. 17). As explained above, de facto control over the data remains with the data holder (cf. Podszun and Pfeifer, 2022, p. 956).

The data holder is thus authorised to decide which data are collected (Specht-Riemenschneider, 2022a, p. 139). They can also delete the data at their discretion, provided they have complied with a reasonable storage period (cf. recital 24 DA). In addition, Article 11 (2) DA introduces safeguards

allowing data holders to require users and recipients to take various actions in case of unlawful use, such as deletion of the data provided (cf. Kerber, 2022, p. 16; Specht-Riemenschneider, 2022a, p. 137). The data holder can also comply with the user's request for access if the user can access the data on the data holder's server. In this case, the data would remain under the control of the data holder (Specht-Riemenschneider, 2022a, p. 139).

The use of non-personal data by the data holder pursuant to Article 4 (13) DA is only possible if the data holder and the user have concluded a corresponding contract. Such a contract would give the user some control. However, these contracts can be made a condition for the IoT product contract without restrictions (Specht-Riemenschneider, 2022a, p. 139).

5. Conclusion

With the intention of making more data usable and disrupting the gatekeeper position held by large companies, the European legislator is pursuing an important goal. However, the specific form of the legislation raises doubts about its effectiveness (cf. Kerber, 2022, p. 3; Specht-Riemenschneider, 2022b, p. 810; Wiebe, 2023, p. 1569; Heinzke, 2023, p. 208). Although positive changes have already been made in the course of the legislative process, both the structure of the parties involved, as established by the DA, and the individual provisions are subject to criticism.

Structurally, it is questionable whether the de facto position of the data holder is strengthened without strengthening the user. For example, tighter requirements for the contract in accordance with Article 4 (13) DA (Specht-Riemenschneider, 2022b, pp. 818–819), would accomplish the latter. The fact that the user's ability to make decisions is limited due to a lack of information, especially in a B2C relationship, will also reduce the benefits of the DA (cf. Eckard and Kerber, 2024, p. 128; Metzger and Schweizer, 2023, pp. 56–57).

Furthermore, legal uncertainty regarding individual provisions of the DA is challenging. If, for example, compensation is demanded for making data accessible to a data recipient in accordance with Article 9 (1) DA and the parties cannot reach an agreement, a lengthy process that delays data access might be initiated (cf. Podszun and Pfeifer, 2022, p. 957). Even in cases where it is necessary to determine whether the necessary measures have been taken to protect a trade secret, a court will have to decide (Metzger and Schweitzer, 2023, p. 75). Delay will be a particular concern if the data

must be made accessible to a third party who is a competitor of the data holder (Podszun and Pfeifer, 2022, p. 959).

Although the DA has been in force since the beginning of 2024, what is certain is that the practical benefits of this legislation – in particular its potential to stimulate the data market – will become apparent in September 2025, when it takes effect.

References

Bakos, Y., Marotta-Wurgler, F. and Trossen, D. R. (2014) 'Does Anyone Read the Fine Print? Consumer Attention to Standard Form Contracts', *Journal of Legal Studies,* 43(1), pp. 1–35.

Ben-Shahar, O. (2009) 'The Myth of the 'Opportunity to Read' in Contract Law', *European Review of Contact Law*, 5(1), pp. 1–28.

Bomhard, D. and Merkle, M. (2022) 'Der Entwurf eines EU Data Acts', *Recht Digital*, 2(4), pp. 168–176.

'Directive 96/9/EC of the European Parliament and of the Council of 11 March 1996 on the legal protection of databases' (1996) *Official Journal* L77, 27 March, pp. 20–28 [Online] Available at: http://data.europa.eu/eli/dir/1996/9/oj (Accessed: 30 January 2025).

Dorner, M. (2014) 'Big Data und „Dateneigentum"', *Computer und Recht*, 30(9), pp. 617–628.

Drexl, J. (2017) 'Designing Competitive Markets for Industrial Data', *Journal of Intellectual Property, Information Technology, and Electronic Commerce Law*, 8(4), pp. 257–292.

Eckard, M. and Kerber, W. (2024) 'Property rights theory, bundles of rights on IoT data, and the EU Data Act', *European Journal of Law and Economics*, 57(1–2), pp. 113–143.

Efroni, Z., von Hagen, P., Völzmann, L., Peter, R. and Sattorov, M. (2022) *Position Paper of the Weizenbaum Institute – Regarding Data Act* [Online]. Available at: https://www.weizenbaum-library.de/handle/id/125 (Accessed: 30 January 2025).

European Commission (2017) *Communication from the commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions 'Building a European data economy'* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52017DC0009 (Accessed: 30 January 2025).

European Commission (2020) *Communication from the Commission to the European Economic and Social Committee and the Committee of the Regions: A European strategy for data* [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52020DC0066 (Accessed: 30 January 2025).

European Commission (2022a) *Press release regarding the Data Act, 23.02.2022* [Online]. Available at: https://ec.europa.eu/commission/presscorner/detail/en/ip_22_1113 (Accessed: 30 January 2025).

European Commission (2022b) *Study on the legal protection of trade secrets in the context of the data economy (2022)* [Online]. Available at: https://beck-link.de/an8vn (Accessed: 30 January 2025).

Etzkorn, P. (2024) 'Datenzugangsansprüche nach dem Data Act', *Recht Digital*, 4(3), pp. 116–123.

'Gesetz zum Schutz von Geschäftsgeheimnissen vom 18. April 2019 (GeschGehG)' (2019) *Bundesgesetzblatt I 2019*, pp. 466-472.

Grapentin, S. (2023) 'Datenzugangsansprüche und Geschäftsgeheimnisse der Hersteller im Lichte des Data Act', *Recht Digital*, 3(4), pp. 173–182.

Heinzke, P. (2023) 'Data Act: Auf dem Weg zur europäischen Datenwirtschaft', *Betriebs Berater*, 2023(5), pp. 201–209.

Hennemann, M. and Steinrötter, B. (2022) 'Data Act – Fundament des neuen EU-Datenwirtschaftsrechts', *Neue Juristische Wochenschrift*, 75(21), pp. 1481–1485.

Hennemann, M. and Steinrötter, B. (2024) 'Der Data Act', *Neue Juristische Wochenschrift,* 77(1), pp. 1–8.

Hillmann, R. and Rachlinski, J. (2002) 'Standard-Form Contract in the Electronic Age', *N.Y.U. Law Review*, 77(2), pp. 429–495.

Kerber, W. (2022) 'Governance of IoT Data: Why the EU Data Act will not Fulfil its Objectives', *GRUR International Journal of European and International IP Law*, 72(2), pp. 120–135.

Kim, D. (2024) 'Der Datenbankschutz sui generis nach dem Data Act', *Multimedia und Recht*, 27(MMR-Beilage), pp. 87–91.

Krämer, J. (2022) *Improving the economic effectiveness of the B2B and B2C data sharing obligations in the proposed Data Act* [Online]. Available at: https://cerre.eu/wp-content/uploads/2022/11/ImproveEffectiveness_DataAct_Final.pdf (Accessed: 30 January 2025).

Leistner, M. and Antoine, L. (2022) *IPR and the use of open data and data sharing initiatives by public and private actors* [Online]. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2022/732266/IPOL_STU(2022)732266_EN.pdf (Accessed: 30 January 2025).

Lorenzen, B. (2022) 'Geschäftsgeheimnisschutz und Data Act', *Zeitschrift für geistiges Eigentum*, 14(3), pp. 250–267.

Macher, E. and Graf Ballestrem, J. (2023) 'Der neue EU Data Act: Zugang zu Daten – und Geschäftsgeheimnissen?', *Gewerblicher Rechtsschutz und Urheberrecht in der Praxis*, 125(9), pp. 661–664.

Martens, B. (2023) *Pro- and anti-competitive provisions in the proposed European Union Data Act (2023)* [Online]. Available at: https://www.bruegel.org/sites/default/files/2023-01/WP%2001.pdf (Accessed: 30 January 2025).

Metzger, A. and Schweitzer, H. (2023) 'Shaping Markets: A Critical Evaluation of the Draft Data Act', *Zeitschrift für Europäisches Privatrecht*, 31(1), pp. 42–80.

Podszun, R. and Pfeifer, C. (2022) 'Datenzugang nach dem EU Data Act: Der Entwurf der Europäischen Kommission', *Gewerblicher Rechtsschutz und Urheberrecht*, 124(13), pp. 953–961.

Rakoff, T. D. (1983) 'Contracts of Adhesion: An Essay in Reconstruction', *Harvard Law Review*, 96(4), pp. 1173–1284.

Rammos, T. and Wilken, T. (2022) 'Der Data Act – Chancen und Risiken für Unternehmen durch das geplante europäische Datengesetz', *Der Betrieb*, 20, pp. 1241–1249.

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) *Official Journal* L119, 4 May, pp. 1–88 [Online]. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 30 January 2025).

'Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act)' (2022) *Official Journal* L152, 3 June, pp. 1–44. [Online]. Available at: http://data.europa.eu/eli/reg/2022/868/oj (Accessed: 30 January 2025).

'Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act)' (2022) *Official Journal* L265, 12 October, pp. 1–66. [Online]. Available at: http://data.europa.eu/eli/reg/2022/1925/oj (Accessed: 30 January 2025).

'Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act)' (2023) *Official Journal* L, 22 December, pp. 1–71. [Online]. Available at: http://data.europa.eu/eli/reg/2023/2854/oj (Accessed: 30 January 2025).

Richter, S. (2022) 'Der schmale Grad zwischen Schutz personenbezogener Daten und Datenkommerzialisierung – Eine Analyse des Zusammenspiels des Entwurfs zum Data Act und der GDPR' in Heinze, C. (ed.) *Tagungsband Herbstakademie 2022 – Daten, Plattformen und KI als Dreiklang unserer Zeit*. Oldenburg, Germany: Oldenburger Verlag für Wirtschaft, Informatik und Recht, pp. 299–311.

Schmidt-Kessel, M. (2024a) 'Einordnung des Data Act in das Mehrebenensystem des Unionsprivatrechts', *Multimedia und Recht*, 27(MMR-Beilage), pp. 122–128.

Schmidt-Kessel, M. (2024b) 'Heraus- und Weitergabe von IoT-Gerätedaten', *Multimedia und Recht*, 27(MMR-Beilage), pp. 75–82.

Specht-Riemenschneider, L. (2022a). 'Data Act – Auf dem (Holz-)Weg zu mehr Dateninnovation?' *Zeitschrift für Rechtspolitik*, 55(5), pp. 137–140.

Specht-Riemenschneider, L. (2022b) 'Der Entwurf des Data Act', *Multimedia und Recht-Beilage*, 25(MMR-Beilage), pp. 809–826.

Specht-Riemenschneider, L. (2023) 'Datennutz und Datenschutz: Zum Verhältnis zwischen Datenwirtschaftsrecht und GDPR', *Zeitschrift für Europäisches Privatrecht*, 31(3), pp. 638–669.

Steinrötter, B. (2023) 'Verhältnis Data Act und DS-GVO: Zugleich ein Beitrag zur Konkurrenzlehre im Rahmen der EU-Digitalgesetzgebung', *Gewerblicher Rechtsschutz und Urheberrecht*, 125(4), pp. 216–226.

Wiebe, A. (2016) 'Protection of industrial data – a new property right for the digital economy?', *GRUR International Journal of European and International IP Law*, 65(10), pp. 877–884.

Wiebe, A. (2023) 'The Data Act Proposal – Access rights at the intersection with Database Rights and Trade Secret Protection', *Gewerblicher Rechtsschutz und Urheberrecht*, 125(4), pp. 227–238.

Zech, H. (2015a) 'Daten als Wirtschaftsgut – Überlegungen zu einem "Recht des Datenerzeugers"', *Computer und Recht*, 31(3), pp. 137–146.

Zech, H. (2015b) '"Industrie 4.0" – Rechtsrahmen für eine Datenwirtschaft im digitalen Binnemarkt', *Gewerblicher Rechtsschutz und Urheberrecht*, 117(2), pp. 1151–1160.

EU Data Protection Law in Action: Introducing the GDPR

Julia Krämer

Abstract

This chapter is intended to introduce the General Data Protection Regulation (GDPR) to social scientists, offering an overview of key legal concepts and provisions from Chapters II and III of the Regulation. The chapter has two main objectives: first, to bridge the gap between empirical and doctrinal research by explaining fundamental GDPR provisions to non-legal audiences; and second, to examine the extent to which these provisions have been explored through empirical research. This includes identifying common methods used, revealing that, only six years after the Regulation's implementation, a rich body of empirical research has emerged to evaluate its effectiveness. The chapter concludes with a discussion of the challenges social scientists face when empirically investigating the impact of the GDPR, such as translating empirical findings into legal conclusions.

1. Introduction

In May 2018, the implementation of the General Data Protection Regulation (GDPR) represented a landmark moment in EU data protection law. As the new legal framework governing the processing of personal data within the EU, the GDPR replaced the outdated provisions of the 1990s, which were drafted when the internet was still in its infancy. Six years after its implementation, the GDPR still stands out as one of the most advanced data protection laws globally (Streinz, 2021, p. 903), prompting questions and reflections on its actual impact. Prior to its implementation, some authors have claimed that the GDPR would not only change EU data protection law, but "nothing less than the whole world as we know it" (Albrecht, 2016, p. 287). Today, six years after the GDPR became enforceable, the empirical reality can help ascertain whether such statements and hopes have been exaggerated or accurately reflect the law's actual impact, and whether the Regulation can succeed in achieving its desired outcomes.

At the heart of the GDPR lies a dual objective: safeguarding fundamental rights and ensuring the free flow of personal data across the EU (Hijmans, 2020, p. 56). As a Regulation, the GDPR harmonises the rules concerning the processing of personal data and is directly applicable in EU Member States. This shift, however, does not imply that national data protection law is no longer applicable. The GDPR contains several opening clauses that permit Member States to establish more specific rules beyond those outlined in the Regulation. The GDPR marks a significant shift from the previous framework, the Data Protection Directive (DPD) (Directive 95/46/EC), which obligated Member States to implement provisions in national law first, resulting in the fragmentation of data protection rules across the EU (Recital 9 GDPR, Regulation (EU) 2016/679). While the shift from Directive to Regulation presented a significant legal transformation, most core concepts and principles of the DPD can also be found in the GDPR. However, despite this continuity, the data protection and business community alike have perceived the GDPR as revolutionary, which can be credited to the increased attention paid to the stringent new sanction regime (Streinz, 2021, p. 909).

The GDPR and its provisions have been subject to a growing body of doctrinal (legal) research, alongside an increasing number of empirical investigations aimed at exploring their impact and effectiveness. Whereas doctrinal research aims to systematically state the principles, rules, and concepts that apply to a particular area of law and create the connections thereof (Smits, 2017), empirical legal research uses observations to systematically examine how the law works (Bos, 2020, p. 3). While doctrinal research forms the theoretical basis for the empirical exploration of the law (Dagan, Kreitner and Kricheli-Katz, 2018, p. 292), empirical assessments can help determine if certain assumptions on which the law is based are actually correct in practice (Galligan, 2010, p. 998). This is particularly important in the context of the GDPR, which operates within a rapidly evolving digital environment where theoretical frameworks need to be tested against real-world data to ensure the Regulation's objective to effectively protect data subjects.

To support this goal, this chapter aims to bridge empirical and doctrinal research by introducing key GDPR provisions to non-legal audiences. Hence, the objective here is twofold: first, to introduce and explain provisions of the GDPR; and second, to investigate the extent to which these provisions have been the subject of empirical legal research. The chapter

presents research identifying the provisions that are effectively achieving their intended effects, as well as those that may be falling short. However, the list of analysed GDPR provisions presented is by no means exhaustive, as this would require more than a single book chapter to sketch the extensive catalogue of provisions and research already surrounding the GDPR.[1] Instead, this chapter offers a brief introduction to the central provisions and provides guidance on their use as the subject of empirical legal research. This approach is crucial as empirical research is most effective when the law presents testable propositions that can be investigated using social science methods (Davies, 2020, p. 135). Accordingly, the focus lies on the general provisions and data subject rights, thus prompting the exploration of Chapters II and III of the GDPR.

This chapter proceeds as follows. The first section clarifies the scope of the GDPR and introduces important concepts and principles. Secondly, the chapter introduces explanations of key provisions of the GDPR relating to data subject rights and transparency, and how they have already been assessed by empirical legal scholarship. The third section offers a comprehensive overview of the empirical methods employed to evaluate the Regulation. The last section highlights the complementary relationship between empirical legal studies and doctrinal research, and presents a method for integrating the two, followed by the conclusion.

2. Key concepts of the GDPR

This section presents key concepts important for social scientists delving into the GDPR, including its scope, the allocation of responsibilities among various actors, and the principles governing the law. For a deeper understanding of individual provisions, researchers can refer to legal commentaries,[2] which offer comprehensive insights into specific laws authored by legal scholars, or institutional guidelines. In the context of EU data protection law, such bodies as the European Data Protection Board (EDPB) and its predecessor, Art. 29 Working Party (Art29WP), routinely publish and

1 A systematic review of empirical research about the GDPR can be found in Li et al. (2025).

2 See, for instance, Kuner et al. (2020) for a GDPR commentary in English.

have published guidelines.[3] While these are non-binding, their influence has been substantial, as evidenced by their citation in judgments and opinions of the Court of Justice of the EU (CJEU), the highest court of the EU that is crucial in interpreting data protection law.[4]

2.1 The scope of the GDPR

The GDPR applies to "the processing of personal data […]" (Art. 2(2) GDPR), which forms the law's material scope, or, in other words, the subject matter to which the law applies. The territorial scope of the GDPR, as outlined in Art. 3, defines the applicable geographical area. The GDPR covers:

a. The processing of personal data by controllers and processors within the EU, regardless of where data subjects are located.
b. The processing of personal data of individuals within the EU by controllers or processors outside of its borders, if the processing activities are related to offering goods or services to, or monitoring the behaviour of, individuals within the EU.

Consequently, the GDPR applies even if an EU-based company is processing personal data from a user outside the EU, or vice versa. As opposed to the narrower territorial scope of the DPD that was limited to the borders of the Member States, the reach of EU data protection law significantly expanded with the introduction of the GDPR (Svantesson, 2020).

2.1.1 Processing

Crucial in determining the application of the GDPR is the *processing* of personal data. Processing encompasses a very broad definition of activities through its definition as "any operation or set of operations which is performed on personal data or on sets of personal data […]" (Art. 4(2) GDPR). Thus, processing data encompasses recording, collecting, structuring, or storing personal data, but also anonymising or destroying data. There are

3 A list of these guidelines with the corresponding GDPR provision can be found in Table 1.

4 See, for instance, the Opinion of the Advocate General Pikamäe in "UF and AB v. Land Hesse (Joined party: SCHUFA Holding AG)" (2023), para. 69.

also exceptions that are not covered by this provision, such as the processing of personal data during a "purely personal or household activity" (Art. 2(2)(c) GDPR). This exemption, often referred to as the "household exemption", clarifies that activities conducted by individuals for strictly personal purposes are excluded from the GDPR's scope. Furthermore, the Regulation does not apply to processing in the context of preventing criminal offences or public-security threats (Art. 2(2)(d) GDPR).

2.1.2 Personal data

Another central element of the GDPR is the legal concept of personal data, as processed data must be *personal* in order for the GDPR to apply. This is further specified in Article 4(1), which defines personal data as "any information relating to an identified or identifiable natural person [..]". This identified or identifiable person is referred to as a "data subject". In general, if the identification of a data subject is not possible, taking into account all of the means *reasonably likely* to be used (Recital 26 GDPR), these data are regarded as non-personal, or "anonymous", data (Bygrave and Tosoni, 2020, p. 105). The "reasonably likely" criterion takes into account the costs, time, effort, and available technological resources at the time of processing, and should thus be regarded as an objective criterion (Hildebrandt, 2020, p. 140). The definition of personal data is almost the same as in the preceding DPD, which is why pre-GDPR case law continues to be relevant today (Bygrave and Tosoni, 2020, p. 108).

One landmark case is "Breyer v. Bundesrepublik Deutschland" (2016), in which the CJEU significantly broadened the scope of the concept of personal data. In this case, the CJEU ruled that "it is not required that all the information enabling the identification of the data subject must be in the hands of one person" (Breyer v. Bundesrepublik Deutschland, 2016, para. 43). In essence, this signifies that, even if an entity lacks the technical means to directly identify someone, if there exists a legal framework or likely means to identify said person, the data must be treated as personal. As an illustration, consider dynamic IP addresses, which are identifiers assigned to devices to connect them to the internet. Despite a website owner's inability to directly connect an IP address with a specific visitor, if there is a lawful method for another party to use said address to ascertain the visitor's identity, the GDPR mandates treating IP addresses as personal data. As such, website hosts are obliged to afford IP addresses the same level

of protection as other identifiable personal data, irrespective of their ability to link the address to a data subject.

2.1.3 Controllership

The GDPR imposes obligations and responsibilities on the controller of personal data. A data controller is defined as the entity "that determines the purposes and means of the processing of personal data" (Art. 4(7) GDPR). Next to controllers, joint controllers, who jointly determine purposes and means of data processing with other controllers (Art. 26 GDPR), and processors, who process data on behalf of a controller (Art. 4(8) GDPR), can be held accountable under the GDPR. Accordingly, the concept of purposes and means of data processing is emphasised, which can be assessed by asking who decides *why* the processing is occurring and *how* this objective, or the purpose of processing, can be reached (EDPB, 2020d, para. 35). When designated as a controller under the GDPR, the responsible entity must implement appropriate technical and organisational means that adequately address the processing in question and minimise risks for data subjects (Art. 24 GDPR). Failure to do so may result in controllers being subject to fines of up to €20 million or up to 4% of their global annual turnover, as outlined in Art. 83(5) GDPR.

Recent jurisprudence has specified some further guidance on the scope of the controllership concept. In "Tietosuojavaltuutettu v. Jehovan todistajat" (2018, para. 75), the CJEU held that an entity can be deemed a controller regardless of whether it has access to personal data. In "Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH" (2018), the CJEU ruled on a similar issue. The question concerned the responsibility of a fan page owner on the social network Facebook. Despite lacking direct access to the data of visitors or the ability to influence its processing, the owner was deemed jointly responsible with Facebook for the processing under Art. 26 GDPR. The CJEU justified its decision by emphasising the entity's role in defining the purpose of the processing, such as establishing criteria for collecting statistics about fan page visitors (para. 36). This case highlights the challenges that platforms pose in determining controllership under the GDPR, especially in situations where platforms influence the extent of data processing practices conducted by their business users. The court, after all, applies the concept of (joint) controllership very broadly.

2.2 Principles of data processing

The processing of personal data is governed by the following principles, enshrined in Art. 5 GDPR, to which data controllers must adhere: fairness and transparency, purpose limitation, data minimisation, accuracy, storage limitation, integrity and confidentiality, and accountability.

The first principle encompasses *lawfulness*, *fairness*, and *transparency* (Art. 5(1)(a) GDPR). *Lawful* processing means that all legal requirements posed by the GDPR should be met. *Fair* processing demands that data subjects are not given misleading information or that the processing is not based on other deceptive means. *Transparency* requires that individuals are informed about who possesses what information about them, and the time and circumstances under which this information was obtained, thus aligning with the principle of informational self-determination. The principle is further specified in Arts. 12–15 GDPR and gives controllers a more detailed overview of what is expected of them.

Purpose limitation (Art. 5 (1)(b) GDPR) requires personal data to be processed solely for the explicit purposes defined by the data controller prior to the data collection. It is one of the most important principles in EU data protection law as it places constraints on data processing and holds the controller, who determines the purposes, accountable and liable (Hildebrandt, 2020, p. 149). The principle consists of two building blocks: (1) the purpose specification, which requires the data processing only for specified, explicit, and legitimate purposes; and (2) the compatible use, which prohibits further processing that is not compatible with those purposes (Art29WP, 2013b, pp. 11–12). Adhering to this principle prevents "function creep" (i.e., the expansion of a process or technology beyond its original purpose) by safeguarding users from privacy risks associated with unforeseen data processing (EDPB, 2020c, p. 14). Furthermore, in order to be effective, the principles of data minimisation and storage limitation depend on this concept.

Data minimisation (Art. 5(1)(c) GDPR) requires that data are processed to the extent necessary for the processing's purpose, by minimising the quantity of processed data to the greatest extent possible.

Accuracy (Art. 5(1)(d) GDPR) means that personal data should be kept up to date and accurate, as inaccurate personal data could put data subject rights at risk, especially when decision-making is based on this inaccurate information (EDPB, 2020a, p. 23).

Storage Limitation (Art. 5(1)(e) GDPR) mandates controllers to implement technical measures and safeguards to ensure that personal data are retained only for the duration necessary for processing purposes, such as by employing internal anonymisation or deletion procedures to prevent data from being stored beyond their intended use (EDPB, 2020a, p. 25).

Integrity and Confidentiality (Art. 5(1)(f) GDPR) aim to prevent security breaches by requiring data controllers to include appropriate technical or organisational measures. These are derived from the "CIA Triad" (Confidentiality, Integrity, and Availability), a fundamental model in information security. Art. 32 GDPR is closely connected to this principle, mandating that data controllers ensure an appropriate level of security relative to the risks posed to data processing

Lastly, *accountability* (Art. 5(2) GDPR) mandates the controller to assume responsibility for ensuring and showcasing compliance with all the aforementioned principles and is linked to transparency, as controllers are obliged to be able to demonstrate their data processing's compliance with the GDPR (Art29WP, 2018, p. 5).

3. Key provisions in the GDPR

The GDPR has frequently served as a subject for empirical research in recent years. These empirical assessments not only shed light on what the implementation of the GDPR has changed with respect to the foregoing DPD, but also on the effectiveness and implementation by data controllers. The following subsections describe some of the provisions that have been subject to empirical legal assessments, and a short description of their results.

3.1 Art 6 GDPR – lawful grounds for processing

The processing of personal data is forbidden, except when based on one of the legal grounds specified in Art. 6(1) GDPR. This involves (a) the consent of the data subject, (b) the performance of a contract, (c) compliance with a legal obligation of the controller, (d) the protection of vital interests of the data subject, (e) the performance of a task in the public interest, and (f) the legitimate interest of the data controller (Art. 6(1)(a–f) GDPR).

Every step of processing of personal data must be based on one of these grounds. Consequently, a legal basis is crucial for ensuring compliance

with the GDPR. A controller should always carefully evaluate which legal basis is appropriate for the intended processing; consent, for instance, is only lawful if the data subject can freely, and without facing negative consequences, accept or reject the proposed terms (EDPB, 2020c, p. 5). Under the legal basis of legitimate interest, a data subject's consent is not necessary to process personal data. A legitimate interest is an interest recognised by EU or national law, and purely commercial interest can thus not qualify as one (Kotschy, 2020, p. 337). Examples include processing data for direct marketing purposes, which could be based on the freedom to conduct a business, or processing data to prevent fraud, linked to the right to property (Kotschy, 2020, p. 337). However, there are also limitations, as the data subjects may still object to the processing based on legitimate interest (Art. 21(1) GDPR) and the controller's interests may be overridden by the fundamental rights or freedoms of data subjects (Art. 6(1)(f) GDPR). For instance, in "Meta Platforms v. Bundeskartellamt" (2023), the CJEU ruled that, following a balancing test, Meta could not rely on legitimate interest as a legal basis for processing personal data for the purposes of personalised advertising (para 117).

Kyi et al (2023) investigated the usage of the legal basis of legitimate interest in the context of privacy notices and the user perceptions thereof. The authors identified a lack of enforcement regarding the use of legitimate interest as a legal basis in cases where advertising practices may have been unaligned with genuinely legitimate grounds, thus highlighting the potential for this provision's exploitation. This empirical assessment thus enhances our understanding of how Art. 6 GDPR is used in practice. Empirical research centred around user consent (Art. 6(1)(a) GDPR), which is further specified in Art. 7, is explained in the following section.

3.2 Art. 7 GDPR – conditions for valid consent

Compared to the previous data protection regime, which defined consent as "any freely given specific informed indication of his wishes by which the data subject signifies his agreement to personal data [...]" (Art. 2 (h) DPD), the rules introduced with the GDPR are stricter. Here, consent is defined as "any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her" (Art. 4(11) GDPR). More context when consent is

lawful is delivered in Art. 7 GDPR. For instance, the request for consent should be intelligible and easily accessible (Art. 7(2) GDPR), and can be revoked by a data subject at any time (Art. 7(3) GDPR). A pre-ticked box, silence, or inactivity cannot constitute valid consent (Recital 32 GDPR), which also has been confirmed by the CJEU in "Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH" (2019).

Obtaining consent is crucial for tracking activities on the web and on mobile devices, as consent constitutes the only lawful basis for tracking that is not technically necessary (Kollnig, Binns, Dewitte, et al, 2021, p. 6).[5] Hence, several studies have investigated the GDPR's impact on the EU's cookie banner landscape. For instance, Degeling et al (2019) illustrated a notable 16% increase in the prevalence of websites displaying cookie banners by examining 6,579 popular EU websites before and after the GDPR's implementation.

The conditions for consent become especially important with the rise of dark patterns, which is an umbrella term for design patterns that steer user behaviour towards actions that benefit the entity implementing the design (Kyi et al, 2023). Often, user interfaces are designed so as to nudge users to agree to options that share personal data with a variety of third parties. However, this stands at odds with the GDPR's requirements, which demand consent to be *an unambiguous indication of wishes*, meaning that controllers should design consent banners that are clear to data subjects (EDPB, 2020c, p. 19). Furthermore, Art. 7(3) GDPR mandates that giving consent shall be as easy as withdrawing consent, which can also be extended to cookie banners.

Against this background, one could assume that the GDPR has reduced the prevalence of dark patterns. However, the analysis of 1,000 cookie banners post-GDPR showed that over half (57.4%) contained dark patterns (Utz et al, 2019, p. 976). Shedding light on user behaviour, Utz et al (2019) additionally showed that, when given a choice, only 0.1% of users would consent to the use of their data by third parties. In addition, some studies have investigated the impact of certain dark pattern designs on user behaviour, which helps to assess which design decisions are most likely to be manipulative, and could thus help enforce the GDPR (Machuletz

5 In this case, in addition to the GDPR, the ePrivacy Directive (2002/58/EC) is applicable to tracking activities on mobile devices, which must be transposed into national law. In Germany, for instance, the Telekommunikation-Digitale-Dienste-Datenschutz-Gesetz (TDDDG) (BGBl. I Nr. 149/2024) applies as soon as mobile devices are involved.

and Böhme, 2020; Nouwens et al, 2020). The issue does not only relate to the design of cookie banners: Santos et al (2021) studied the text of 407 banners, revealing that 89% of them did not comply with GDPR standards, notably by omitting or vaguely describing the purposes of data processing.

Moving from websites to the mobile ecosystem, Kollnig, Binns, Dewitte, et al (2021) studied consent notices offered by mobile apps to their users. Their study revealed that a considerable number of the 1,297 investigated Android apps failed to comply with the GDPR: of the 76% of apps that had been updated following the GDPR, and could thus have implemented the necessary adaptation, only 9% asked for user consent (Kollnig, Binns, Dewitte, et al, 2021, p. 7). On a yet-larger scale, Nguyen, Backes and Stock (2022, p. 13) studied consent notices across 239,381 Android apps, revealing that 13,082 implemented consent notices, and over 20% of those failed to meet the GDPR's consent standards.

These studies are important as they highlight the shortcomings of the GDPR's enforcement regarding consent on multiple fronts: first, by showcasing instances of non-compliance where the option to provide consent is not even offered; second, by exposing instances of uninformed consent resulting from the implementation of dark patterns; and third, by shedding light on user behaviour indicating a general reluctance to consent to tracking activities.

3.3 Art. 9 GDPR – Data revealing special categories of personal data

Art. 9 GDPR protects data revealing special categories of personal data, often referred to as "sensitive data" (Recital 10 GDPR). The following information is considered sensitive: "data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic and biometric data for the purpose of uniquely identifying a natural person and data concerning health or data concerning a natural person's sex life or sexual orientation" (Art. 9(1) GDPR). The rationale behind Art. 9 GDPR is to protect types of data whose processing may facilitate human rights violations or other serious consequences for an individual (Georgieva and Kuner, 2020). While the DPD already included a provision concerning special categories of data (Art. 8 DPD), the GDPR introduced additional categories, namely genetic and biometric data, and data concerning a person's sexual orientation. Recent advancements in data mining and the increased availability of data have made it possible to

infer sensitive information from seemingly harmless data, which poses a challenge to their effective protection (Quinn and Malgieri, 2021, p. 1596). To illustrate, accelerometers in mobile phone are used to stabilise images captured by the camera or detect certain movements like the shaking of a device. While considered non-sensitive, accelerometer data from mobile devices may be used to reveal a wide range of (sensitive) personal data, such as a data subject's location, degree of mobility, sleep patterns or gender (Kröger, Raschke and Bhuiyan, 2019).

Several studies have investigated the compliance of apps collecting their users' sensitive data. For instance, Parker et al (2019) analysed disclosures of 61 prominent mental health apps, including their privacy policies and permissions that process personal data concerning health. They highlighted that, while the GDPR has prompted some improvements in transparency, half of the investigated apps had no privacy policy whatsoever (Parker et al, 2019). These results are particularly alarming, considering that the disclosure of personal health information could result in serious emotional harm to users. Fan et al (2020) examined the degree of GDPR compliance among 736 general Android health apps. Their findings indicate non-compliance with transparency provisions and data minimisation, with a considerable number of apps failing to ensure the encryption of collected health data (Fan et al, 2020).

Shipp and Blasco (2020) conducted a study on 30 period tracking apps, which enable users to monitor menstruation and sexual activity to gain insights into their menstrual health. These apps track sensitive data, such as a user's sexual orientation or pregnancy-related information. The researchers discovered that 23 of these apps shared user data with third parties, raising concerns about insufficient disclosure regarding data collection purposes, user rights, and the failure to classify the collected data as sensitive (Shipp and Blasco, 2020). The findings are particularly concerning given the potential exploitation of sensitive data for targeted advertising purposes, especially considering the heightened vulnerability of users in such contexts (Siapka and Biasin, 2021).

These observations contribute to the discussion on the protection of sensitive data. Past incidents, such as data protection violations by Grindr – a dating app predominantly used within the queer community – underscore the critical need for adherence to the GDPR-mandated safeguards. Grindr, which collects data encompassing a data subject's sexual orientation, HIV status, and precise location, incurred a fine from the Norwegian Data Protection Authority for sharing these sensitive data with third parties without

valid user consent (Datatilsynet, 2021). While the GDPR was enforced, this instance likely represents only a fraction of the cases where controllers have failed to implement adequate safeguards for protecting users and their sensitive data. The case underlines the importance for further research in these areas of data protection law, particularly where marginalised communities are affected.

3.4 Arts. 12-14 GDPR – Transparency

In order to make informed decisions about who collects user data and under which circumstances, users should be provided with adequate information. Art. 12 GDPR specifies *how* this information should be provided to the user. The provision involves an entirely new transparency standard, namely that information should be "concise, transparent, intelligible and easily accessible form, using clear and plain language" (Art. 12(1) GDPR). Furthermore, Arts. 13 and 14 GDPR specify on *which* elements users should be informed. This list includes such elements as the identity of the data controller, for what the data will be used, the period for which the data are stored, and information about the user's rights under the GDPR. This information must be provided when personal data are obtained. The rationale behind these provisions is to ensure the effectiveness of personal data protection, as users can only exercise their rights if they are aware of the details of the processing of their data (Zanfir-Fortuna, 2020, p. 415). A privacy policy is the most popular form of providing this information.

3.4.1 Privacy policies (Arts. 12, 13, 14 GDPR)

Several studies have evaluated the GDPR's impact in the realm of transparency by evaluating the content of privacy policies with text-as-data methods over time (Degeling et al, 2019; Linden et al, 2019; Amos et al, 2021; Frankenreiter, 2022; Wagner, 2023). Advances in text-based methods allow for large corpora of privacy policies, and the patterns within them, to be analysed and identified. Web scraping, i.e. downloading website content from the internet, enables the creation of large text corpora. A particularly powerful tool for collecting and comparing pre- and post-GDPR privacy policies over a long period of time is the web scraping of past web pages. This is made possible by the Wayback Machine, a non-profit initiative which has archived over 850 billion web pages since 1996 (Internet Archive,

2024) and has been used in several studies investigating the impact of the GDPR (see, for instance, Wagner, 2023; Linden, 2019; Ganglmair, Krämer and Gambato, 2024).

In 2018, privacy policies in the EU underwent substantial revisions, as evidenced by Degeling et al (2019), who observed updates on the majority of 6,579 popular webpages post-GDPR enforcement. Similar observations were made by Linden et al (2019), who analysed 6,278 privacy policies both within and outside the EU. After the GDPR became enforceable, policies within the EU expanded by a third in length, while those outside the Union experienced a slightly smaller, but still notable, increase (Linden et al, 2019, p. 7).

Privacy policies have also been used to advance the computational methods for analysing legal content. The CLAUDETTE project, for instance, developed a methodology for the automated analysis of privacy policies using machine learning (Contissa et al, 2018). While the project remains in its preliminary stages, an automated analysis of privacy policies could help users, consumer associations, and researchers alike efficiently identify GDPR violations. Recent developments in natural language processing are likely to further develop the automated analysis of privacy policies, such as by analysing their content with the help of large language models (Rodriguez et al, 2024).

To test the impact of the higher standards of clear and plain language in privacy policies, which Art. 12(1) GDPR mandates, the readability of privacy policies has been measured quantitatively. This assessment can be done, for instance, via so-called readability indices that compute scores based on the length of words or sentences or the counting of obfuscating words perceived to lower a text's readability. While Becher and Benoliel (2021) found that privacy policies have become more readable, Wagner (2023) showed how they tend to use more obfuscating words since the GDPR. However, compared to Wagner's (2023) corpus of 56,416 unique privacy policies, Becher and Benoliel (2021) investigated a corpus of 24 pre- and post-GDPR policies, and their findings may, therefore, overgeneralise the GDPR's actual impact. Using a corpus of 585,000 Germany privacy policies, Ganglmair, Krämer and Gambato (2024) showed that, although the length of the average policy tripled after the GDPR came into force and contained more information, the average results for readability remained mixed. The authors argued that the enforcement of Art. 12(1) GDPR is inherently challenging due to its subjective nature, in contrast to the objective and readily enforceable information requirements in Arts. 13–14

(Ganglmair, Krämer and Gambato, 2024, p. 4). This study thus illustrates the "tension" inherent in the GDPR between improving the readability of privacy policies and the parallel obligation to add more comprehensive information (Art29WP, 2018, para. 34).

Further to quantitative assessments, some authors have conducted qualitative evaluations by individually analysing privacy policy content. Using this approach, Serveto (2020, p. 597) demonstrated that rules already established within the DPD were more frequently incorporated into the privacy policies of internet service providers than those newly introduced by the GDPR.

The effectiveness of GDPR provisions can also be assessed through the observation of users' responses and behaviours towards them. Before the adoption of the GDPR, empirical evidence had already demonstrated that users tend not to read lengthy legal documents online (Bakos, Marotta-Wurgler and Trossen, 2014). Ben-Shahar and Chilton (2016) demonstrated that, even when privacy policies are drafted in a readable manner, as the GDPR prescribes in Art. 12(1), user behaviour remains largely unchanged, with an overwhelming majority of individuals opting not to read them. These findings indicate that the anticipated behaviour envisioned by the GDPR is often not realised among data subjects. Subsequently, it should come as no surprise that doctrinal legal research has been critical of transparency provisions in data protection and privacy laws. Indeed, Solove (2012) claimed that, due to cognitive and structural limitations, data subjects are not able to engage effectively in privacy self-management. Similarly, Waldman (2021, p. 61) criticised the GDPR's "privacy-as-control" approach, which mandates readable privacy policies for data controllers, but does little to protect users from structural power imbalances and deceptive practices employed by powerful platforms.

3.4.2 Privacy labels and standardised icons (Art. 12(7) GDPR)

Due to the overwhelming criticism of privacy policies and the evidence that users rarely read online legal documents, researchers have devised various strategies with which to inform users about data processing practices. Examples are so-called privacy labels, which inform users more quickly and efficiently than privacy policies by using icons or other images (Kelley et al, 2009). A provision about privacy labels has also been incorporated into the GDPR and allows for the combination of the information delivered with "standardised icons in order to give an easily visible, intelligible and

clearly legible manner a meaningful overview of the intended processing" (Art. 12(7) GDPR).

Although the European Commission bears the responsibility of establishing a procedure to introduce these standardised icons (Art. 12(8) GDPR) – which has yet to make use of its competence (Polčák, 2020, p. 411) – an initial large-scale adoption of privacy labels has been launched in the Apple App Store and Google Play Store. In the absence of established procedures, these private actors have introduced their own (native) label designs. However, while these may enhance a data subject's awareness of data processing within apps, they have faced criticism for failing to adequately reflect privacy risks (Kollnig et al, 2022), as well as for favouring Apple's and Google's native tracking practices while not complying with the GDPR (Krämer, 2024). Furthermore, recent qualitative studies have shown that the categories chosen by the app stores confuse users and developers (Gardner et al, 2022; Zhang et al, 2022), which calls into question whether the labels can meet the GDPR's transparency standards. These examples make it clear that alleged improvements should be critically and empirically examined in order to determine whether the new measures actually improve user privacy.

3.5 Measuring data flows and tracking – transparency and data minimisation

The aforementioned studies investigated compliance with the GDPR based on the disclosures firms have made in their privacy policies. Rather than analysing statements by data controllers, certain authors opted to directly measure data flows and assess whether the GDPR has effectively reduced personal data collection.

In the realm of mobile apps, this has been done by Kollnig, Binns, Van Kleek et al (2021), who investigated how the amount of tracker libraries in apps has developed post-GDPR. The authors found that third-party tracking has not changed significantly, which they interpreted as a lack of GDPR enforcement within the mobile ecosystem (Kollnig, Binns, Van Kleek et al, 2021). Regarding webpages, Sanchez-Rola et al (2019) investigated 2,000 popular websites around the world. While the majority of websites (e.g., those in the US) try to somehow comply with the GDPR by having privacy policies or consent banners, 90% of those investigated engage in tracking by placing long-lasting identifiers on user devices, despite the

GDPR's mandate that personal data should only be stored for a minimum necessary duration. Relatedly, Matte et al (2020) investigated whether data subjects' cookie choices are respected. They examined 1,426 websites to determine which choices were actually saved in the browser and found that 141 websites recorded positive consent despite the user having rejected cookies.

These findings are alarming as they showcase the extent of tracking via the web or mobile devices. Tracking can facilitate various harms, including discrimination, financial harms, or threats to democracy (Cofone, 2023, p. 112). For example, individuals may suffer financial harm when coerced into purchasing products they neither want nor need (Cofone, 2023, p. 112). The preceding empirical studies can, therefore, provide the necessary evidence to support doctrinal assessments that have pointed out various privacy risks and harms connected to tracking.

3.6 Art. 15 GDPR – right of access

Art. 15 GDPR gives data subjects the right to confirm whether their personal data has been processed, to obtain access to their processed personal data, and to receive information about the processing activities themselves. Consequently, the right of access empowers data subjects to confirm the accuracy of their personal data and ascertain whether the data controller holds any such data in the first place (EDPB, 2023, p. 8).

While data subject rights are empowering, they must also be respected by data controllers so that they can unravel their full potential. Dexe et al (2020) explored the responsiveness of the Swedish home insurance market to data subject requests during late 2018 and early 2019. They identified deficiencies in adequately describing requested components, such as legal bases or processing descriptions, and noted failures to meet designated time limits. In a subsequent study encompassing insurance companies across five EU countries in 2021, the researchers analysed access requests detailing automated decision-making (Dexe et al, 2022). Although responses were received from all contacted data controllers, the majority were notably vague, with the researchers uncovering disparities among these responses, possibly due to the subtle differences in the translations of the GDPR (Dexe et al, 2022).

The effectiveness of Art. 15 GDPR in relation to online service providers was investigated by Dewitte and Ausloos (2024), who sent access requests

to 70 data controllers in 2020 and 2022. The results show that, although the majority of the controllers surveyed responded to the requests, many of the responses were generalised and untailored to the individual case, thereby possibly violating Art. 15. In addition, over half of the responses took more than a month to be issued (Dewitte and Ausloos, 2024, p. 21) despite this exceeding the deadline stipulated in Art. 12(3). Instead of looking at the compliance of controllers, Borem et al (2024) explored the experiences of 33 data subjects to the responses of data access requests. While the responses often left participants' specific questions unanswered, some participants were shocked and angry about the privacy implications after discovering the amount of data that was held by the controller.

Furthermore, the scope of Art. 15(1)(h) has been examined, which, in the context of automated decision-making, requires controllers to provide meaningful information about the logic involved and the significance and envisaged consequences of data processing for the data subject. Custers and Heijne (2022) examined the interpretation of these elements by conducting a survey addressed to data protection authorities, which was accompanied by several expert interviews. The survey revealed that only a small fraction of respondents considered code as relevant, while the majority viewed the categories in which a data subject is placed as "meaningful information" (Custers and Heijne, 2022, p. 11).

In conclusion, the presented studies serve as useful guides for understanding and assessing the extent of GDPR compliance among data controllers in different EU Member States, and thereby offer valuable guidance to data protection authorities and policymakers.

3.7 Art. 17 GDPR – right to be forgotten

The right to erasure, also known as the right to be forgotten, grants users the possibility to have their personal data erased from the records of data controllers under specific circumstances, such as if the data subject withdraws consent, the data have been unlawfully processed, or the data are no longer necessary in relation to the purposes for which they were initially collected (Art. 17(1) GDPR). This obligation can involve users requesting search engines to delist websites that appear when searching for the user's name (EDPB, 2020b, p. 4). The CJEU established the right to be forgotten in the landmark case "Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González"

(2014), by interpreting provisions of the DPD as ensuring such a right. The GDPR subsequently codified this right, elevating it to a standalone Article. While this seems to represent a significant deviation from the DPD, it is also viewed by some as merely a "more detailed elaboration of the already existing right of erasure" (Kranenborg, 2020, p. 477).

The right to erasure has been tested regarding its effectiveness and how controllers manage these challenges. For instance, Rupp et al (2022) sent erasure requests to 90 different service providers, of which 27% failed to respond. To explore potential challenges that data controllers face when complying with this right, Mangini et al (2020) conducted a structured survey to explore the right's implications for data controllers. The authors found that tight deadlines and a lack of knowledge connected with complying to the right have been particularly challenging for controllers, but the GDPR also introduced advantages regarding processing, such as an increased awareness regarding internal data processing activities. In highlighting the continued challenges for both data subjects and controllers, these studies showcase that there is still room for improvement in complying with the right to be forgotten.

4. A rich methodological toolbox

The preceding section has demonstrated how empirical research provides valuable insights into the effectiveness of the GDPR, highlighting the diverse methods available for studying its provisions. Table 1 lists the research discussed above, accompanied by the types of measurement employed.

Table 1: Overview of empirical (legal) research regarding specific GDPR provisions, and the type of method used

GDPR provision	Official Guidelines	Prior empirical work	Type of method
Lawful grounds for processing			
Art. 6(1)(f)		Kyi et al (2023)	Observational data analysis
Consent	European Data Protection Board (2020c)		
Art. 7 GDPR		Santos et al (2021)	Observational data analysis
		Utz et al (2019) Nouwens et al (2020)	Field experiment
		Kollnig, Binns, Dewitte et al (2021) Nguyen et al (2022)	Dynamic analysis of mobile data flows
Sensitive data			
Art. 9 GDPR		Parker et al (2019) Fan et al (2020) Shipp and Blasco (2020)	Systematic analysis of health apps
Transparency	Art. 29 Working Party (2018)		
Art. 5(1) GDPR, Arts. 12–14 GDPR		Degeling et al (2019) Linden et al (2019) Amos et al (2021) Wagner (2023) Contissa et al (2018)	Natural language processing and text-as-data methods
		Bakos et al (2014)	Field study into online browsing behaviour
		Ben-Shahar and Chilton (2016)	Experiment
Art. 12(7) GDPR		Kollnig, Binns, Van Kleek et al (2022) Gardner et al (2022) Krämer (2024)	Observational data analysis
		Zhang et al (2022)	Interviews

GDPR provision	Official Guidelines	Prior empirical work	Type of method
Transparency, data minimisation, and storage limitation			
	ENISA (2017) Art. 29 Working Party (2013a)	Kollnig, Binns, Van Kleek et al (2021)	Static analysis of mobile apps
		Matte, Bielova and Santos (2020)	Systematic analysis of back-end cookie banner choices
		Sanchez-Rola et al (2019)	Systematic analysis of cookie banners and trackers
Right to access Art. 15 GDPR	European Data Protection Board (2023)	Dexe et al (2020) Dexe et al (2022) Dewitte and Ausloos (2024)	Field study
		Borem et al (2024) Custers and Heijne (2022)	Survey
Right to erasure / right to be forgotten Art. 17 GDPR	European Data Protection Board (2020b)	Mangini, Tal and Moldovan (2020)	Survey
		Rupp, Syrmoudis and Grossklags (2022)	Field study

Surveys and studies involving data controllers and subjects that send out erasure or access requests can showcase how controllers perceive and respond to certain GDPR provisions. Experiments complement this perspective by showing how data subjects behave when confronted, for instance, with cookie banners or privacy policies. A rich methodological toolbox can thus paint a detailed picture of the GDPR's impact on different aspects of data processing.

4.1 Challenges for empirical (legal) studies in the context of the GDPR

The previous sections have shown a growing field of empirical (legal) research connected to the GDPR, with a variety of methodological approaches employed. These studies are crucial for understanding the practical implementation of the GDPR. Nevertheless, there are also challenges. Empirical research begins with certain basic ideas about how laws work, and how these ideas are put into practice within legal systems (Dagan, Kreitner and Kricheli-Katz, 2018, p. 302). Some authors have claimed, therefore, that empirical research should use legal theory as a point of departure so as to prevent it from operating in isolation (Smits, 2017, p. 17; Davies, 2020, p. 9). Thus, two challenges arise: first, how to properly design empirical studies exploring the GDPR and, second, how to translate these empirical insights into normative statements within legal doctrine.

For this reason, Towfigh (2014, p. 678) suggested some key points to consider for ensuring that empirical evidence can be effectively integrated into legal expertise. Firstly, an empirical study should define variables according to existing legal norms. Secondly, results should be generalisable to the legal context and properly operationalised. Lastly, the design, methods, statistics, and conclusions of an empirical study must pass tests of validity (Towfigh, 2014).

The first step in Towfigh's (2014) method ensures the correct definition of legal concepts to avoid any inconsistencies between legal concepts and social science methods, which may carry different assumptions. In the context of privacy, for instance, there is often a conceptual gap between the legal concept and the mathematical understanding of this concept (Cohen and Nissim, 2020, p. 8344). In addition to legal provisions, further guidance for defining a legal concept may be found in CJEU rulings, which are legally binding, and EDPB guidelines, which, while not, can still serve as valuable tools.

Secondly, the operationalisation of the legal concept is of importance, as it is not always easy to measure the legally defined concepts of the first step. Determining operators that define legal compliance is complex, particularly in the case of the GDPR, where legal uncertainty remains regarding its newly introduced provisions. To give a well-designed example in the context of consent, Nouwens et al (2020) translated GDPR provisions into three quantifiable minimum requirements necessary for cookie banners to be compliant (e.g., no pre-ticked boxes, consent being an explicit act like clicking a button, accepting being as easy as rejecting cookies). While

the authors acknowledged that meeting these conditions alone does not guarantee compliance, as additional factors must be assessed qualitatively, they were able to demonstrate that only 11.8% of cookie banners met these minimal requirements, with the rest violating the GDPR (Nouwens et al, 2020, p. 5). Consequently, these findings, while not covering all elements of compliance, are useful for highlighting widespread non-compliance in cookie banners.

Thirdly, in the final step of Towfigh's (2014, p. 680) method, the results must be checked for validity. When considering the implications of results, it is important to distinguish between challenges that can be addressed within the framework of the GDPR and those challenges that question the Regulation's underlying assumptions or structural issues. For example, the issue of privacy label designs being influenced by private interests (as discussed in Section 3.4) could be resolved through a procedure that standardises these labels, as permitted by the GDPR (Art. 12(7)). However, the European Commission (who must initiate the procedure) has yet to materialise this competence. Furthermore, many studies have cited a lack of enforcement of GDPR provisions as the reason why empirical results consistently identify non-compliance, which could also be mitigated within the existing framework.

On the other hand, the problem that users rarely read privacy policies because they often lack the cognitive ability and training to process large amounts of text written in legalese (Waldman, 2020) is a structural problem that will not be solved by the (properly enforced) GDPR. This problem persists despite the new requirement for readability in privacy policies (Art. 12(1) GDPR). In fact, while the GDPR mandates clearer disclosures, it also requires that users be informed about more categories of information, which has led to studies showing that the length of the average privacy policy post-GDPR has tripled (Ganglmair, Krämer and Gambato, 2024) and that more obfuscatory words are used (Wagner, 2023). As such, mechanisms dependent on transparency, such as *informed* consent (Art. 4(11) GDPR), may fall short of realising their potential, not necessarily because to a lack of enforcement by data protection authorities, but due to the underlying assumptions within the GDPR itself. It is therefore important to reconcile the conclusions from empirical studies with the distinction between challenges that can be resolved within the legal framework of the GDPR and those that fundamentally challenge its basic principles.

While empirical research is a powerful and necessary tool for exploring GDPR provisions next to a doctrinal analysis, it is important for both legal

scholars and social scientists to also consider the challenges that may arise when employing these methods. As this section has shown, a plurality of methods can help evaluate the GDPR's impacts from data subject and controller perspectives, and allows for the identification of dynamics that can inform regulators and policy makers.

5. Conclusion

This chapter has introduced several key provisions of the GDPR, with the aim of inspiring future empirical studies and mapping existing ones on EU data protection law. While doctrinal analysis in the GDPR's context has traditionally received more attention, the chapter has shown that empirical (legal) research in the context of the GDPR is already prominent. The described studies have helped identify areas in which compliance presents several shortcomings, such as the challenge stemming from a lack of the Regulation's enforcement. Despite legal obligations imposed on controllers, the empirical evidence provided reveals non-compliance, such as the absence of privacy policies, deceptive consent practices, and irregular data handling, which calls into question the effectiveness of the Regulation. A distinction must be made here as to the extent to which these shortcomings are due to the GDPR's design or to a lack of enforcement and compliance that could potentially be mitigated in the future.

Moreover, this chapter has stressed the need for interdisciplinary research regarding the GDPR and data protection law in general. As seen in the research surrounding the effectiveness of privacy policies and the prevalence of dark patterns, empirical research can provide the necessary evidence to pinpoint major deficiencies in the assumptions on which the law is based. By bridging legal analysis with empirical findings, interdisciplinary research can yield important insights into the practical implications and shortcomings of data protection laws. Such collaborative efforts pave the way for more effective policy interventions and regulatory responses aimed at safeguarding fundamental rights in the Digital Age.

References

Albrecht, J.P. (2016) 'How the GDPR will change the world: the General Data Protection Regulation: foreword', *European Data Protection Law Review (EDPL)*, 2(3), pp. 287–289.

Amos, R., Acar, G., Lucherini, E. et al (2021) 'Privacy policies over time: curation and analysis of a million-document dataset', in *Proceedings of the Web Conference 2021. WWW '21: The Web Conference 2021*, ACM, pp. 2165–2176.

Art29WP (2013a) *Opinion 02/2013 on apps on smart devices*. 00461/13/EN WP 202. Article 29 Working Party [Online]. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp202_en.pdf (Accessed: 30 January 2025).

Art29WP (2013b) *Opinion 03/2013 on purpose limitation*. Article 29 Working Party [Online]. Available at: https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2013/wp203_en.pdf (Accessed: 30 January 2025).

Art29WP (2018) *Guidelines on transparency under Regulation 2019/679*. 17/EN WP260 rev.01. Article 29 Working Party [Online]. Available at: https://www.edpb.europa.eu/system/files/2023-09/wp260rev01_en.pdf (Accessed: 30 January 2025).

Bakos, Y., Marotta-Wurgler, F. and Trossen, D.R. (2014) 'Does anyone read the fine print? Consumer attention to standard-form contracts', *The Journal of Legal Studies*, 43(1), pp. 1–35.

Becher, S.I. and Benoliel, U. (2021) 'Law in books and law in action: the readability of privacy policies and the GDPR' in Mathis, K. and Tor, A. (eds.) *Consumer law and economics*. Cham: Springer International Publishing, pp. 179–204.

Ben-Shahar, O. and Chilton, A. (2016) 'Simplification of privacy disclosures: an experimental test', *The Journal of Legal Studies*, 45(S2), pp. S41–S67.

Borem, A., Pan, E., Obielodan, O. et al (2024) 'Data subjects' reactions to exercising their right of access', in *33rd USENIX Security Symposium. USENIX* [Online]. Available at: https://www.usenix.org/conference/usenixsecurity24/presentation/borem (Accessed: 22 July 2024).

Bos, K. (2020) *Empirical legal research: a primer*. Cheltenham: Edward Elgar Publishing.

Bygrave, L.A. and Tosoni, L. (2020) 'Article 4(1). Personal data' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 103–115.

Cofone, I. (2023) *The privacy fallacy: harm and power in the information economy*. Cambridge: Cambridge University Press.

Cohen, A. and Nissim, K. (2020) 'Towards formalizing the GDPR's notion of singling out', *Proceedings of the National Academy of Sciences*, 117(15), pp. 8344–8352.

Contissa, G., Docter, K., Lagioia, F. et al (2018) '(C)laudette meets GDPR: automating the evaluation of privacy policies using artificial intelligence'. Rochester, NY. Available at: https://doi.org/10.2139/ssrn.3208596.

Custers, B. and Heijne, A.-S. (2022) 'The right of access in automated decision-making: The scope of Article 15(1)(h) GDPR in theory and practice', *Computer Law & Security Review*, 46, 105727 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105727 (Accessed: 30 January 2025).

Dagan, H., Kreitner, R. and Kricheli-Katz, T. (2018) 'Legal theory for legal empiricists', *Law & Social Inquiry*, 43(02), pp. 292–318.

Datatilsynet (2021) *The NO DPA imposes fine against Grindr LLC*. Datatilsynet [Online]. Available at: https://www.datatilsynet.no/en/regulations-and-tools/regulations/avgjorelser-fra-datatilsynet/2021/gebyr-til-grindr/ (Accessed: 26 April 2024).

Davies, G. (2020) 'the relationship between empirical legal studies and doctrinal legal research', *Erasmus Law Review*, 13(2), pp. 3–12.

Degeling, M., Utz, C., Lentzsch, C. et al (2019) 'We value your privacy ... now take some cookies: measuring the GDPR's impact on web privacy', in *Proceedings 2019 Network and Distributed System Security Symposium. Network and Distributed System Security Symposium*, Internet Society [Online]. Available at: https://doi.org/10.14722/ndss.2019.23378 (accessed: 30 January 2025).

Dewitte, P. and Ausloos, J. (2024) 'Chronicling GDPR transparency rights in practice: the good, the bad and the challenges ahead', *International Data Privacy Law*, pp. 106–133.

Dexe, J., Franke, U., Söderlund, K. et al (2022) 'Explaining automated decision-making: a multinational study of the GDPR right to meaningful information', *The Geneva Papers on Risk and Insurance – Issues and Practice*, 47(3), pp. 669–697.

Dexe, J., Ledendal, J. and Franke, U. (2020) 'An empirical investigation of the right to explanation under GDPR in insurance' in S. Gritzalis et al. (eds.) *Trust, privacy and security in digital business*. Cham: Springer International Publishing, pp. 125–139.

'Digitale-Dienste-Gesetz (DDG)' BGBl. I Nr. 149/2024 [Online]. Available at: https://www.recht.bund.de/bgbl/1/2024/149/VO (Accessed on: 30 January 2025).

'Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data' (1995) *Official Journal* L 281, 23 November, pp. 31–50 [Online]. Available at: http://data.europa.eu/eli/dir/1995/46/oj (Accessed: 30 January 2025).

'Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)' (2002) *Official Journal* L 201, 31 July, pp. 37–47 [Online]. Available at: http://data.europa.eu/eli/dir/2002/58/oj (Accessed: 30 January 2025).

EDPB (2020a) *Guidelines 4/2019 on Article 25 data protection by design and by default*. Brussels: European Data Protection Board [Online]. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201904_dataprotection_by_design_and_by_default_v2.0_en.pdf (Accessed: 30 January 2025).

EDPB (2020b) *Guidelines 5/2019 on the criteria of the right to be forgotten in the search engines cases under the GDPR* [Online]. Brussels: European Data Protection Board. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_201905_rtbfsearchengines_afterpublicconsultation_en.pdf (Accessed: 30 January 2025).

EDPB (2020c) *Guidelines 05/2020 on consent under Regulation 2016/679* [Online]. Brussels: European Data Protection Board. Available at: https://www.edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf (Accessed: 30 January 2025).

EDPB (2020d) *Guidelines 07/2020 on the concepts of controller and processor in the GDPR*. Brussels: European Data Protection Board [Online]. Available at: https://edpb.europa.eu/sites/default/files/consultation/edpb_guidelines_202007_controllerprocessor_en.pdf (Accessed: 30 January 2025).

EDPB (2023) *Guidelines 01/2022 on data subject rights – right of access*. Brussels: European Data Protection Board [Online]. Available at: https://www.edpb.europa.eu/system/files/2023-04/edpb_guidelines_202201_data_subject_rights_access_v2_en.pdf (Accessed: 30 January 2025).

ENISA (2017) *Privacy and data protection in mobile applications – a study on the app development ecosystem and the technical implementation of the GDPR*. European Union Agency for Network and Information security [Online]. Available at: https://www.enisa.europa.eu/publications/privacy-and-data-protection-in-mobile-applications (Accessed: 31 January 2025).

Fan, M., Yu, L., Chen, S. et al (2020) 'An empirical evaluation of GDPR compliance violations in Android mHealth apps', in *2020 IEEE 31st International Symposium on Software Reliability Engineering (ISSRE)*, IEEE, pp. 253–264.

Frankenreiter, J. (2022) 'Cost-based California effects', *Yale Journal on Regulation*, 39(3), pp. 1155–1217.

Galligan, D.J. (2010) *Legal theory and empirical research*. Oxford: Oxford University Press.

Ganglmair, B., Krämer, J. and Gambato, J. (2024) 'Regulatory compliance with limited enforceability: evidence from privacy policies', *ZEW Discussion Paper No. 24-012* [Preprint Online]. Available at: https://doi.org/10.2139/ssrn.4774514 (Accessed: 30 January 2025).

Gardner, J., Feng, Y., Reiman, K. et al (2022) 'Helping mobile application developers create accurate privacy labels', in *2022 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, IEEE, pp. 212–230.

Georgieva, L. and Kuner, C. (2020) 'Article 9 processing of special categories of personal data' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 365–384.

'Google Spain SL and Google Inc. v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González' (2014) Case no. C-131/12. *European Court of Justice*, ECLI:EU:C:2014:317 [Online]. Available at: https://eur-lex.europa.eu/legal-content/DE/TXT/?uri=CELEX:62012CJ0131 (Accessed: 31 January 2025).

Hijmans, H. (2020) 'Article 1 subject-matter and objectives', in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 48–59.

Hildebrandt, M. (2020) 'Privacy and data protection', in Hildebrandt, M. (ed.) *Law for computer scientists and other folk*. Oxford: Oxford University Press, pp. 99–162.

Internet Archive (2024) *Wayback machine* [Online]. Available at: https://web.archive.org/ (Accessed: 28 April 2024).

Kelley, P.G., Bresee, J., Cranor, L.F. et al (2009) 'A "nutrition label" for privacy', in *Proceedings of the 5th Symposium on Usable Privacy and Security - SOUPS '09. the 5th Symposium*, ACM Press, pp.1-12.

Kollnig, K., Binns, R., Dewitte, P. et al (2021) 'A fait accompli? An empirical study into the absence of consent to {third-party} tracking in Android apps', in *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)* [Online]. Available at: https://www.usenix.org/system/files/soups2021-kollnig.pdf (Accessed: 30 January 2025).

Kollnig, K., Binns, R., Van Kleek, M. et al (2021) 'Before and after GDPR: tracking in mobile apps', *Internet Policy Review*, 10(4) [Online]. Available at: https://doi.org/10.14763/2021.4.1611 (Accessed: 30 January 2025).

Kollnig, K., Shuba, A., Van Kleek, M. et al (2022) 'Goodbye tracking? Impact of iOS app tracking transparency and privacy labels', in *2022 ACM Conference on Fairness, Accountability, and Transparency. FAccT '22*, ACM, pp. 508–520.

Kotschy, W. (2020) 'Article 6 lawfulness of processing' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 321–344.

Krämer, J. (2024) 'The death of privacy policies: how app stores shape GDPR compliance of apps', *Internet Policy Review*, 13(2) [Online]. Available at: https://doi.org/10.14763/2024.2.1757 (Accessed: 30 January 2025).

Kranenborg, H. (2020) 'Article 17 right to erasure ("right to be forgotten")' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 475–484.

Kröger, J.L., Raschke, P. and Bhuiyan, T.R. (2019) 'Privacy implications of accelerometer data: a review of possible inferences', in *Proceedings of the 3rd International Conference on Cryptography, Security and Privacy. ICCSP*, ACM, pp. 81–87.

Kuner, C., L.A. Bygrave, and C. Docksey (eds) (2020) *The EU General Data Protection Regulation (GDPR): a commentary*. Oxford: Oxford University Press.

Kyi, L., Shivakumar, S. A., Santos, C. T. et al (2023) 'Investigating deceptive design in GDPR's legitimate interest', in *Proceedings of the 2023 CHI Conference on Human Factors in Computing Systems. CHI '23*, ACM, pp. 1–16.

Li, W., Li, Z., Li, W., Zhang, Y., & Li, A. (2025). 'Mapping the empirical literature of the GDPR's (In-) effectiveness: A systematic review', in *Computer Law & Security Review*, *57*, 106129 [Online]. Available at: https://doi.org/10.1016/j.clsr.2025.106129 (Accessed: 9 May 2025).

Linden, T., Khandelwal, R., Harkous, H. et al (2019) 'The privacy policy landscape after the GDPR'. arXiv [Online]. Available at: https://doi.org/10.48550/arXiv.1809.08396 (Accessed: 30 January 2025).

Machuletz, D. and Böhme, R. (2020) 'Multiple purposes, multiple problems: a user study of consent dialogs after GDPR', *Proceedings on Privacy Enhancing Technologies*, 2020(2), pp. 481–498.

Mangini, V., Tal, I. and Moldovan, A.-N. (2020) 'An empirical study on the impact of GDPR and right to be forgotten – organisations and users perspective', in *Proceedings of the 15th International Conference on Availability, Reliability and Security. ARES 2020*, ACM, pp. 1–9.

Matte, C., Bielova, N. and Santos, C. (2020) 'Do cookie banners respect my choice?: Measuring legal compliance of banners from IAB Europe's transparency and consent framework', in *2020 IEEE Symposium on Security and Privacy (SP)*, IEEE, pp. 791–809.

'Meta Platforms v. Bundeskartellamt' (2023) Case no. C-252/21. *European Court of Justice*, ECLI:EU:C:2023:674 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62021CJ0252 (Accessed: 31 January 2025).

Nguyen, T.T., Backes, M. and Stock, B. (2022) 'Freely given consent?: Studying consent notice of third-party tracking and its violations of GDPR in Android apps', in *Proceedings of the 2022 ACM SIGSAC Conference on Computer and Communications Security. CCS '22*, ACM, pp. 2369–2383.

Nouwens, M., Liccardi, I., Veale, M. et al (2020) 'Dark patterns after the GDPR: scraping consent pop-ups and demonstrating their influence', in *Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems. CHI '20*, ACM, pp. 1–13.

Parker, L. Halter, V., Karliychuk, T. et al (2019) 'How private is your mental health app data? An empirical study of mental health app privacy policies and practices', *International Journal of Law and Psychiatry*, 64, pp. 198–204.

'Patrick Breyer v. Bundesrepublik Deutschland' (2016) Case no. C-582/14. *European Court of Justice*, ECLI:EU:C:2016:779 [Online]. Available at: https://eur-lex.europa.eu/legal-content/DE/ALL/?uri=CELEX:62014CJ0582 (Accessed: 31 January 2025).

Polčák, R. (2020) 'Article 12. Transparent information, communication and modalities for the exercise of the rights of the data subject', in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 398-412.

Quinn, P. and Malgieri, G. (2021) 'The difficulty of defining sensitive data – the concept of sensitive data in the EU data protection framework', *German Law Journal*, 22(8), pp. 1583–1612.

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (Text with EEA relevance)' (2016) *Official Journal* L 119, 4 May, pp. 1–88, [Online]. Available at: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 30 January 2025).

Rodriguez, D., Yang, I., del Alamo, J. M. et al (2024) 'Large language models: a new approach for privacy policy analysis at scale', *Computing* [Preprint Online]. Available at: https://doi.org/10.1007/s00607-024-01331-9 (Accessed: 30 January 2025).

Rupp, E., Syrmoudis, E. and Grossklags, J. (2022) 'Leave no data behind – empirical insights into data erasure from online services', *Proceedings on Privacy Enhancing Technologies*, 2022(3), pp. 437–455.

Sanchez-Rola, I., Dell'Amico, M., Kotzias, P. et al (2019) 'Can I opt out yet?: GDPR and the global illusion of cookie control', in *Proceedings of the 2019 ACM Asia Conference on Computer and Communications Security. Asia CCS '19*, ACM, pp. 340–351.

Santos, C. Rossi, A., Chamorro, L. S. et al (2021) 'Cookie banners, what's the purpose?: Analyzing cookie banner text through a legal lens', in *Proceedings of the 20th Workshop on Workshop on Privacy in the Electronic Society*. *CCS '21*, ACM, pp. 187–194.

Serveto, M.M. (2020) 'Exercising GDPR data subjects' rights: empirical research on the right to explanation of news recommender systems reports: practitioner's corner', *European Data Protection Law Review (EDPL)*, 6(4), pp. 593–601.

Shipp, L. and Blasco, J. (2020) 'How private is your period?: A systematic analysis of menstrual app privacy policies', *Proceedings on Privacy Enhancing Technologies*, 2020(4), pp. 491–510.

Siapka, A. and Biasin, E. (2021) 'Bleeding data: the case of fertility and menstruation tracking apps', *Internet Policy Review*, 10(4) [Online]. Available at: https://doi.org/10.14763/2021.4.1599 (Accessed: 30 January 2025).

Smits, J.M. (2017) 'What is legal doctrine? On the aims and methods of legal-dogmatic research' in Van Gestel, R., Micklitz, H.-W. and Rubin, E.L. (eds.) *Rethinking legal scholarship: a transatlantic dialogue*. New York: Cambridge University Press, pp. 207–228.

Solove, D.J. (2012) 'Privacy self-management and the consent dilemma', *Harvard Law Review*, 126, pp. 1880-1903

Streinz, T. (2021) 'The evolution of European data law' in Craig, P. and De Búrca, G. (eds.) *The evolution of EU law*. 3rd edn. Oxford: Oxford University Press, pp. 902–937.

Svantesson, D.J.B. (2020) 'Article 3 territorial scope' in Kuner, C. et al (eds.) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 74–99.

'Tietosuojavaltuutettu v. Jehovan todistajat' (2018) Case no. C-25/17. *European Court of Justice*, ECLI:EU:C:2018:551 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0025 (Accessed: 31 January 2025).

Towfigh, E.V. (2014) 'Empirical arguments in public law doctrine: should empirical legal studies make a "doctrinal turn"?', *International Journal of Constitutional Law*, 12(3), pp. 670–691.

'UF and AB v. Land Hesse (Joined party: SCHUFA Holding AG)' (2023) Joined Cases C-26/22 and C-64/22. *Opinion of Advocate General Pikamäe*, ECLI:EU:C:2023:222 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62022CJ0026 (Accessed: 31 January 2025).

'Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein v. Wirtschaftsakademie Schleswig-Holstein GmbH' (2018) Case no. C-210/16. *European Court of Justice*, ECLI:EU:C:2018:388 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62016CC0210 (Accessed: 31 January 2025).

Utz, C., Degeling, M., Fahl, S. et al (2019) '(Un)informed consent: studying GDPR consent notices in the field', in *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*. *CCS '19*, ACM, pp. 973–990.

'Verbraucherzentrale Bundesverband e.V. v. Planet49 GmbH' (2019) Case no. C-673/17, *European Court of Justice*, ECLI:EU:C:2019:801 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:62017CJ0673 (Accessed: 31 January 2025).

Wagner, I. (2023) 'Privacy policies across the ages: content of privacy policies 1996–2021', *ACM Transactions on Privacy and Security*, 26(3), pp. 1–32.

Waldman, A.E. (2020) 'Cognitive biases, dark patterns, and the "privacy paradox"', *Current Opinion in Psychology*, 31, pp. 105–109.

Waldman, A.E. (2021) *Industry unbound: the inside story of privacy, data, and corporate power*. Cambridge, New York: Cambridge University Press.

Zanfir-Fortuna, G. (2020) 'Article 13 information to be provided where personal data are collected from the data subject' in Kuner, C. et al (eds) *The EU General Data Protection Regulation (GDPR)*. New York: Oxford University Press, pp. 413–433.

Zhang, S., Feng, Y., Yao, Y. et al (2022) 'How usable are iOS app privacy labels?', *Proceedings on Privacy Enhancing Technologies*, 2022(4), pp. 204–228.

The European Health Data Space: The Next Step in Data Regulation

Lisa Markschies

Abstract

The European Health Data Space (Regulation (EU) 2025/327, EHDS) is an ambitious regulatory project concerning the accessibility of health data. The rules established through this initiative can play a crucial role in addressing the currently fragmented state of digitalisation in healthcare across Member States. Major changes occur in the area of primary use of health data. By granting individuals more autonomy over their electronic health records, the EHDS ensures that patients can access, add, rectify and manage their health records more easily. This also provides healthcare professionals with a greater understanding of a patient's medical history, thus improving treatment quality, especially in cross-border scenarios. Furthermore, the EHDS creates a novel framework for the secondary use of health data, mainly for research, innovation and policymaking. It does so by stipulating specific cases of secondary use for which different categories of data can be accessed. If all criteria are fulfilled, a data permit will be issued. The EHDS establishes a set of rules and guidelines for such application processes. However, the implementation of the EHDS raises complex questions, particularly regarding its relationship with the General Data Protection Regulation and the resulting legal conflicts. Additionally, the risk of national fragmentation in interpretation and application of the EHDS could hinder its effectiveness. Despite these challenges, the EHDS could represent an important step towards harnessing the vast potential of health data within the European Union. With its focus on empowerment of individuals, improved healthcare, and research facilitation, the EHDS might transform European healthcare systems and drive innovation in the sector. If successful, the initiative could possibly shape future data-sharing practices and influencing the development of other European data spaces

1. Introduction

The COVID-19 pandemic has thrown an alarming spotlight on the problems facing modern European healthcare systems: often insufficiently digitalised health authorities, a lack of reliable data, and inadequate international cooperation (European Commission, Directorate-General for Health and Food Safety, 2022). Moreover, Europe has long since ceased to lead the way in the development of innovative pharmaceuticals (Horgan et al, 2022, p. 3). At the same time, vast amounts of health data are collected every day through various methods, but often remain unused. Indeed, just think of the information that doctors routinely collect about their patients or the amount of data that fitness applications collect from smartwatches. Here, existing potential within the EU is not being sufficiently utilised. This imbalance has also been recognised by European legislators, who wish to remedy the situation with by establishing a European Health Data Space (Regulation (EU) 2025/327, EHDS). On the one hand, this will establish a new framework for the primary use of health data so as to provide patients with increased autonomy over their own data and healthcare professionals with better information for their treatment (especially in the context of cross-border treatments). On the other, the EHDS will establish an access right to health data for secondary uses – in particular, research.

After a brief description of the legislative history, this chapter seeks to show the new law's structure. To this end, the regulatory regime of the new primary and secondary use are outlined. Subsequently, existing uncertainties and difficulties in the Regulation's implementation are highlighted through pertinent examples. At its close, the chapter ventures an outlook and examines the extent to which the EHDS is suitable as a model for other sectoral data spaces.

2. Legislative history

As with the Data Act and the Data Governance Act,[1] the origins of the EHDS can be traced back to the Data Strategy published by the European Commission in 2020 (European Commission, 2020a). The strategy intro-

1 For more information on the Data Act, see Chapter 13 'Internet of Things Data within the Context of the Data Act: Between Opportunities and Obstacles' by Prisca von Hagen. For more information on the Data Governance Act, see Chapter 11 'The Data Governance Act – Is "Trust" the key for Incentivising Data Sharing?' by Lucie Antoine.

duces the implementation of nine sector-specific data spaces with the aim to make larger pools of data available (European Commission, 2020a, p. 21). Sectors in which data spaces are envisioned include for example mobility, finance, and agriculture.

It may well have been the impact of the COVID-19 pandemic that prompted the establishment of a European health data space as a primary legislative initiative – a goal which also aligns with the declared aim of establishing a European Health Union (European Commission, 2020b). To this end, the European Commission presented a proposal for a European Health Data Space in May 2022 (European Commission, 2022). Existing health data spaces in Member States, particularly in Finland (*Laki sosiaali- ja terveystietojen toissijaisesta käytöstä*, see also: Männikkö et al, 2024), may have served as an inspiration. At the end of 2023, both the European Parliament and Council agreed on a negotiating mandate. This signalled the start of the trialogue negotiations, in which an agreement was reached in March 2024. The EHDS was then voted on by the European Parliament in April 2024, with formal approval from the Council granted in January 2025. I The EHDS was published in the Official Journal of the European Union on 5 March 2025 as Regulation (EU) 2025/327, and enters into force on 26 March 2025. The key parts of the EHDS will enter into application in March 2029.

3. Primary use

The first major innovation introduced by the EHDS concerns the primary use of electronic health data. Primary use refers to "the processing of electronic health data for the provision of healthcare, in order to assess, maintain or restore the state of health of the natural person to whom those data relate, including the prescription, dispensation and provision of medicinal products and medical devices, as well as for relevant social, administrative or reimbursement services" (Art. 2(2)(d) EHDS). Electronic health data within the meaning of this definition include both personal and non-personal data (cf. Art. 2(2)(c) EHDS).

The declared aim in the area of primary use is "to empower individuals to take control of their own health data and to allow its use for better healthcare delivery" (European Commission, 2022b, p. 2). The mechanisms by which this is to be achieved are outlined below.

3.1 More control over the individual's electronic health data

When it comes to achieving the ambitious goal of unlocking the potential of electronic health data, the first step envisioned is to create more data sovereignty for patients. At present, this varies greatly within the EU. While the Nordic and Baltic states already have extensive options for accessing one's own health data, this status quo is far from being established across the EU (European Commission, Directorate-General for Communications Networks, Content and Technology et al, 2023).

This is where the EHDS comes into play. Art. 3 EHDS is key in establishing the right of natural persons to access their electronic health data. Art. 3(1) EHDS stipulates that "natural persons shall have the right to access at least personal electronic health data relating to them that belong to the priority categories referred to in Article 14 and are processed for the provision of healthcare". Moreover, Art. 7 EHDS grants a right to data portability. A natural person can request healthcare providers to transmit the data to another healthcare provider (Art. 7(1) EHDS) or a to a clearly identified recipient in the social security or reimbursement services sector (Art. 7(3) EHDS).

Furthermore, the EHDS ensures that natural persons have the opportunity to influence the data that is stored about them. Specifically, this means that they can rectify incorrect data and insert missing data, Arts. 5 and 6, Recitals 12 and 13 EHDS. If data has been added in such a way, it will be clearly distinguishable to take account of the fact that the information may be less reliable than that of healthcare professionals (Art. 5 EHDS).

It is also possible for patients to make the reversible decision to block certain, often sensitive, information from third parties. Especially in the areas of sexual or mental health, this is often of great importance to those affected. In such cases, however they should be informed of the possible risks associated with such decisions and the incomplete datasets that result from them. However, an exception applies to "protect vital interests in emergency situations", (Art. 8, Recital 17 EHDS). In addition, the Member States are free to enact such a right even without an emergency override (Recital 18 EHDS). In order to have effective control over their own health data, Art. 9 EHDS standardises a natural person's right to information about the healthcare providers who have been granted access to their data.

Many of these rights have already been laid out in principle in the General Data Protection Regulation (GDPR). For example, Arts. 15–22 of

the GDPR grant the right to access by the data subject (Art. 15 GDPR), the right to rectification (Art. 16 GDPR), and the right to data portability (Art. 20 GDPR). The rights introduced by the EHDS are therefore ultimately more of a concretisation (Petri, 2022, p. 418) or an add-on (EDPB-EDPS, 2022, para. 47). As a result, the exact relationship between the EHDS and GDPR must also be further explored (EDPB-EDPS, 2022, para. 47; see also Section 5).[2]

3.2 Better treatment through better data

The improved data accessibility in the area of primary use is intended to ultimately lead to more needs-based medical treatment (Recital 19 EHDS). Practitioners in Member States with low levels of digitalisation in the medical sector are currently often faced with incomplete documentation of patients' health histories. Obtaining relevant information frequently involves a considerable amount of administrative work and time. Therefore, in Art. 11, the EHDS establishes a possibility for healthcare professionals to access the electronic health data of their patients. However, the above-mentioned restrictions that natural persons can impose regarding access to their health data still apply.

Special attention is also paid to the cross-border flow of data. This is intended to ensure the possibility of continuous treatment when travelling or moving to another Member State, cf. Art. 11(2) and Recital 33 EHDS. For example, if a Dutch tourist suffers a broken leg while on a skiing holiday in Austria and receives surgery there, the doctor providing follow-up treatment in the Netherlands can access the crucial findings and X-ray images. Currently, a direct and safe health data transfer from one country to another fails due to a lack of interoperability and a missing legal framework.

3.3 Data access made easy?

According to Art. 3(1) EHDS, patients must be able to access their health data immediately, free of charge, and in an easily readable, commonly used format, which is also necessary for access for treatment purposes. Due to the high sensitivity of the data, a secure infrastructure must be created for

2 For more information on the GDPR, see Chapter 14 'EU Data Protection Law in Action: Introducing the GDPR' by Julia Krämer.

this purpose. Art. 4 EHDS obliges Member States to create health data access services. In Chapter III, the EHDS also establishes rules and standards against which those EHR systems will be measured in future. This includes, for example, requirements for both the security and interoperability of the systems, with the aim of fostering a genuine internal market for such systems (Recitals 1, 36, 41, and 110 EHDS).

It should also be noted that, as seen above, inconsistent systems in the various Member States could lead to access to health data failing due to technical hurdles, particularly in the case of cross-border treatment. Accordingly (and pursuant to Art. 23 EHDS), the MyHealth@EU service is to be further expanded, and national contact points created. This will enable access to prescriptions abroad, as well as to patient summaries.

4. Secondary use

The regulatory regime of the EHDS promises to foster innovation in the area of secondary use. According to Art. 2(2)(e) EHDS, secondary use is understood as "the processing of electronic health data for the purposes set out in Chapter IV of this Regulation, other than the initial purposes for which they were collected or produced". As such, this is a use of data that does not serve the original healthcare provision, but rather subsequent, additional purposes.

Access to health data is currently difficult, predominantly due to a fragmented legal landscape, both at Member State and EU-wide levels (European Commission, Directorate-General for Health and Food Safety et al, 2022, Kühling and Schildbach, 2024). The EHDS now creates a standardised legal framework for the secondary use of electronic health data.

4.1 Application process

The EHDS introduces a new system for organising access to health data. Unlike the Data Act (DA; see Art. 4(13), (14), Art. 6(1), Art 8(1) DA), the EHDS does not rely on contractual solutions. Instead, so-called data permits are to be issued. To obtain such a permit, in accordance with Art. 67 EHDS, an application for data access can be submitted to a national health data access body – according to Art. 67(1) EHDS, any natural or legal person is eligible to apply. The article also specifies a range of information

that the applicant must provide. The national data access body then checks the requirements in accordance with Art. 68 EHDS, particularly in terms of whether one of the purposes specified in Art. 53 EHDS (see Section 4.2) applies and whether the requested data is necessary for this purpose. If so, a data permit will be issued. Access to the data is granted by the health data access bodies in a secure processing environment (Art. 73 EHDS). The Commission's original proposal also consisted of a simplified application process from a single data holder (Art. 49 EHDS-P). The amendments made during the trilogue negotiations will, however, likely result in limited applicability of the provision (Art. 72 EHDS).

The cost regulations established in the EHDS are also interesting to consider, especially compared to the DA, which, like the EHDS, is part of the European Commission's Data Strategy. Costs within the EHDS amount to administrative fees (described in detail in Art. 62 EHDS), meaning that it is not the data themselves for which the applicant must pay, but rather the work that must be conducted to make it accessible. This becomes all the clearer when one considers that the DA refers to "compensation" (Art. 9 DA), which may be subject to FRAND (Fair, Reasonable, and Non-Discriminatory) conditions. The terminology of the EHDS, on the other hand, is based around "fees" (Art. 62 EHDS), which may include compensation for the data holder: "compensation for part of the costs for collecting the electronic health data specifically under this Regulation in addition to the fees that may be charged" (Art. 62(2) EHDS). However, the inclusion of a margin is, in contrast to Art. 9(1) DA, not intended in the EHDS. Consequently, the EHDS does not create a market for electronic health data. This concept is not entirely new as the Open-Data-Directive (ODD)[3] has similar provisions in Art. 6. However, the ODD only applies to public sector information, whereas the EHDS does not distinguish between public and private data (see also Richter, 2018).

3 For more information on the ODD, see Chapter 12 'The Open Data Directive: Potential and Pitfalls for the Social Sciences' by Nik Roeingh and David Wagner.

4.2 Purposes

Art. 53 EHDS lists the purposes for which the access to electronic health data for secondary use can be granted:

(a) public interest in the area of public and occupational health, such as activities for protection against serious cross-border threats to health and public health surveillance or activities ensuring high levels of quality and safety of healthcare, including patient safety, and of medicinal products or medical devices;
(b) policy-making and regulatory activities to support public sector bodies or Union institutions, bodies, offices or agencies, including regulatory authorities, in the health or care sector to carry out their tasks defined in their mandate;
(c) statistics as defined in Article 3, point (1), of Regulation (EU) No 223/2009, such as national, multi-national and Union-level official statistics, related to health or care sectors;
(d) education or teaching activities in health or care sectors at vocational or higher education level;
(e) scientific research related to health or care sectors that contributes to public health or health technology assessments, or ensures high levels of quality and safety of healthcare, of medicinal products or of medical devices, with the aim of benefiting end-users, such as patients, health professionals and health administrators, including:
    (i) development and innovation activities for products or services;
    (ii) training, testing and evaluation of algorithms, including in medical devices, in vitro diagnostic medical devices, AI systems and digital health applications;
(f) improvement of the delivery of care, of the optimisation of treatment and of the provision of healthcare, based on the electronic health data of other natural persons

The list is exhaustive. There is consequently no possibility of gaining access to data for any other purpose, which, due to the sensitive nature of health data, is to be welcomed. Nevertheless, there is already a highly broad range of purposes covered. It is interesting to note that commercial research also constitutes a purpose for which data can be processed for secondary use, as Art. 53(1)(e) EHDS contains no restriction to public research. On the contrary, Recital 61 EHDS explicitly lists privately funded research as well. In the debate surrounding the legislation, the fear was often expressed that

both Big Pharma and Big Tech would have unrestricted access to data (European Digital Rights, 2023, Schipper and Ollivier de Leth, 2024). The extent to which certain actors have gained access to health data under the EHDS will therefore be quite interesting to study once the regulation has come into effect.

4.3 Scope of data that can be accessed

To assess the scope of the rules on secondary use, it is necessary to examine the data for which permits may be issued.

4.3.1 Categories

In accordance with Art. 51 EHDS, a wide range of data can be accessed. The following is an incomplete selection of the collected data to be made available for secondary use by data holders:

(a) electronic health data from EHRs;
(b) data on factors impacting on health, including socio-economic, environmental and behavioural determinants of health;
(f) human genetic, epigenomic and genomic data;
(g) other human molecular data such as proteomic transcriptomic, metabolomic, lipidomic and other omic data;
(h) personal electronic health data automatically generated through medical devices;
(i) data from wellness applications;
(j) data on professional status, and on the specialisation and institution of health professionals involved in the treatment of a natural person;
(o) data from registries for medicinal products and medical devices;
(q) health data from biobanks and associated databases.

According to Art. 50(1) EHDS, there are two groups of health data holders that are exempted from the obligation to make the data outlined in this chapter available. The first group consists of individual researchers and natural persons; the second are legal persons that qualify as micro-enterprises, as defined in Art. 2 of the Annex to Commission Recommendation 2003/361/EC. Here, a micro-enterprise is defined as one which employs fewer than 10 persons and whose annual turnover and/or annual balance sheet total does not exceed 2 million EUR.

The far reaches of the data categories are remarkable. Human genetic, epigenomic, genomic, and other molecular data in particular (Art. 51(1)(f) and (g) EHDS), but also data on socio-economic, environmental, and behavioural determinants of health (Art. 51(1)(b) EHDS) can contain a particularly large amount of information about the natural person from whom they originate. In addition, Art. 51(2) EHDS provides that Member States can add further data categories to this list on a national level. In this context, it is interesting to note that the mandates of the Parliament and the Council have led to several changes that appear minor at first glance but are nevertheless capable of significantly influencing data availability. For example, "social" became "socio-economic determinants of health" (cf. Art. 33(1)(b) EHDS-P, Art. 51(1)(b) EHDS). Compared with the current Art. 53(1)(f) and (g) EHDS, the original Commission draft only included human genetic, genomic, and proteomic data (Art. 33(1)(e) EHDS-P).

Furthermore, the EC's proposal had faced criticisms over privacy concerns, in that data from wellness applications were also covered under Art. 33(1)(f) EHDS-P (EDPB-EDPS, 2022, para. 79–81). However, this criticism was not adopted in the trilogue procedure, meaning that wellness applications are still covered by the law (Art. 51(1)(i).

4.3.2 Patient protection through anonymisation and pseudonymisation

Electronic health data should generally be made available to applicants in anonymised forms (Art. 66(2) EHDS) or, if this is not possible, in pseudonymised forms (Art. 66(3) EHDS). This distinction has consequences, particularly in terms of the scope of the GDPR's application. Anonymised data is not personal, and thus outside the GDPR's scope. In contrast, pseudonymised data, in accordance with Art. 4(4), Recital 26 GDPR, is still considered personal, meaning that the Regulation's regime applies.

Anonymisation or pseudonymisation should occur as early as possible during the process, but must be done at the latest by the health data access body before the data is shared with applicants (Recital 72 EHDS). It should be noted that the enormous increase in computing capacity means that re-identification is now possible with increasingly less effort (Rocher et al, 2019). Since the range of data collected is potentially extremely large (see above), and the nature of health data, it is necessary that anonymisation or pseudonymisation processes function securely and reliably for efficient patient protection to be guaranteed. It is therefore a key point for the

success of the proposed legislation. In order to ensure this, Art. 61(3) EHDS explicitly bans re-identification. After initial criticism that the penalty rules in case of an infringement of this ban stated in the commission proposal were insufficiently clear (EDPB-EDPS, 2022, para. 127), the agreement text now offers more detailed rules: the re-identification of natural persons can lead to a fine of up to 20 million EUR or of up to 4% of the total worldwide annual turnover of the preceding financial year (Art. 64(5)(c) EHDS). It remains to be seen whether this instrument can suitably prevent re-identification, and thus sufficiently guarantee data protection.

4.4 Prohibited secondary uses

Art. 54 EHDS explicitly states purposes that are not permitted in the context of secondary use. The decisive factor here is the protection of natural persons:

(a) taking decisions detrimental to a natural person or a group of natural persons based on their electronic health data; […]
(b) taking decisions in relation to a natural person or groups of natural persons in relation to job offers, offering less favourable terms in the provision of goods or services, including exclusion of such persons or groups from the benefit of an insurance or credit contract, the modification of their contributions and insurance premiums or conditions of loans, or taking any other decisions in relation to a natural person or a group of natural persons which result in discriminating against them on the basis of the health data obtained;
(c) carrying out advertising or marketing activities;
(d) developing products or services that may harm individuals, public health or societies at large […];
(e) carrying out activities in conflict with ethical provisions pursuant to national law.

The categories listed are hardly surprising. For example, the risks of using AI to select job applications are well known (Dinika and Sloane, 2023). In this context, it is conceivable that an applicant could be screened out based on their medical history due to an algorithm predicting long periods of illness-related absences. European legislators also seem to be aware of the risks of medical data being used to adjust insurance premiums to the detriment of consumers. Suppose, for example, that a health insurance

company can access data from a fitness app and concludes that the person in question leads an unhealthy lifestyle. This could result in high costs for the insurance in the long term and, subsequently, entice it to significantly increase this person's insurance premiums. Art. 54(b) EHDS attempts to prevent such developments.

Another danger is the misuse of data relating to reproductive health. This has been discussed in the course of the overturning of *Roe v. Wade* in the USA (Malki et al, 2024). For example, there are a number of apps that enable women to track their periods. This data can also provide information on abortions, possibly endangering women in states with strict anti-abortion laws. Although this problem is currently less imminent in the EU, it should be used as an example of how far-reaching the consequences of malicious use of health data can be for natural persons. Art. 54(a) EHDS provides a general provision for such, or previously unforeseeable, risks. However, it should be noted that the rather vague wording of this Article could also lead to legal uncertainty.

As shown previously, the EHDS constitutes a basis by which various players could access vast amounts of health data. The prohibitions stated in Art. 54 EHDS, together with the option to penalise their infringement pursuant to Art. 64(5)(a) EHDS, could be a central part of ensuring that natural persons are sufficiently protected. Whether this is enough to prevent a misuse of health data remains an open question.

5. To consent or not to consent

Perhaps the most passionately debated issue in the legislative process was the extent to which patient consent is required for the processing of health data for primary and secondary uses. There are three options here. The first and strictest is the opt-in solution, which means that explicit consent must be given. However, this could also be done in a somewhat weakened form by way of broad consent (on the concept of broad consent Cepik, 2021). A second option is to create an opt-out solution, which in turn means that consent is initially assumed, but one can object. Finally, there is also the option of simply not requiring any form of a patient's consent. The model choice likely has an impact on the chances of the EHDS's success. For example, the consent rates of studies using an opt-in procedure for processing for secondary uses are lower than in opt-out scenarios (de Man et al, 2023). It is also remarkable that the consenting study participants are less repre-

sentative of the overall population than in those with an opt-out procedure (de Man et al, 2023). Consequently, the decision to require natural persons to opt-in might result in a less complete dataset with limited applicability. The Commission certainly had these trends in mind when drawing up its legislative proposal. It therefore decided to completely abstain from the need for consent for secondary uses. This led to criticism, particularly from those with data protection in mind (Datenschutzkonferenz, 2023).

After a long struggle (for an overview of the differentiating mandates, (see Salokannel, 2024; Sokol, 2024), it was ultimately agreed that there should be no general opt-out option for primary use, but that Member States should have the possibility of introducing a modified option at a national level (Art. 10 EHDS). While Member States cannot provide a basis for data subjects to opt-out of the creation of an EHR, they can provide rules that allow the data subject to block access for primary use altogether (Sokol, 2024). For example, Germany has followed a similar approach and established such options with the introduction of the *Gesetz zur Beschleunigung der Digitalisierung des Gesundheitswesens* in the existing *Sozialgesetzbuch* (§§ 342, 353 SGB V, Kühling and Schildbach, 2024).

In the context of secondary use, Art. 71 EHDS introduced an opt-out option. According to this, patients should be able to object to the use of their data for secondary purposes at any time and without giving reasons. This represents a compromise between protecting patients' rights and achieving the goal of containing an as-complete-as-possible dataset.

6. Remaining questions

Even after the adjustments to the European Commission's proposal in the trilogue negotiations, there are still unanswered questions about the implementation of the EHDS that could significantly hinder its success. Some of them are presented here as examples.

6.1 Relation to the GDPR

The EHDS is just one building block in an abstract web of European data regulations. In particular, its relationship to the GDPR still raises a number of questions.

Few forms of data are as sensitive as health data. Accordingly, Art. 4(1) GDPR constitutes health data as personal data. This is especially true for

the primary use scenarios described earlier. Whenever health data are not anonymised (see Section 4.3), the processing of pseudonymised data also falls under the scope of the GDPR (see Art. 2(1)). As the relationship between the two legal acts is controversial in many places, only a few open questions will be addressed here.

The processing of personal data always requires a legal basis, according to Art. 6(1) GDPR. Health data is also a special category of personal data pursuant to Art. 9(1) GDPR and is therefore subject to stricter rules. The EHDS bases the processing of health data for secondary purposes on Art. 9(2) (g)–(j) GDPR (cf. Recital 52 EHDS). However, it is doubtful whether this can really be sufficient in view of the sensitivity of this data (Slokenberga, 2022).

The GDPR also stipulates that the principle of data minimisation must be met when processing personal data, which requires such data to be "adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed" (Art. 5(1)(c) GDPR). However, this is not the case when the data is specifically passed on to the health data access bodies and is only taken into account in the context of subsequent anonymisation (Petri, 2022, p. 418).

Another aspect that raises questions is the fact that the EHDS could deviate from Art. 14 GDPR. Indeed, Art. 38(2) EHDS-P stipulates that:

> Health data access bodies shall not be obliged to provide the specific information under Article 14 of Regulation (EU) 2016/679 to each natural person concerning the use of their data for projects subject to a data permit and shall provide general public information on all the data permits issued pursuant to Article 46.

Although this is possible in principle in accordance with Art. 14(5)(b)–(c) GDPR, a potential restriction of the rights of natural persons has been criticised (EDPB-EDPS, 2022, para. 25f.). For this reason, that wording can no longer be found in the corresponding Art. 58 of the final text. However, no obligation corresponding to Art. 14 GDPR has been introduced. Whether this is sufficient from a data protection standpoint is questionable.

6.2 Differences between the Member States

It is also unclear to what extent any national fragmentation in the handling of the law may affect its success. This starts with the primary use of health data, as some countries will make use of the option to block access to the EHR, such as Germany (see Section 5). In addition, the health data

access bodies are under the control of the Member States. This means that the establishment of these access bodies progresses at different speeds, and the processing times for applications could also vary greatly. This in turn might open up the possibility of forum shopping if certain Member States process applications more quickly or interpret the requirements to issue a data permit less strictly. In this context, it is also unclear to what extent the fee system will be harmonised. While fees are broken down transparently on the Finnish access body's website (Findata, 2024), it remains to be seen how other Member States will handle this in future. It has also already been pointed out that the issuing practice can differ between Member States (Staunton et al, 2024). The Joint Action Towards the European Health Data Space (TEHDAS), which consists of 30 European states, has set itself the task of eliminating remaining uncertainties resulting from the different handling of the EHDS at national levels (TEHDAS, 2022). The project has now reached the second phase (TEHDAS 2), yet to what extent harmonisation will ultimately be possible remains unclear. Additionally, a uniform level of cybersecurity must be guaranteed by all Member States, especially considering the data's sensitivity.

6.3 Garbage in/garbage out?

The quality of the research that can be conducted with the data that is now made accessible is only as good as the data itself (Kilkenny and Robinson, 2018). Accordingly, it is important to bear in mind that data do not constitute a panacea ("Dataism": van Dijck, 2014; Haggart and Tusikov, 2023, p. 117). In order for the EHDS's objectives to be achieved, especially in the area of secondary use, clear formats and designations are needed to facilitate data exchanges (TEHDAS, 2022, 6.10). It is also necessary to ensure high data quality (TEHDAS, 2022, 6.11). Only then can truly meaningful research be conducted with the data. The introduction of a label for data quality that is also interlinked with the diligence obligations for data governance in Art. 10 AI Act is envisaged in Art. 78 EHDS and could contribute to more high-quality data.

7. Outlook

The EHDS is the first of its kind. Although the list of data spaces envisaged in the future is long, these are not necessarily accompanied by a legally

enshrined right of access to the respective data, but are often limited to the de facto establishment of a sharing infrastructure (an overview can be found at European Commission, 2024). It should be noted that there is also an initial proposal for a Financial Data Access Regulation (FIDA) in the financial sector (European Commission, 2023). However, there are significant differences in the regulatory structure: for example, data is transferred from holder to user following a request from a costumer (see Art. 4 FIDA). In practice, this is done through data access permission dashboards (Art. 5(3)(d), Recital 21 FIDA). The FIDA mechanism differs considerably from that of the EHDS, where data is collected across the board and made available by health data access bodies. Whether the EHDS concept can and should also be transferred to other data spaces will be a point of discussion in the future. However, it must be taken into account that the interests are not necessarily the same as those of the healthcare sector. Ultimately, much will depend on whether the EHDS proves successful or fails to achieve its ambitious goals.

References

Cepik, M. (2021) 'Broad Consent: Die erweiterte Einwilligung in der Forschung', *Zeitschrift für Datenschutz-Aktuell*, 10(05214).

Council of the European Union (2024*) Proposal for a Regulation on the European Health Data Space - Analysis of the final compromise text with a view to agreement.* Interinstitutional File: 2022/0140(COD). Luxembourg: Publications Office of the European Union. [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0197 (Accessed: 5 February 2025).

Datenschutzkonferenz. (2023) *Stellungnahme der Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder vom 27. März 2023. Nutzung von Gesundheitsdaten braucht Vertrauen – Der Europäische Gesundheitsdatenraum darf das Datenschutzniveau der Datenschutz-Grundverordnung nicht aushöhlen* [Online]. Available at: https://datenschutzkonferenz-online.de/media/st/2023-03-27_DSK-Stellungnahme_EHDS.pdf (Accessed: 5 February 2025).

De Man, Y., Wieland-Jorna, Y., Torensma, B., de Wit, K., Francke, A. L., Oosterveld-Vlug, M. G. and Verheij, R. A. (2023) 'Opt-in and opt-out consent procedures for the reuse of routinely recorded health data in scientific research and their consequences for consent rate and consent bias: systematic review. *Journal of Medical Internet Research*, 25, e42131 [Online]. Available at: https://doi.org/10.2196/42131 (Accessed: 5 February 2025).

Dinika, A.-A. and Sloane, M. (2023) 'AI and inequality in hiring and recruiting: a field scan', in *Proceedings of the Weizenbaum Conference 2023: AI, Big Data, Social Media, and People on the Move* [Online]. Available at: https://doi.org/10.34669/wi.cp/5.3 (Accessed: 5 February 2025).

European Commission (2020a) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. A European strategy for data.* COM(2020) 66 final. Luxembourg: Publications Office of the European Union [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0066 (Accessed: 5 February 2025).

European Commission (2020b) *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Building a European Health Union: Reinforcing the EU's resilience for cross-border health threats.* COM(2020) 724 final. Luxembourg: Publications Office of the European Union [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0724 (Accessed: 5 February 2025).

European Commission (2022) *Proposal for a Regulation of the European Parliament and of the Council on the European Health Data Space.* COM(2022) 197 final. Luxembourg: Publications Office of the European Union [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0197 (Accessed: 5 February 2025).

European Commission (2023) *Proposal for a Regulation of the European Parliament and of the Council on a framework for financial data access and amending Regulations (EU) No 1093/2010, (EU) No 1094/2010, (EU) No 1095/2010 and (EU) 2022/2554.* 2023/0205(COD). Publications Office of the European Union [Online]. Available at: https://eur-lex.europa.eu/procedure/EN/2023_205 (Accessed: 5 February 2025).

European Commission (2024). *Commission Staff Working Document on Common European Data Spaces*. SWD(2022) 45 final. Luxembourg: Publications Office of the European Union [Online]. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/83562 (Accessed: 5 February 2025).

European Commission, Directorate-General for Communications Networks, Content and Technology, Deimel, L., Hentges, M., and Latronico, V. et al (2023) *Digital decade e-Health indicators development: final report*. CNECT/LUX/2022/MVP/0027. Luxembourg: Publications Office of the European Union [Online]. Available at: https://data.europa.eu/doi/10.2759/530348 (Accessed: 5 February 2025).

European Commission, Directorate-General for Health and Food Safety (2022) *State of health in the EU: companion report 2021*. Luxembourg: Publications Office of the European Union [Online]. Available at: https://data.europa.eu/doi/10.2875/835293 (Accessed: 5 February 2025).

European Commission, Directorate-General for Health and Food Safety, Lupiáñez-Villanueva, F., Gunderson, L. and Vitiello, S. et al (2022) *Study on health data, digital health and artificial intelligence in healthcare*. Luxembourg: Publications Office of the European Union [Online]. Available at: https://data.europa.eu/doi/10.2875/702007 (Accessed: 5 February 2025).

European Data Protection Board, European Data Protection Supervisor [EDPB-EDPS] (2022) *EDPB-EDPS Joint Opinion 03/2022 on the Proposal for a Regulation on the European Health Data Space*. Luxembourg: Publications Office of the European Union [Online]. Available at: https://op.europa.eu/s/zIy6 (Accessed: 5 February 2025).

European Digital Rights (2023) *EU plans allow Big Tech to exploit your medical records, without permission*. European Digital Rights [Online]. Available at: https://edri.org/our-work/eu-plans-allow-big-tech-to-exploit-your-medical-records-without-permission/ (Accessed: 5 February 2025).

Findata. (2024) *Pricing*. Findata [Online]. Available at: https://findata.fi/en/pricing/ (Accessed: 5 February 2025).

Haggart, B. and Tusikov, N. (2023) *The new knowledge. Information, data and the remaking of global power*. London: Rowman & Littlefield Publishers.

Horgan, D., Spanic, T., Apostolidis, K., Curigliano, G., Chorostowska-Wynimko, J., Dauben, H. P., Lal, J. A., Dziadziuszko, R., Mayer-Nicolai, C., Kozaric, M., Jönsson, B., Gutierrez-Ibarluzea, I., Fandel, M. H. and Lopert, R. (2022) 'Towards Better Pharmaceutical Provision in Europe-Who Decides the Future?', *Healthcare*, 10(8), 1594 [Online]. Available at: https://doi.org/10.3390/healthcare10081594 (Accessed: 5 February 2025).

Kühling, J. and Schildbach, R. (2024) 'Datenschutzrechtliche Spielräume für eine forschungsfreundliche digitale Gesundheitsversorgung – von DSGVO, SGB etc. zur EHDS-VO und zum GDNG', *Zeitschrift für Digitalisierung und Recht*, 4(1), pp. 1-26.

Malki, L. M., Kaleva, I., Patel, D., Warner, M. and Abu-Salma, R. (2024) 'Exploring privacy practices of female mHealth apps in a post-Roe world', *Proceedings of the CHI Conference on Human Factors in Computing Systems (CHI '24)*, 576, pp. 1–24.

Kilkenny, M.F. and Robinson K.M. (2018) 'Data quality: "Garbage in – garbage out"', *Health Information Management Journal.* 47(3), pp. 103–105.

Männikkö, V., Förger, K., Urhonen, H., Tikkanen, J., Antikainen, S. and Munukka, J. (2024) 'Overview of Finnish national patient data repository for research on medical risk assessment', *TechRxiv* [Online]. Available at: https://doi.org/10.36227/techrxiv.170862135.56728930/v1 (Accessed: 5 February 2025).

Petri, T. (2022) 'Die primäre und sekundäre Nutzung elektronischer Gesundheitsdaten - Zum Vorschlag der EU-Kommission für einen Europäischen Gesundheitsdatenraum', *Datenschutz und Datensicherheit*, 46(7), pp. 413-418.

'Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847 (Text with EEA relevance)', *Official Journal* L 2025/327, 5 March, Available at: http://data.europa.eu/eli/reg/2025/327/oj (Accessed: 26 March 2025).

Richter, H. (2018) 'Open science and public sector information – reconsidering the exemption for educational and research establishments under the Directive on re-use of public sector information', *Journal of Intellectual Property, Information Technology and E-Commerce Law*,9(1), pp. 51–74.

Rocher, L., Hendrickx, J.M. and de Montjoye, YA. (2019) 'Estimating the success of re-identifications in incomplete datasets using generative models', *Nature Communications*, 10, 3069 [Online]. Available at: https://doi.org/10.1038/s41467-019-10933-3 (Accessed: 5 February 2025).

Salokannel, M. (2024) *Opting-in or -out or not at all: secondary use of health data in the EHDS framework*. European Law Blog [Online]. Available at: https://doi.org/10.21428/9885764c.83333982 (Accessed: 5 February 2025).

Schipper, I. and Ollivier de Leth, D. (2024) *EU health data law rolls out the red carpet for Big Tech. European Parliament should vote against the EHDS in its current form.* Centre for Research on Multinational Corporations (SOMO) [Online]. Available at: https://www.somo.nl/eu-health-data-law-rolls-out-the-red-carpet-for-big-tech/ (Accessed: 5 February 2025).

Slokenberga, S. (2022) 'Scientific research regime 2.0?: How the proposed EHDS Regulation may change the GDPR Research Regime. *Technology and Regulation*, pp. 135–147. Available at: https://doi.org/10.26116/techreg.2022.014

Sokol, T. (2024) 'European Health Data Space, use of data and data subjects' control over their own health data: can an opt-out restore the balance?' *European Journal of Health Law*, pp. 1–24.

Staunton, C., Shabani, M., Mascalzoni, D., Mežinska, S. and Slokenberga, S. (2024) 'Ethical and social reflections on the proposed European Health Data Space', *European Journal of Human Genetics*, 32, pp. 498–505.

Joint Action Towards the European Health Data Space [TEHDAS] (2022) *Report on secondary use of health data through European case studies.* TEHDAS [Online]. Available at: https://tehdas.eu/app/uploads/2022/08/tehdas-report-on-secondary-use-of-health-data-through-european-case-studies-.pdf (Accessed: 5 February 2025).

Van Dijck, J. (2014) 'Datafcation, Dataism and Dataveillance: big data between Scientifc paradigm and ideology', *Surveillance and Society*, 12(2), pp. 197–208.

The CRA and the Challenges of Regulating Cybersecurity in Open Environments: The Case of Free and Open Source Software

Lucas Lasota

Abstract

This chapter provides a bird's eye view of the Cyber Resilience Act (CRA) from the perspective of the policy, legal, and socio-economic elements that prompted regulators to intervene in the digital markets. Its focus centres on the market and regulatory failures regarding cybersecurity, treating the regulatory path taken by the EU as a reaction. An interdisciplinary approach is proposed as a methodology for listing the technical aspects of cybersecurity and the nature of vulnerabilities, and balancing economic factors with ethical and legal concerns. A practical context is given with the study case of a stakeholder intervention during the CRA's legislative process: the liability issue raised by Free and Open Source Software (FOSS) stakeholders. The collective intercession of different FOSS organisations galvanised broad changes in the text of the law. This chapter concludes with the recommendation that policymakers should not lose touch with civil society during the implementation phase and monitoring process.

1. Introduction – making cybersecurity a priority for digital markets

Recognising that *any connected device can be maliciously hacked* is one of the hard pills that digital users must swallow nowadays. As the Internet has now spread to over 66% of the world's population (Statista, 2024), and digital products are more pervasive than ever in all spheres of life, a sensation of impotence subtly imposes a perception that it is too late for any adequate reaction by policymakers. This feeling is accentuated when noting that cybercrime involving digital products has cost trillions of euros in recent years (European Commission, 2022a, p. 2), and that current EU legislation does not comprehensively impose mandatory cybersecurity for economic actors. Indeed, securing the vast number of elements in the internet value chain – composed of interconnected devices, encryption,

software and hardware interoperability, and integration of networks and data streams – is one of the significant challenges of the contemporary world.

This sombre attitude stands in stark contrast to the enthusiastically progressive view proposed by the *cyberculture*. After all, *cyberspace* was thought to be a civilising refuge from traditional oppressive state-led forces (Barlow, 1996). Admittedly, as early as the beginning of the 1990s, disenchanted whistleblowers warned about how the *cyber-rhetoric*, with its articulated dichotomous discourse of immunity from sovereignty of traditional state forces, ended up being co-opted by capitalist interests (Curtis, 2016). The resulting neoliberal-style interventionism facilitated an intimate relationship of co-dependence between liberal governments and corporations favouring profitability and dominance over distributed economic welfare and efficiency in digital markets (Powers and Jablonski, 2015). This symbiosis produced a contradictory outcome: an overemphasis on cybersecurity for surveillance and law enforcement that contrasts with a lack of regulatory oversight of corporate control, leading to the persistent, structural market failures in the realm of cybersecurity (European Commission, 2022a, p. 17).

The opposition to the status quo encompasses far-reaching reactions, ranging from voices demanding deep structural reorganisation over the production and ownership of wealth in the digital age to reformist approaches via legislative and regulatory updates (Lasota, 2023). The Cyber Resilience Act (CRA) (Regulation (EU) 2024/2847) emerged from this content, as the European Union (EU) seized the regulatory momentum to complement product safety and liability legislation by forcing tech companies to improve the security of their products through compliance with the CE quality marking.[1] The CRA is the outcome of a regulatory approach which evolved to conceive of cybersecurity as a cross-sector policy for digital markets. This complementary addition to the safety of digital products marks the EU taking a more interventionist approach in digital markets, aiming towards stricter behaviour rules for economic activities (Bygrave, 2024).

This chapter, therefore, seeks to understand the conditions under which the CRA emerged. The editorial contour skips an in-depth legal analysis

1 CE marking indicates that a product has been assessed by the manufacturer and deemed to meet EU safety, health, and environmental protection requirements. For more information, please see Your Europe (2024).

and favours an interdisciplinary approach merging legal, social-economic, and historical analysis. As a portrait of the codification of cybersecurity into law, a particular aspect of the public debate is here reported: the contributions from Free and Open Source Software (FOSS) stakeholders reacting to new, CRA-imposed liability regimes. The choice for this portrayal is relevant. As the CRA's envisioned scope applies to commercialised products with digital elements – from small internet of things (IoT) devices to operating systems and security hardware – the rules necessarily touch both embedded and non-embedded software. Since up to 90% of software developed today has FOSS elements (Nagle et al, 2022, p. 4), the law necessarily relates to FOSS. Nevertheless, as revealed by the fierce reaction from different FOSS stakeholders, the European Commission's 2022 CRA Proposal fell short on understanding the dynamics of the production, distribution, and maintaining of FOSS (BEUC, 2022; Hendrick and Mckeay, 2022; FSFE, 2023; Phipps, 2023; Sander, 2024). The diverse legislative iterations that followed display a valuable dialectical experience among policy makers and FOSS stakeholders, shedding light on the intricacies of the FOSS economy and developing new legal constructions to accommodate the responsibilities tailored for the sector in relation to liability and cybersecurity rules.

The line of argument follows the above-stated objectives. Cybersecurity is presented not only as a technical discipline, but also as a complex social-economic phenomenon with deep political consequences. Then, security vulnerabilities and the efforts required for their mitigation are considered. Later parts dive deeper into the emergence of the CRA as legislation by addressing three topics: how cybersecurity has been historically regulated in the EU, the CRA as a solution for security as a *quality* of digital products, and, finally, a case study of the entanglement of the CRA and FOSS. The concluding remarks reflect on how cybersecurity is negatively affected by corporate influence on fragile communities, and how policymakers and regulators will need to take this reality into consideration when implementing the CRA.

2. Cybersecurity is broader than computer security

Cybersecurity is a broad discipline involving technology, information, and, above all, people developing processes for the security of computer systems (Christen, Gordjin and Loi, 2020). The diverse aspects of creating,

operating, analysing, and testing digital systems involve such subjects as law, policy, ethics, risk management, computer science, networking, and data science (ACM et al, 2017). As a field of endeavour, cybersecurity emerged with mainframe computers in the 1960s as a safeguard for data storage, and grew to include device integrity, infrastructure protection, and internet security (Warner, 2012). In its origins, cybersecurity was practiced in terms of the physical security of devices to prevent theft and sabotage, and document classification to prevent espionage. The Internet increased complexities to new heights: mass connectivity translated into software and devices being presented in all spheres of life, requiring a multidisciplinary approach to encompass the profound risks (DeNardis, 2020).

However, this is not to say that cybersecurity should be seen as an absolute value. More than a matter of individual effort, cybersecurity is a social project. Its multifaceted characteristics cannot, and should not, be oversimplified with binary assumptions of *more is good, less is bad*. Instead, depending on the context, other values may be supportive or conflicting. Overemphasising cybersecurity may violate fundamental values, such as equality, fairness, freedom, or privacy (van de Poel, 2020). At the same time, neglecting cybersecurity could also undermine privacy and safety, and detrimentally impact trust and confidence in digital infrastructure and institutions (Christen et al, 2020, p. 2). For instance, increasing cybersecurity measures for accessing devices by requiring users to provide personal data may decrease their level of privacy. At the same time, the anonymisation of users in a system may create difficulties for monitoring their activities, and thus the security of the whole system (Van de Poel, 2020).

The term *cybersecurity* itself is ideologically charged. Before 1989, discussions instead focused on *computer security*. The word *cyber* originates from *cybernetics* – a transdisciplinary philosophy of the 1940s, but was etymologically linked to security in the 1990s under the auspices of the *cyberculture* (Newitz, 2013). With that, cybersecurity fell under the online-offline dichotomy within the broader concepts of digital libertarian claims that the Internet had to be immune from the regulation of the offline (Barlow, 1996). This mindset permeated the following two decades, creating a regulatory gap between security and safety (as explained in the next sections). Strangely enough, starting in the 2010s, the naming of legislative and regulatory initiatives began to reclaim the term *cyber*, as the denomination of several laws and policies in this chapter illustrates. However, legally speaking, Art. 2(1) of the Cybersecurity Act (2019) defines cybersecurity in the EU as:

"activities necessary to protect network and information systems, the users of such systems, and other persons affected by cyber threats".

The dimensions of cybersecurity are technical, ethical, political, economic, and legal (ACM et al, 2017; Papakonstantinou, 2022). Traditionally, the technical aspects of cybersecurity relate to the protection of such valuable assets as hardware, software, and data by (i) information security and (ii) system security. System security is not limited to information and can refer to so-called digital systems with physical components, such as personal devices or larger equipment used in industrial manufacturing, finance, energy, healthcare and infrastructure. Both aspects comprise the following values (Herrmann and Pridöhl, 2020, pp. 13–14):

Confidentiality: Only authorised users and processes should be able to access or modify the system's data or parameters. Example: encrypting emails and messages so that only intended recipients can read the contents;
Integrity: Accuracy and completeness of the data and the system during their entire lifecycle. Example: implementing measures to detect and prevent unauthorised alterations to files;
Availability: Ensuring that information and resources are accessible to authorised users when needed. Example: deploying redundant servers to keep a website online even during malicious attacks or hardware failures;
Authenticity: Verifying that data and communications are genuine and have not been tampered with. Example: using digital signatures to confirm a document's origin.

The ethical dimension of cybersecurity is multifaceted. Issues prompting ethical consideration include legitimacy of hacking, dilemmas involving vulnerability reporting, access grants, privacy, conflicting attitudes in law enforcement, and encryption (Christen, Gordjin and Loi, 2020).

Due to its inherent focus on power in the information society, cybersecurity raises diverse political issues as well (Guiora, 2017). Such topics as the regulation of information flows, the protection of civil and political rights, privacy, security of government systems, and market issues necessarily invoke political consideration from decision makers. International relations, interstate competition related to technology, economical aspects, internet governance, and national security are also areas in which states, governments, and public agencies have a stake in cybersecurity (Ishikawa and Kryvoi, 2023).

The economic dimension in cybersecurity has been a convergence point in EU law-making. Security services compose an entire industry, ranging from hardware production to software development, consultancy, penetration testing, cyberdefence, and encryption technologies. How economic actors prioritise cybersecurity involves complex trade-offs between security and other values, asymmetries of defence and attack, social gains and losses, and the costs of adopted strategies (Grady and Parisi, 2006). The several market failures involving cybersecurity have been subject to scrutiny from policymakers, and will be analysed further.

Legal and regulatory aspects of cybersecurity can include rules imposed on individuals, organisations, and governments related to the protection of information technology and computer systems (Schreider and Noakes-Fry, 2020). Regulations aim to minimise security risks and enhance protection, as well as determine the legality of security and encryption technologies. Many diverse legal areas fall under the overarching scope of cybersecurity, such as cybercrime, liability and accountability, certification, security of critical infrastructures, and goods (Fuster and Jasmontaite, 2020).

Cybersecurity's corpus of legal and standards frameworks in relation to software products and services took longer to develop and mature than those for safety and privacy *precisely because of* how the above-mentioned elements differentiate cybersecurity from safety and data protection (Vedder, 2019). Product safety is a subset in the larger area of consumer protection and includes procedures to minimise the likelihood of accident or injury (Ruohonen, 2022). Cybersecurity is concerned with diminishing vulnerabilities and protecting against intentional and non-intentional harm caused by human and technical factors and cyberattacks. Cybersecurity measures include human-related preventive activities and technical elements, such as firewalls, anti-virus software, intrusion detection and prevention systems, encryption, and login passwords. In software engineering, cybersecurity includes best practices, guidelines, quality control, and standardisation for securing software and diminishing vulnerabilities (ACM, 2017). However, as the importance of artificial intelligence (AI) and the IoT increases, so too does cybersecurity become more connected to consumer safety and critical industrial infrastructure, as well as to the digital economy and democratic systems (DeNardis, 2020). In its turn, although data protection has similarities and often overlaps with cybersecurity, it has a closer relation to privacy. Cybersecurity and privacy have historically shared a common ground in protecting confidentiality, integrity, and access to data, but many cybersecurity problems have lesser implications for pri-

vacy, and vice versa (Porcedda, 2023, p. 130). For instance, the collection of non-personalised industrial data can be sensitive from a cybersecurity perspective, but has less of an impact on individuals' privacy. Similarly, advertising in social media prompts serious privacy concerns and other social risks, whereas cybersecurity threats can be of lesser concern (Grotto and Schallbruch, 2021).

Prevention and resilience are two foundational elements of cybersecurity. When attacks are not prevented, resilience means withstanding, recovering, and evolving from them (Bendiek et al, 2017, p. 2). Resilience in this sense complements prevention by involving procedures to respond and recover in case of a cyberattack (Bygrave, 2024). Anticipating attacks means understanding vulnerabilities, how they occur, and what is necessary to mitigate them. The following section delves more deeply into these aspects.

3. Vulnerabilities are inescapable in the digital world

When related to software, cybersecurity is considered a *software quality* that spans all stages of the software life cycle (Salvaggio and González, 2023). As such, it refers to software's capabilities to: prevent unauthorised actions in relation to information and other resources of the system; tolerate security-related attacks and violations of the system; and quickly and securely recover from an attack.

Vulnerabilities are failures in these qualities that can be exploited against the system's security policy (Shirey, 2007). Vulnerabilities in software are also characterised by the information asymmetry between creation and detection. Exploitable vulnerabilities have been repeatedly shown to be easy to introduce in the code base, but their detection and remediation are not only difficult, but can take weeks or months (Hendrick and Mckeay, 2022, p. 3). Vulnerabilities are often found in systems composed of multiple components or in the interactions between components and systems. Infections derived from supply chain compromises are one of the most relevant challenges for cybersecurity nowadays (ENISA, 2023, p. 5). However, not all vulnerabilities are necessarily exploited. A *cyberthreat* refers to the hypothetical event wherein an invader or attacker uses the vulnerability (Paulsen and Byers, 2019). Common examples of vulnerabilities include:

Broken authentications: With authentication credentials compromised, identities can be hijacked. Other attacks may trick an authenticated user

into performing an action they did not intend. This, paired with social engineering,[2] can deceive users into providing a malicious actor with sensitive data (Feil and Nyffenegger, 2008);

SQL injections[3] **and malicious scripts (malware)**: Intentional malicious or defective code can be inserted into software to grant unauthorised access to databases, websites, and other assets (Aslan and Samet, 2020);

Misconfiguration and outdated software: A configuration error can be used to violate security. Unpatched or outdated software is a common source of vulnerability exploitation (Mugarza et al, 2020);

Unsecured Application Programming Interfaces (APIs):[4] Due to how APIs can share data and functionalities among connected devices, they can also create a broad attack surface through insufficient monitoring, configuration errors, and excessive data exposure (OWASP, 2019). If an API lacks proper authentication, authorisation, or encryption, it would be vulnerable to attacks and unauthorised data access.

Once a vulnerability is identified, it can either be kept secret or reported. There are ethical, policy, and legal issues to be considered here. Motivations for keeping a vulnerability secret may include its illegal exploitation or planned further legal action. Disclosures can be made publicly or privately in coordination with the software developer. Unreported vulnerabilities – also called *zero days* – may remain unfixed for a long time. Vendors, manufacturers, and developers respond to such reporting in different ways. For instance, they can react positively and expeditiously to fix the issue or disregard the report. Some have even taken a defensive approach and

2 Social engineering in this context refers to manipulations that exploit human error to trick someone into divulging specific information or performing a specific action for fraudulent purposes. "Phishing" is a common example where an attacker sends an email posing as a trusted entity to trick the recipient into clicking a malicious link or providing sensitive information, such as passwords or credit card numbers. More can be found at Wang, Z. Sun, L. and Zhu, H (2020).

3 SQL injections refer to a technique used to attack data-driven applications and systems. SQL is a language used to manage data bases, including access to, and the recording, control, manipulation, and deletion of data. SQL injections allow attackers to interfere with the queries that an application makes to its database. For more, please see OWASP (2025).

4 An application programming interface (API) is a connection between computers or between computer programs. It is a type of software interface, offering a service to other pieces of software.[1] A document or standard that describes how to build such a connection or interface is called an API specification. A computer system that meets this standard is said to implement or expose an API. The term API may refer either to the specification or to the implementation. More at Wikipedia (2025).

retaliated with legal actions. Discoverers may find themselves in a delicate position due to the grey area of the methods used to discover the vulnerability and how it was disclosed (ENISA, 2015, p. 7). Furthermore, keeping vulnerabilities secret or threatening the reporter can be considered immoral and illegal in some cases (van de Poel, 2020). For instance, a company could behave immorally and illegally by offering a bribe to a security engineer who discovered a vulnerability in the system in order to gain time to fix it without alerting its customers. Although there are competing and conflicting interests in disclosures between companies, researchers, the media, and the general public, it is recommended to protect the discoverer by recognising their whistleblower status and creating safeguards for researchers involved in vulnerability and ethical hacking (ENISA, 2022, p. 74). It is also recommended that cybersecurity agencies and governments establish policies fostering responsible disclosures to promote research, discovery, and transparency (ENISA, 2022, p. 8).

Vulnerabilities can be found by testing, auditing, and discovery efforts. Access to source code is helpful for security audits (Hermanowski, 2015). In the case of proprietary software, analyses may involve reverse engineering[5] (Payne, 2002, p. 68). The process for handling vulnerabilities differs by company and organisation, but generally involves detection, assessment, reporting, and mitigation (ENISA, 2015). Once the vulnerability has been detected, it should be assessed to determine the risks and threat levels. Next, it can be directly reported to those affected, as well as in public catalogues. Vulnerabilities in widely deployed products can be included in public databases, such as the "Common Vulnerabilities and Exposures (CVE)", "Open Source Vulnerabilities (OSV)", and "National Vulnerability Database (NVD)" (Townsend, 2024). There they receive a unique identifier (i.e., an alphanumeric code) and a score to reflect the potential risk they represent.[6] Public catalogues serve as reference points for vulnerability management for the general public.

After being discovered, assessed, and reported, vulnerabilities should be fixed. The release and integration of new updates and patches require further scanning, testing, and new iterations to avoid new vulnerabilities. Best practices indicate that organisations should have necessary process

5 Reverse engineering involves analysing a system, software, or device to discover its design, architecture, or code, often to duplicate or enhance the system without access to the original source. For more, see Wikipedia (2025a).

6 See, for example, the CVE process for recording vulnerabilities (CVE, no date).

in place, including responsible teams, short reaction times, and structured schedules, and publish as much information as possible to allow their users to accurately assess any risks to which they may be exposed (ENISA, 2015).

Remediation processes tend to be long and resource-consuming. Due to the impossibility of developing completely flawless software, *security by design* principles are important for saving remediation resources (OWASP, 2020). Managing and resolving vulnerabilities aim to reduce *attack surfaces*, which refer to every point or area in a system where an attacker could attempt to break in, extract data, or cause harm to the system.[7] Surface attack possibilities encompass the various vulnerabilities that attackers can exploit. For instance, in a web application, attack surfaces include user input fields, API endpoints, and network interfaces. If a web application has multiple outdated plugins, each could serve as a potential entry point for attackers to exploit. The existence of vulnerabilities does not necessarily translate into inevitable attack, so a risk assessment is useful for determining its probability and the consequent prioritisation for remediation (NIST, 2012). Risks can be avoided by eliminating the software feature or mitigated by implementing security measures. Risks can be transferred to users or covered by insurance (European Commission, 2022a, p. 10). Risks can also be accepted when a fix cannot be performed because the equipment cannot be replaced (OWASP, 2020, p. 15) or when the choice is made to cover the costs of an attack (Shostack, 2014).

There are several elements to consider in the risk assessment process. For instance, competitive pressure to bring products quickly to market, design factors, and requirements related to energy, power, size, speed, portability, and interoperability are decisive factors for developers and manufacturers when implementing security mechanisms (DeNardis, 2020). As the next section elaborates, industrial policies adopted for the tech sector have caused a market and regulatory failure for cybersecurity. Tracking how the EU regulatory approach reacted can elucidate how the CRA came to fruition.

7 See more at Computer Security Resource Center (no date).

4. From safety to security – understanding the EU's cybersecurity regulatory path

While expansionist policies for the Internet have brought connectivity to over 5 billion users (Statista, 2024), a collateral effect resulted in deprioritising security in favour of availability (ACM, 2017, p. 16; Powers and Jablonski, 2015, p. 22). This prioritisation affected how cybersecurity has been regulated. Although some aspects of computer security have been covered under data protection, national defence, law enforcement, and criminal law, regulation concerning *security as a quality of digital products* has lagged behind, and not accidentally so. Fostered by the waves of economic deregulation in the 1990s and 2000s in the US and EU, manufacturers and vendors of digital products have enlarged profit margins at the cost of better cybersecurity policies, commercialising products with exploitable vulnerabilities, which not only jeopardised the correct functioning of the markets (Lasota, 2023), but also negatively affected fundamental rights and safety (Chiara, 2022).

The neoliberal status quo established in the 1990s dominated the technology industry and boosted a symbiosis between corporations and governments in relation to security policies. The massive surveillance practices revealed by Edward Snowden in 2013 have demonstrated that, especially since 9/11, a *security hyperprevention mindset* has allowed governments and corporations to intervene and operate in many cases outside the law and due process to enforce security mechanisms (Lemke, 2014). *Surveillance capitalism* is the outcome of this symbiosis permeating digital societies (Zuboff, 2019), facilitating an intimate relationship of co-dependence between liberal governments and corporations in areas of surveillance, control, defence, and law enforcement (Powers and Jablonski, 2015). The overemphasis on cybersecurity for surveillance and law enforcement contrasts with the lack of regulatory oversight in digital markets, which creates an environment of less security and privacy that privileges corporate profit over distributed economic welfare and efficiency. The situation is rather puzzling: while surveillance capitalism misuses concepts of cybersecurity, capable of bypassing traditional constitutional safeguards and human rights (Lemke, 2014), consumers are increasingly exposed to faulty digital products with low levels of privacy and security due to regulatory and market failures.

Indeed, market aspects related to cybersecurity are characterised by diverse failures: information asymmetries, negative externalities, and inad-

equate levels of private investment (Carr and Tanczer, 2018; European Commission, 2022a). Heightening the security of digital products is no trivial task, and leaving it to market forces has historically led to suboptimal and inconsistent levels of confidentiality, integrity, and authenticity in said products (ENISA, 2011; Chung, 2017; DeNardis, 2020; Hendrick and Mckeay, 2022). Besides, turning from the security sector to a broader consideration, the extreme returns to scale, network externalities, and dependence on data pose challenges to digital markets' efficiency (Crémer, Montjoye and Schweitzer, 2019). The focus on internet expansion led policy makers to deviate from their traditional regulatory role, resulting in weakened oversight and accountability of industry in favour of profitability and dominance (Powers and Jablonski, 2015, pp. 22–24).

Safety regulations followed a different path from security. Liability derived from safety regulations was already a reality in the '80s, while the chronological gap for security was not closed in the next decades, leaving the behaviour of suppliers of digital products in the markets out of regulatory scope (European Commission, 2022a, p. 11). Unlike safety in the energy, finance, medical, and pharmaceutical sectors, cybersecurity as a quality of digital products remained under the auspices of industry self-regulation (Moore, 2013) and took a long time to be established in the EU, leaving consumers exposed to threats due to an absence of harmonised regulation (ENISA, 2022, p. 12). The legislative and regulatory landscape for cybersecurity in the EU scaled up from fragmented initiatives addressing specific domains to the latest large-scale horizontal regulations covering practically all elements of digital products. Security laws benefited from advancements in data protection and product safety regulation. Data protection norms emerged in Europe in the 1960s, mainly with the public sector's regulation of the collection and processing of data by public institutions, which, at the time, possessed the largest data banks and were the main processors. The *rediscovery* of the economic value of data at the end of the 1990s, coupled with the expansion of the Internet and the industrial strategies derived from it, led to a renewed concern about privacy in digital environments, raising concerns about cybersecurity as well (Mantelero, 2022, pp. 139–159). A risk-based approach to regulation emerged from product safety in the 1980s (Ruohonen, 2022). While chemicals and cosmetics required a more rigorous approach, software was permitted more lax supervision, leaving it industry players to self-assess their own standards, documentation, engineering practices, quality controls, and safety verification. The Product Liability Directive (Council Directive 85/374/EEC) represented a landmark

mechanism to incorporate four strategic goals (known at the time as the *New Approach*): fair trading, public health, public controls, and consumer information, as unified by standardisation. The Directive also strengthened consumer law by introducing some aspects of strict liability for producers, but software liability was left for a 2022 review (European Commission, 2022b).

The EU's cybersecurity institutional apparatus emerged at the end of the 1990s as a technical, engineering-driven governance system among various national teams responsible for network and computer security, known as Computer Emergency Response Teams (CERTs). The modus operandi of some European CERTs served as an initial base for further regulatory actions by the EU (Ruohonen et al, 2016). However, CERTs, including the coordination hub ENISA – founded in 2004 – followed a different track from other law enforcement agencies, such as Europol. The Cybersecurity Act (Regulation (EU) 2019/881) granted ENISA a permanent mandate with decision-making powers regarding policy issues and tasks, including technical supervision, certification frameworks, and dealing with large-scale cross-border cyberattacks and crises.

With the 2013 Cybersecurity Strategy (European Commission, 2013), cybersecurity became an official policy area in the EU by collating and combining sectoral rules for defence and law enforcement under a unified umbrella. Five years later, the revised 2017 strategy called for a complex approach to resilience that encompasses economic, societal, and political actors, enlarging the traditional and limited technical aspect of cybersecurity (European Commission, 2017). Although both strategies identified principles that would later be incorporated in legislative proposals, they did not include mandatory roles for the EU in the protection of the digital internal market (Bendiek et al, 2017). This changed with the third EU cybersecurity strategy of 2020, which evolved from being an essentially declarative policy to an operational document proposing concrete regulatory solutions by conceiving cybersecurity as a horizontal or cross-cutting policy for digital markets (Robles-Carrillo, 2023). This move integrates with other policy frameworks, marking the EU's more interventionist approach in digital markets, with the aim of stricter behaviour rules on economic activities (European Union, 2023). The next section dwells upon the CRA itself and contextualises the new law in a broader picture of other related legislation.

5. CRA: setting far-reaching cybersecurity rules for digital products

Over the last 20 years, cybersecurity rules have been established in sector-specific legislation related to cybercrime,[8] mobility and transport,[9] healthcare,[10] finance,[11] telecommunications,[12] and critical infrastructure.[13] However, as already mentioned several times in this chapter, an economics-led approach to cybersecurity as a quality of digital products was still notably absent. For instance, the GDPR (Regulation (EU) 2016/679) contains several provisions regarding information security, but does not deal with the cybersecurity of products. The Cybersecurity Act (Regulation (EU) 2019/881) concerns itself with certification and the ENISA's mandate, but does not establish any mandatory requirements for economic actors. The NIS 2 Directive (Directive (EU) 2022/2555), while serving as a follow-up to the first piece of EU-wide legislation on cybersecurity, does not entail requirements for the design, development, and security support of prod-

8 The Budapest Convention (Council of Europe, 2001) is the first binding instrument of international law aimed at harmonising domestic legislation related to cybercrime, dealing with copyright infringements, fraud, pornography, and network security violations. The convention has been signed by the 26 EU member states except Ireland.

9 Examples include the Vehicle General Safety Regulation (Regulation (EU) 2019/2144), the Common Rules in Civil Aviation Regulation (Regulation (EC) No 216/2008), and the Machinery Regulation (Regulation (EU) 2023/1230).

10 The Medical Device Regulation (Regulation (EU) 2017/745) and the In Vitro Diagnostic Medical Devices Regulation (Regulation (EU) 2017/746) are examples containing some aspects of cybersecurity.

11 The Regulation on Digital Operational Resilience for the Financial Sector (DORA) (Regulation (EU) 2022/2554) addresses this trend and aims to strengthen the cyber resilience of financial entities, such as banks, insurance companies, investment firms, and crypto-asset service providers.

12 Before the CRA, the Radio Equipment Directive (Directive 2014/53/EU) was the legislation with broad cybersecurity rules regarding transmitting devices (routers, smartphones, etc). Similarly, the European Electronic Communications Code (Directive (EU) 2018/1972) regulates how telecom operators should safeguard the security of their networks and services.

13 The European Network and Information Security Directive (NIS 1 Directive) (Directive (EU) 2016/1148) promulgated a minimum set of security requirements, including reporting obligations, for critical infrastructure in the EU. The NIS 2 Directive (Directive (EU) 2022/2555) expanded the sectors considered critical to encompass digital infrastructure, public administration, and space. The updated rules mandate more rigorous security requirements, which include enhanced cybersecurity risk management and reporting obligations. For more information on the NIS 2 Directive, see Chapter 17 'Unpacking the NIS 2 Directive: enhancing EU cybersecurity for the Digital Age' by Eyup Kun.

ucts. While the Radio Equipment Directive (Directive 2014/53/EU)[14] does include security requirements for network and fraud protection, it only covers wireless products (hardware and their embedded software), leaving other products and non-radio components (e.g., processors) out of the equation. Such safety laws as the Product Liability Directive (European Commission, 2022c) and Machinery Regulation (Regulation 2023/1230) address aspects of risk management and liability derived from flawed products, but do not include requirements of duty of care and other specific aspects of cybersecurity. The CRA has come to close this regulatory gap.

The CRA is a legislative initiative to regulate economic operators producing and commercialising products with digital elements (PDEs) in the EU internal market (Recital 2). Cybercrime involving such products has cost trillions of euros in recent years and the market dynamics have not been able to improve the situation for business and consumers (European Commission, 2022a, p. 2). The law addresses two main issues: (i) how to elevate the level of cybersecurity and (ii) how to provide better cybersecurity information to consumers (European Commission, 2022a, p. 4). Admittedly, these are not simple tasks, because:

Cross-border dimension: Cybersecurity has a strong cross-border dimension, as products are manufactured and used by consumers in different countries (European Commission, 2022a, p. 7);
Commercial interests: Cybersecurity has been not a commercial priority for manufacturers, as the emphasis on product security can be occasionally detrimental to corporate interests (European Commission, 2022a, p. 11). The development of new features is aimed towards market access and compatibility with existing products, with security properties suffering in the process (Burri and Zihlmann, 2023, p. 5). Security support (updates and handling of vulnerabilities) has been neglected or not provided for the product life cycle (European Commission, 2022a, p. 13);
Risk transfer to consumers: The higher switching costs and vendor lock-ins shift the costs of security vulnerabilities to consumers (European Commission, 2022a, p. 7). Although device providers can suffer reputational damage, consumers do not necessarily change the product or leave the provider's ecosystem (FSFE, 2023a, p. 22);
Lower security levels involving IoT: The massive number of smaller connected devices, IoT gadgets, toys, sensors, and other systems not run-

14 See also the Commission Delegated Regulation (EU) 2022/30, which further implemented cybersecurity requirements in the RED.

ning traditional operating systems have substantially lower levels of security protection. They present an entry gate to networks and may serve as hideouts in more complex environments (Meneghello et al, 2019). Besides, the apparent simplicity of such devices hides the complexity of their purpose and configuration, lowering the awareness of consumers (Palmer, 2021);

Information asymmetries: There are information asymmetries involved among manufacturers and consumers. Manufacturers have not provided adequate information about security features, vulnerabilities, and how to use a device safely (European Commission, 2022a, p. 13). Coupled with the fact that consumers generally lack even the most basic cybersecurity skills, this information asymmetry affects businesses as well: decision makers cannot properly evaluate risks posed to their organisation (European Commission, 2022a, p. 14).

Among the diverse possible regulatory approaches to deal with these issues, in 2021 the EC concluded that a strong interventionist approach would the most suited to improving the functioning and harmonisation of the internal market (Georgiev et al, 2021, p. 10). Therefore, the CRA aims to (European Commission, 2022b, p. 96):

Establish "security by design" for PDEs by requiring higher levels of confidentiality, integrity and availability;

Ensure "security support" for the whole life-cycle of the PDE by requiring mechanisms for updates and reporting vulnerabilities;

Foster "transparency of security information" by requiring the identification of dependencies and vulnerabilities, including the composition of software used and supply-chain-related information.

With that, the CRA affects all market participants involved in PDE supply chains: manufacturers (Art. 13), importers (Art. 19), distributors (Art. 20), and FOSS stewards (Art. 24).[15] Depending on their role and responsibility within the supply chain, these economic actors will have to fulfil several obligations before and while they place products on the market. Manufacturers bear the largest number of obligations as they are assumed to form the beginning of the supply chain, thus typically having the greatest influence on the conception, design, and development of their products (Burri and Zihlmann, 2023, p. 29). Some examples of obligations for manufactur-

15 The definition of FOSS Stewards and their obligations are detailed in Section 6.

ers include (Art. 13 and following provisions): they should ensure appropriate levels of cybersecurity by design and avoid delivering products with known exploits; they are also expected to adequately handle vulnerabilities throughout a product's life cycle, conduct due diligence and conformity assessments, and comply with reporting obligations. Importers and distributors are assigned a *watchdog* function by being permitted only to import or distribute products that meet the essential cybersecurity requirements outlined by the Regulation (Burri and Zihlmann, 2023, p. 36). They also should report vulnerabilities expeditiously if they become aware of them. However, if an importer or distributor modifies products or uses its own trademark, manufacturer obligations will apply (Art. 15).

The material scope of the CRA refers to PDEs – any commercialised product in the EU containing digital elements (Art. 2) – end-devices, such as laptops, smartphones, routers, cameras, sensors; software, including operating systems, mobile apps, video games; and components, such as chips, video cards, and software libraries. AI systems classified as high risk[16] are also included (Art. 12).[17] PDEs are classified in two groups based on their level of risk (Arts. 7 and 8), and subject to less or more stringent obligations ranging from a simple cybersecurity self-assessment to a third-party conformity assessment. Exceptions include products covered by sector-specific legislation, such as medical, aviation, and military devices. The underlying logic is that horizontal cross-sector overarching legislation will help significantly reduce products' attack surfaces by implementing a systematic approach to cybersecurity, such as security by design, conformity assessments, transparency obligations, and standard harmonisation (Georgiev et al, 2021, p. 10).

Compliance monitoring will be done by the European Commission, ENISA, and market surveillance authorities (Art. 52). The EU Member States shall be responsible for applying penalties (Art. 64). Non-compliance

16 The AI Act classifies AI according to its risk. Unacceptable risk is prohibited (e.g., social scoring systems and manipulative AI), while the law addresses mostly high-risk AI systems. Limited risks are subjected to transparency obligations (e.g., chatbots), and minimal risks are not regulated (e.g., AI in videogames). High-risk AI systems are those which can significantly impact individuals' rights and safety, such as systems used in critical infrastructures, employment processes, or law enforcement. See Section 2 of the AI Act (Regulation (EU) 2024/1689).

17 Products falling under the scope of the CRA which are eventually classified as high-risk AI systems according to Art. 6 of the AI Act shall comply with the essential requirements of the CRA (Recital 51).

may result in fines of up to 15 million EUR or 2,5% of the company's annual turnover.

The CRA aims to reach social goals, such as reducing cybercrime, increasing data protection and privacy, raising the population's overall awareness level, and creating a new market for cybersecurity-trained specialists (European Commission, 2022b, p. 69). However, admittedly, the 2022 Proposal was unable to capture some of the complexities of software development in open environments. The 2022 Proposal addressed FOSS, misapplying liability and compliance burdens onto those who could not reasonably be expected to deal with them. The analysis in the next section shows how the CRA affects FOSS, and how the rich debates during the legislative phase shaped a completely different result in the final approved version of the law.

6. The challenge of regulating FOSS cybersecurity

Considered by some to be the most impactful driver of innovation in the world today (Herstatt and Ehls, 2015), FOSS emerged as an idealistic movement to become a foundational element of the economy of the Digital Age (Benkler, 2006) and its notion of democracy (Foletto, 2021). Technically, FOSS refers to licensed source code guaranteeing the *four freedoms* to use, study, share, and improve the source code of a computer program.[18] From software running in devices, such as drivers, operating systems, apps, and embedded software of IoT devices, to software running less obviously in servers, digital libraries, APIs, operating system kernels, and encryption and security applications, FOSS has become a critical element of up to 90% of the software developed today (Nagle et al, 2022, p. 4). FOSS differs from proprietary software in its licensing. When a license does not grant these four freedoms, the software is considered proprietary (FSFE, 2020). In comparison with proprietary security by obscurity, where the details or mechanisms of a system are concealed and cannot be openly discovered and fixed, the open and transparent approach of FOSS is generally highly regarded due to the benefits of responsible disclosure and collaborative repair (NIST, 2008, p. 15; Smith, 2012; Norwood, 2023). Nevertheless,

18 The CRA follows this traditional definition in Art. 3 (40a): "'free and open-source software' means software the source code of which is openly shared and which is made available under a free and open-source license which provides for all rights to make it freely accessible, usable, modifiable and redistributable".

open environments where FOSS operates still have their own challenges. Hendrick and Mckeay (2022) listed the following:

Diversity of approaches: FOSS communities can vary significantly in their development of practices and techniques to reduce the risk of defects in code, or to respond quickly and safely when one is discovered by others;
Security as low priority: Organisations have been negligent in managing security of their software dependencies, opening more surface attack possibilities. Smaller FOSS organisations and communities bear disproportionate risks due to the lack of security policies covering FOSS;
Slow responses: Depending on the project's organisation and staffing, responsive actions to fix vulnerabilities can take months with open review processes.

Nagle et al (2022) added:

Lack of security review: Although FOSS benefits from transparent and open review for vulnerabilities, and their collaborative repair, not all FOSS projects are regularly reviewed equally. Vulnerabilities in widely used projects with smaller maintainer bases can remain unnoticed;
Lack of standardisation: The lack of standardised software component naming schemas as a time-delaying issue mean that organisations are unable to share such information with each other on a large scale;
Versioning challenges: Software versioning issues create incompatibilities in supply chains when organisations maintain internal versions of a package and do not contribute their changes back to the upstream repository;
Legacy technology: FOSS, similarly to proprietary software, suffers from persistent legacy technology. As technology (both software and hardware) ages, it loses support. The number of developers working to ensure updates – including feature improvements, as well as security and stability updates – decreases over time;
Lack of human capacity: Heavy reliance upon individual developers has legal, bureaucratic, and security consequences, as individuals may have fewer protections than companies. To illustrate, Koebler (2024) reported that bullying against individual developers can also impact volunteer-led projects when malicious actors conduct long campaigns in contribution processes to introduce vulnerabilities.

Since the CRA comprehensively affects digital products, the law has deep implications for FOSS. The CRA's impact assessment concluded that, in 2019 alone, investments in FOSS surpassed 1 billion euros, and small and micro enterprises could attribute over half their revenues to FOSS (European Commission, 2022b, p. 30). The software industry in the EU is almost entirely composed of small and medium-sized enterprises (SMEs), the vast majority of which (94%) are micro enterprises with fewer than nine employees (European Commission, 2022b, p. 29). Against this background, the European Commission's 2022 Proposal established an exception for FOSS in Recital 10: "in order not to hamper innovation or research, free and open-source software developed or supplied outside the course of a commercial activity should not be covered by this Regulation. [...] In the context of software, a commercial activity might be characterized not only by charging a price for a product, but also by charging a price for technical support services [...]".

However, the proposed distinction made for "commercial activity" prompted fierce criticism from some FOSS organisations about the potential chilling effects caused by liability consequences imposed on individuals and not-for-profit entities developing, curating, and distributing FOSS (Phipps, 2023). The core of the complaints deemed the EC's Proposal to disrupt the FOSS ecosystem by deterring volunteer contributors with strict liability regimes and compliance overload, affecting the entire software industry (Phipps, 2023). Demands highlighted the role of hobbyists, volunteers, and developer communities contributing to critical FOSS projects on a non-commercial basis. For instance, those receiving micro donations or small financial contributions for project maintenance would unduly and disproportionately bear the same level of responsibility and compliance costs as companies and corporations commercialising software (FSFE, 2023). Indeed, development models involving FOSS approaches cybersecurity differently from proprietary ones. FOSS is produced in a decentralised and distributed manner, meaning that there is no central authority to ensure quality and maintenance (Hendrick and Mckeay, 2022). FOSS is provided at zero cost to the consumer, decoupling its intrinsic value from its sale price. The huge quantity of FOSS systems made publicly available at no cost supports multi-billion-euro ecosystems (Milinkovich, 2023). Against this backdrop, although diverse FOSS stakeholders were displeased by the solution proposed for "commercial activity", they acknowledged the need for such a law, recognising that FOSS-related cybersecurity suffered from deregulation (Phipps, 2023). For instance, security incidents that affected

the entire FOSS industry, such as SolarWinds and Apache Log4j, have demonstrated the urgent need for improvement (Alkhadra et al, 2021; Feng and Lubis, 2022).

The following two years of the legislative process were marked by a transition to an updated regulatory attitude towards FOSS. While some civil-society and consumer-protection organisations supported the role of regulation to enhance cybersecurity as a public good, corporate-oriented deregulatory rhetoric was a source of concern by demanding the full exclusion of liability regimes (BEUC, 2022; Sander, 2024). The dialectical exchange during the Trilogues ultimately led to the incorporation of substantial changes that addressed concerns over exclusions and carved out specific roles and new legal constructions to address developer liabilities (Aertsen, 2024). The debates focused on improving clarity in terms of the liability of contributors acting outside of commercial activities (Art. 16 of the Proposal). Imposing stricter liability regimes on small or non-profit entities would undermine the consolidated logic of FOSS developers providing the software for free to the public, but accepting no liability or provision of warranty for its use. Since individual developers still represent the majority of the workforce in FOSS projects, the chilling effect could be tragic (FSFE, 2023). FOSS stakeholders demanded that businesses commercialising software and significantly profiting from the code should be the ones to bear liability for security flaws and provide warranties to their customers (Phipps, 2023). The incorporation of such demands substantially changed the structure of the law. If the CRA Proposal FOSS was timidly mentioned in Recital 10, the term now appears 57 times in the official text, permeating 10 Recitals and 13 Articles (Regulation (EU) 2024/2847). The applicability of the CRA to commercialised FOSS was clarified, and "FOSS Stewards" as a new regulatory category for organisations providing sustained support for the development of FOSS products was introduced.

The scope of application is explained in Recital 18:

> In relation to economic operators that fall within the scope of this Regulation, only free and open-source software made available on the market, and therefore supplied for distribution or use in the course of a commercial activity. The mere circumstances under which the product with digital elements has been developed, or how the development has been financed, should therefore not be taken into account when determining the commercial or non-commercial nature of that activity. More specifically, [...] to ensure that there is a clear distinction between the de-

> velopment and the supply phases, the provision of free and open-source software products with digital elements that are not monetised by their manufacturers is not considered a commercial activity.

To address the specific nuances of the FOSS industry, the legislators proposed a new "light-touch and tailor-made regulatory regime" of FOSS Stewards. Recital 19 provides a verbose explanation justifying the novel institution, mentioning that:

> Taking into account the importance for cybersecurity of many products with digital elements qualifying as free and open-source software that are published, but not made available on the market within the meaning of this Regulation, legal persons who provide support on a sustained basis for the development of such products which are intended for commercial activities, and who play a main role in ensuring the viability of those products (open-source software stewards), should be subject to a light-touch and tailor-made regulatory regime. Open-source software stewards include certain foundations as well as entities that develop and publish free and open-source software in a business context, including not-for-profit entities. [...] Given that the light-touch and tailor-made regulatory regime does not subject those acting as open-source software stewards to the same obligations as those acting as manufacturers under this Regulation, they should not be permitted to affix the CE marking to the products with digital elements whose development they support.

FOSS stewards are counterparts to manufacturers who ship products to market. They play an essential role in enabling manufacturers to deliver their products, but are subject to fewer requirements. Art. 3 (14) defines a FOSS Steward as: "a legal person, other than a manufacturer, that has the purpose or objective of systematically providing support on a sustained basis for the development of specific products with digital elements, qualifying as free and open-source software and intended for commercial activities, and that ensures the viability of those products". The obligations of FOSS Stewards differ from manufacturers (Art. 24): the former should develop cybersecurity policies for FOSS projects, handle vulnerabilities, help report incidents, and cooperate with market surveillance authorities to mitigate the cybersecurity risks posed by a PDE qualifying as FOSS. The CRA also allows the Commission to further establish voluntary security attestation programmes for FOSS developers and users to assess conformity with the CRA (Art. 25, Art. 32 (5)). The monitoring of FOSS Stewards'

activities should be done by market surveillance authorities (Art. 52 (3)). In case FOSS Stewards are not compliant with the law, corrective actions should be undertaken by such authorities. However, the CRA has excluded FOSS Stewards from administrative fines when the law is infringed (Recital 120 and Art. 64 (10b)).

In sum, the clarification of the liability regime and the introduction of FOSS Stewards reflect the EU's deeper understanding of how FOSS collaborative environments function. However, the practical implementation of the law will still face relevant challenges in relation to FOSS, especially involving different standardisation efforts related to conformity assessments, security policies and procedures, supply chain risk management (e.g., software bills of materials), documentation, and reporting (European Commission, 2024).

7. Conclusion and future research

As the old adage reminds us: *with great power comes great responsibility*. The ambitious CRA has a long way to go to accomplish its desired effect of raising the cybersecurity bar for digital markets. As discussed in the first sections of this chapter, cybersecurity is a multidisciplinary subject that cannot approached simplistically. Fundamental rights and values should be balanced in the process of increasing security measures in the digital society to improve and eliminate the contradictions of surveillance capitalism. Cybersecurity should be an instrument with which to promote the common good (Bendiek et al, 2017), and its effects across data protection, platform regulation, and consumer protection should conform to democratic principles. The CRA is inserted in a regulatory momentum that confront corporate power. As seen, market forces alone have not been able to promote safer and more secure digital environments. This historical experience should not be dismissed when corporate pressure defies reasoning that privileges consumer protection, digital commons, and human rights.

This chapter has served as an introduction to the CRA and focused on some of the history that led to its creation. It leaves now as a follow-up task the analysis of its implementation, but with a caveat: as has happened with other large and far-reaching legislation, its enforcement can be more challenging than the legislative process itself, and expectations should be adjusted accordingly. Regulators will struggle to make sense of the solutions proposed by affected parties, prompting strict monitoring (especially from

civil society) to confirm whether the interests of consumers and citizens are being prioritised. As concluded in the preceding section, the regulatory interaction with FOSS stakeholders reveals how open innovation depends on complex intricate dynamics that escape the traditional classifications of industrial economic actors (Phipps, 2023a). Volunteers, not-for-profit communities, and non-commercial actors are frail key players in environments that are highly exposed to corporate power and domination (Birkinbine, 2020; Brazeal, 2024). Such fragility impacts cybersecurity and will require special care and attention from policymakers.

Acknowledgments

This study was enriched by the invaluable contribution of several people. I am grateful to Elisabetta Biasin, Alexander Sander and Carlo Piana for their insights and comments. I thank the participants of the 2024 Workshop "Digital Decade: How the EU shapes digitalisation research" at the Weizenbaum Institute who interacted and provided feedback on a previous version of this paper. I am grateful to Prof. Dr. Christoph Rademacher and Prof. Dr. Jyh-An Lee for allowing me to present and discuss the outcome of this research at the Waseda University in Tokyo. My appreciation is also extended to Richard Schmeidler for his thorough and meticulous volunteer proofreading. Mariam Sattorov's compilation of EU legislation and literature review was instrumental, for which I am sincerely appreciative. I thank also the reviewers, the official proofreader and the editors, in particular Marie-Therese Sekwenz and Rita Gsenger, who dedicated time and expertise to improving this paper. Any inconsistency and imprecision in the text is my sole responsibility.

References

ACM et al (2017) *Cybersecurity curricula 2017: curriculum guidelines for post-secondary degree programs in cybersecurity*. ACM, IEEE, AIS SIGSEC, IFIP WG [Online], 11 August. Available at: https://www.acm.org/binaries/content/assets/education/curricula-recommendations/csec2017.pdf (Accessed: 11 April 2024).

Aertsen, M. (2024) *What I learned in Brussels: the Cyber Resilience Act*. NLnet Labs [Online]. Available at: https://blog.nlnetlabs.nl/what-i-learned-in-brussels-the-cyber-resilience-act/. (Accessed: 1 May 2024).

Alkhadra, R., Abuzald, J. and AlShammari, M. (2021) 'Solar winds hack: in-depth analysis and countermeasures', in *2021 12th International Conference on Computing Communication and Networking Technologies (ICCCNT)*, pp. 1–7.

Apache Foundation (2023) *Save open source: the impending tragedy of the Cyber Resilience Act* [Online]. Available at: https://news.apache.org/foundation/entry/save-open-source-the-impending-tragedy-of-the-cyber-resilience-act (Accessed: 9 May 2024).

Aslan, A. and Samet, R. (2020) 'A comprehensive review on malware detection approaches', *IEEE Access*, 8, pp. 6249–6271.

Barlow, J. (1996) *A declaration of the independence of cyberspace*. Electronic Frontier Foundation [Online]. Available at: https://www.eff.org/cyberspace-independence (Accessed: 1 May 2024).

Bendiek, A., Bossong, R. and Schultze, M. (2017) *The EU's revised cybersecurity strategy*. SWP Comments [Online]. Available at: https://www.swp-berlin.org/publications/products/comments/2017C47_bdk_etal.pdf (Accessed 9 May 2024).

Benkler, Y. (2006) *The wealth of networks: how social production transforms markets and freedom*. New Haven: Yale University Press.

BEUC (2022) *Cyber Resilience Act: cybersecurity of digital products and ancillary services. BEUC response to public consultation*. BEUC [Online]. Available at: https://www.beuc.eu/position-papers/cyber-resilience-act-cybersecurity-digital-products-and-ancillary-services (Accessed: 1 May 2024).

Birkinbine, B. (2020) *Incorporating the digital commons: corporate involvement in free and open source software*. London: University of Westminster Press.

Brazeal, F. (2024) *The threat to open source comes from within*. Good Tech Things [Online]. Available at: https://newsletter.goodtechthings.com/p/the-threat-to-open-source-comes-from (Accessed: 11 April 2024).

Burri, M. and Zihlmann, Z. (2023) 'The EU Cyber Resilience Act – an appraisal and contextualization', *Zeitschrift für Europarecht (EuZ)*, 2, pp. 2–37.

Bygrave, L.A. (2024) 'The emergence of EU cybersecurity law: a tale of lemons, angst, turf, surf and grey boxes', *Computer Law & Security Review*, 56, 106071 [Online]. Available at: https://doi.org/10.1016/j.clsr.2024.106071 (Accessed: 29 January 2025).

Carr, M. and Tanczer, L. (2018) 'UK cybersecurity industrial policy: an analysis of drivers, market failures and interventions', *Journal of Cyber Policy*, 3(3), pp. 430–444.

Chiara, G. (2022) 'The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements', *International Cybersecurity Law Review*, 3, pp. 255–272.

Christen, M., Gordjin, B. and Loi, M. (eds.) (2020) *The ethics of cybersecurity*. London: Springer Nature.

Chung, J. (2017). 'Critical infrastructure, cybersecurity, and market failure', *Oregon Law Review*, 96, pp. 441–474.

'Commission Delegated Regulation (EU) 2022/30 of 29 October 2021 supplementing Directive 2014/53/EU of the European Parliament and of the Council with regard to the application of the essential requirements referred to in Article 3(3), points (d), (e), and (f), of that Directive' (2022) *Official Journal* L 7, 12 January, pp. 6–10 [Online]. Available at: http://data.europa.eu/eli/reg_del/2022/30/oj (Accessed: 29 January 2025).

Computer Security Resource Center (no date) *attack surface* [Online]. Available at: https://csrc.nist.gov/glossary/term/attack_surface (Accessed: 29 January 2025).

'Council Directive 85/374/EEC of 25 July 1985 on the approximation of the laws, regulations and administrative provisions of the Member States concerning liability for defective products' (1985) *Official Journal* L 210, 7 August, pp. 29–33 [Online]. Available at: http://data.europa.eu/eli/dir/1985/374/oj (Accessed: 1 May 2024).

Council of Europe (2001) *Convention on Cybercrime. European Treaty Series – No. 185*. Council of Europe [Online]. Available at: https://www.coe.int/en/web/cybercrime/the-budapest-convention (Accessed: 11 April 2024).

Crémer, J., Montjoye, Y. and Schweitzer, H. (2019) *Competition policy for the digital era*. European Commission Publications Office [Online]. Available at: https://data.europa.eu/doi/10.2763/407537 (Accessed: 5 May 2024).

CVE (no date) Process [Online] Available at: https://www.cve.org/About/Process (Accessed: 29 January 2025).

DeNardis, L. (2020) 'Cyber-physical security' in Denardis, L. (ed.) *The internet in everything: freedom and security in a world with no off switch*. New Haven: Yale University Press, pp. 93-131.

'Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment and repealing Directive 1999/5/EC' (2014) *Official Journal* L 153, 22 May, pp. 62–106 [Online]. ELI: http://data.europa.eu/eli/dir/2014/53/oj (Accessed: 5 May 2024).

'Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union' (2016) *Official Journal* L 194, 19 July, pp. 1–30 [Online]. ELI: http://data.europa.eu/eli/dir/2016/1148/oj (Accessed: 5 May 2024).

'Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code. Recast. Text with EEA relevance' *Official Journal* L 321, 17 December, pp. 36–214 [Online]. ELI: http://data.europa.eu/eli/dir/2018/1972/oj (Accessed: 05.05.24).

'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)' (2022) *Official Journal* L 333, 27 December, pp. 80–152 [Online]. ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27 (Accessed: 11 April 2024).

ENISA (2011) *The working group contribution, economics of security: facing the challenging*. ENISA [Online]. Available at: https://www.enisa.europa.eu/topics/risk-management/files/EoS%20Final%20report/view (Accessed 1 May 2024).

ENISA (2015) *Good practice guide on vulnerability disclosure: from challenges to recommendations*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/vulnerability-disclosure (Accessed: 1 May 2024).

ENISA (2022) *Coordinated vulnerability disclosure policies in the EU*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/coordinated-vulnerability-disclosure-policies-in-the-eu (Accessed 1 May 2024).

ENISA (2023) *Good practices for supply chain cybersecurity*. ENISA [Online]. Available at: https://op.europa.eu/en/publication-detail/-/publication/866c8abe-1ba8-11ee-806b-01aa75ed71a1 (Accessed: 11 April 2024).

European Commission (2017) *State of the Union 2017 – cybersecurity: Commission scales up EU's response to cyberattacks*. European Commission [Online]. Available at: https://ec.europa.eu/commission/presscorner/api/files/document/print/en/ip_17_3193/IP_17_3193_EN.pdf (Accessed: 9 May 2024).

European Commission (2020) *Joint communication to the European Parliament and the Council: the EU's cybersecurity strategy for the digital decade. JOIN(2020) 18 final*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0 (Accessed 9 May 2024).

European Commission (2021) *2030 digital compass: the European way for the digital decade. COM(2021) 118 final*. European Commission [Online]. Available at: https://commission.europa.eu/system/files/2023-01/cellar_12e835e2-81af-11eb-9ac9-01aa75ed71a1.0001.02_DOC_1.pdf (Accessed: 11 April 2024).

European Commission (2022) *Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending regulation (EU) 2019/1020. COM(2022) 454 final 2022/0272(COD)*. European Commission [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0454 (Accessed: 11 April 2024).

European Commission (2022a) *Commission Staff Working Document. Impact Assessment Report. Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. COM(2022) 454 final, SEC(2022) 321 final, SWD(2022) 283 final. Part 1/3*. European Commission [Online]. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/89545 (Accessed: 11 April 2024).

European Commission (2022b) *Commission Staff Working Document. Impact Assessment Report. Annexes to the Impact Assessment Report Accompanying the document Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements and amending Regulation (EU) 2019/1020. COM(2022) 454 final, SEC(2022) 321 final, SWD(2022) 283 final. Part 2/3*. European Commission [Online]. Available at: https://ec.europa.eu/newsroom/dae/redirection/document/89546 (Accessed: 11 April 2024).

European Commission (2022c) *Proposal for a Directive of the European Parliament and of the Council on liability for defective products. COM(2022) 495 final 2022/0302(COD)*. EUR-Lex [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52022PC0495 (Accessed: 5 January 2024).

European Commission (2024) *Draft on the Commission Implementing Decision on standardisation request to European Standards Organisations in support of Union policy on cybersecurity requirements for products with digital elements. Notification under Article 12 of Regulation (EU) No 1025/2012*. European Commission [Online]. Available at: https://ec.europa.eu/docsroom/documents/58974. (Accessed 23 May 2024)

European Union (2013) *Cybersecurity strategy of the European Union: an open, safe and secure cyberspace (JOIN/2013/01 final)*. EDPS [Online]. Available at: https://www.edps.europa.eu/data-protection/our-work/publications/opinions/cyber-security-strategy-european-union-open-safe-and_en (Accessed: 5 May 2024).

European Union (2023) *European Declaration on digital rights and principles for the digital decade 2023/C 23/01. Official Journal* C 23, 23 January, pp. 1–7 [Online]. Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:JOC_2023_023_R_0001. (Accessed: 11 April 2024)

Feil, R. and Nyffenegger, L. (2008) 'Evolution of cross site request forgery attacks', *Journal in Computer Virology*, 4(1), pp. 61–71.

Feng, S. and Lubis, M. (2022) 'Defense-in-depth security strategy in log4j vulnerability analysis', in *2022 International Conference Advancement in Data Science, E-learning and Information Systems (ICADEIS)*, pp. 1–4.

Foletto, L. (2021) *A cultura é livre: uma história da resistência antipropriedade*. São Paulo: Autonomia Literária [Online]. Available at: https://rosalux.org.br/wp-content/uploads/2021/03/aculturaelivre-1.pdf (Accessed: 19 May 2024).

FSFE (2020) *What is free software*. Free Software Foundation Europe [Online]. Available at: https://fsfe.org/freesoftware/ (Accessed: 15 April 2024).

FSFE (2023) *CRA & PLD: EU: proposed liability rules will harm free software*. Free Software Foundation Europe [Online]. Available at: https://fsfe.org/news/2023/news-20230323-01.html (Accessed: 11 April 2024).

FSFE (2023a) *Router Freedom Survey Report – the end-user perspective on freedom of terminal equipment in Europe*. Free Software Foundation Europe [Online]. Available at: https://download.fsfe.org/routers/rf-survey-report-2023.pdf. (Accessed: 11 April 2024)

Fuster, G. and Jasmontaite, L. (2020) 'Cybersecurity regulation in the European Union: the digital, the critical and fundamental rights' in Christen, M., Gordjin, B. and Loi, M. (eds.) *The ethics of cybersecurity*. London: Springer Nature, pp. 97–115.

Georgiev, S. et al (2021) *Study on the need of cybersecurity requirements for ICT products – No. 2020-0715 Final Study Report*. Luxembourg: Publications Office of the European Union.

Grady, F. and Parisi, F. (2006) *The law and economics of cybersecurity*. Cambridge: Cambridge University Press.

Grotto, J. and Schallbruch, M. (2021) 'Cybersecurity and the risk governance triangle', *International Cybersecurity Law Review*, 2, pp. 77–92. Available at: https://doi.org/10.1365/s43439-021-00016-9 (Accessed: 11 April 2024).

Guiora, N. (2017) *Cybersecurity: geopolitics, law, and policy*. Abingdon: Routledge.

Hendrick, S. and Mckeay, M. (2022) *Addressing cybersecurity challenges in open source software*. Report from Linux Foundation & Snyk [Online]. Available at: https://www.linuxfoundation.org/research/addressing-cybersecurity-challenges-in-open-source-software (Accessed: 11 April 2024).

Hermanowski, D. (2015) 'Open source security information management system supporting it security audit', *2015 IEEE 2nd International Conference on Cybernetics*, pp. 336–341.

Herrmann, D. and Pridöhl, H. (2020) 'Basic concepts and models of cybersecurity' in Christen, M., Gordjin, B., and Loi, M. (eds.) *The ethics of cybersecurity*. London: Springer Nature, pp. 11-44.

Herstatt, C. and Ehls, D. (2015) *Open source innovation: the phenomenon, participant's behaviour, business implications*. Abingdon: Routledge.

Hypernormalisation (2016) Directed by Adam Curtis [Documentary]. London: BBC Documentary. Available at: https://www.bbc.co.uk/programmes/p04b183c (Accessed: 19.04.2024).

Ishikawa, T. and Kryvoi, Y. (eds.) (2023) *Public and private governance of cybersecurity: challenges and potential*. Cambridge: Cambridge University Press.

Koebler, J. (2024) *Bullying in open source software is a massive security vulnerability*. 404 Media [Online]. Available at: https://www.404media.co/xz-backdoor-bullying-in-open-source-software-is-a-massive-security-vulnerability/ (Accessed 11 April 2024).

Kryvoi, Y. (2023) 'Responding to public and private cyberattacks: jurisdiction, self-defence, and countermeasures' in Ishikawa, T. and Kryvoi, Y. (eds.) *Public and private governance of cybersecurity: challenges and potential*. Cambridge: Cambridge University Press.

Lasota, L. (2023) 'Regulating corporate behaviour in digital ecosystems: increasing fairness and contestability of digital markets with free software', *Toward Green, Inclusive, and Digital Growth* [Online]. Available at: https://doi.org/10.26493/978-961-293-306-7 (Accessed: 11 April 2024).

Lemke, T. (2014) 'The risks of security: liberalism, biopolitics, and fear' in Lemm, V. and Vatter, M. (eds.) *The government of Life: Foucault, biopolitics, and neoliberalism*. New York: Fordham University Press, pp. 59-74.

Mantelero, A. (2022). *Beyond data: human rights, ethical and social impact assessment in AI*. The Hague: Springer.

Meneghello, F. et al. (2019) 'IoT: internet of threats? A survey of practical security vulnerabilities in real IoT devices', *IEEE Internet of Things Journal*, 6(5), pp. 8182–8201.

Milinkovich, M. (2023) *Cyber Resilience Act: good intentions and unintended consequences*. Eclipse Foundation [Online]. Available at: https://blogs.eclipse.org/post/mike-milinkovich/cyber-resilience-act-good-intentions-and-unintended-consequences (Accessed 11 April 2024).

Moore, R, (2013) 'Standardisation: a tool for addressing market failure within the software industry', *Computer Law & Security Review*, 29(4), pp. 413–429.

Mugarza, I., Flores, J.L., Montero, J.L. (2020) 'Security issues and software updates management in the Industrial Internet of Things (IIoT) era', *Sensors*, 20(24), 7160 [Online]. Available at: https://doi.org/10.3390/s20247160 (accessed: 29 January 2025).

Nagle, F. et al (2022) *Census II of free and open source software – application libraries*. The Linux Foundation and The Laboratory for Innovation Science at Harvard [Online]. Available at: https://www.linuxfoundation.org/tools/census-ii-of-free-and-open-source-software-application-libraries (Accessed 11 April 2024).

Newitz, A. (2013) *The bizarre evolution of the word "cyber"*. Gizmodo [Online]. Available at: https://gizmodo.com/today-cyber-means-war-but-back-in-the-1990s-it-mean-1325671487 (Accessed: 23 April 2024).

NIST (2008) *Guide to general server security: recommendations of the National Institute of Standards and Technology*. National Institute of Technology and Standards [Online], v.800-123. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-123.pdf (Accessed: 19 May 2024).

NIST (2012) *Guide for conducting risk assessments*. National Institute of Technology and Standards [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf (Accessed: 1 May 2024).

Norwood, D. (2023) *Debian public statement about the EU Cyber Resilience Act and the Product Liability Directive*. Bits from Debian [Online]. Available at: https://bits.debian.org/2023/12/debian-statement-cyber-resillience-act.md.html (Accessed: 1 May 2024).

OWASP (2019) *API security top 10 2019: the ten most critical API security risks*. The Open Worldwide Application Security Project [Online]. Available at: https://owasp.org/API-Security/editions/2019/en/dist/owasp-api-security-top-10.pdf (Accessed: 11 April 2024).

OWASP (2020) *OWASP Vulnerability Management Guide (OVMG)*. The Open Worldwide Application Security Project [Online]. Available at: https://owasp.org/www-project-vulnerability-management-guide/OWASP-Vuln-Mgm-Guide-Jul23-2020.pdf (Accessed: 1 May 2024).

OWASP (2025). *SQL Injection* [Online] Available at: https://owasp.org/www-community/attacks/SQL_Injection (Accessed: 29 January 2025).

Palmer, D. (2021) *Critical IoT security camera vulnerability allows attackers to remotely watch live video – and gain access to networks*. Zdnet [Online]. Available at: https://www.zdnet.com/article/critical-iot-security-camera-vulnerability-allows-attackers-to-remotely-watch-live-video-and-gain-access-to-networks/ (Accessed: 1 May 2024).

Papakonstantinou, V. (2022) 'Cybersecurity as praxis and as a state: the EU law path towards acknowledgement of a new right to cybersecurity?', *Computer Law & Security Review*, 44, 105653 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105653 (accessed: 29 January 2025).

Paulsen, C. and Byers, R. (2019) *Glossary of key information security terms*. National Institute of Technology and Standards [Online]. Available at: https://nvlpubs.nist.gov/nistpubs/ir/2019/NIST.IR.7298r3.pdf (Accessed: 1 May 2024).

Payne, C. (2002) 'On the security of open source software', *Information Systems Journal*, 12, pp. 61–78.

Phipps, S. (2023) *The ultimate list of reactions to the Cyber Resilience Act*. Open Source Initiative [Online]. Available at: https://opensource.org/blog/the-ultimate-list-of-reactions-to-the-cyber-resilience-act (Accessed: 15 May 2024).

Phipps, S. (2023a) *What is the Cyber Resilience Act and why it's dangerous for open source*. Open Source Initiative [Online]. Available at: https://opensource.org/blog/modern-eu-policies-need-the-voices-of-the-fourth-sector (Accessed: 15 May 2024).

Porcedda, M. (2023) *Cybersecurity, privacy and data protection in EU law: a law, policy and technology analysis*. Oxford: Hart Publishing.

Powers, M. and Jablonski, M. (2015) *The real cyber war: the political economy of internet freedom*. Champaign: University of Illinois Press.

'Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)' (2016) *Official Journal* L 119, 4 May, pp. 1–88 [Online]. ELI: http://data.europa.eu/eli/reg/2016/679/oj (Accessed: 5 May 2024). 'Regulation (EU) 2017/745 of the European Parliament and of the Council of 5 April 2017 on medical devices, amending Directive 2001/83/EC, Regulation (EC) No 178/2002 and Regulation (EC) No 1223/2009 and repealing Council Directives 90/385/EEC and 93/42/EEC' (2017) *Official Journal* L 117, 5 May, pp. 1–175 [Online]. ELI: http://data.europa.eu/eli/reg/2017/745/oj (Accessed: 5 May 2024).

'Regulation (EU) 2017/746 of the European Parliament and of the Council of 5 April 2017 on in vitro diagnostic medical devices and repealing Directive 98/79/EC and Commission Decision 2010/227/EU' (2017) *Official Journal* L 117, 5 May, pp. 176–332 [Online]. ELI: http://data.europa.eu/eli/reg/2017/746/oj (Accessed: 5 May 2024).

'Regulation (EU) 2018/1139 of the European Parliament and of the Council of 4 July 2018 on common rules in the field of civil aviation and establishing a European Union Aviation Safety Agency, and amending Regulations (EC) No 2111/2005, (EC) No 1008/2008, (EU) No 996/2010, (EU) No 376/2014 and Directives 2014/30/EU and 2014/53/EU of the European Parliament and of the Council, and repealing Regulations (EC) No 552/2004 and (EC) No 216/2008 of the European Parliament and of the Council and Council Regulation (EEC) No 3922/91 (Text with EEA relevance)' (2018) *Official Journal* L 212, 22 August, pp. 1 [Online]. ELI: http://data.europa.eu/eli/reg/2018/1139/2024-12-01 (Accessed: 29 January 2025).

'Regulation (EU) 2019/2144 of the European Parliament and of the Council of 27 November 2019 on type-approval requirements for motor vehicles and their trailers, and systems, components and separate technical units intended for such vehicles, as regards their general safety and the protection of vehicle occupants and vulnerable road users, amending Regulation (EU) 2018/858 of the European Parliament and of the Council and repealing Regulations (EC) No 78/2009, (EC) No 79/2009 and (EC) No 661/2009 of the European Parliament and of the Council and Commission Regulations (EC) No 631/2009, (EU) No 406/2010, (EU) No 672/2010, (EU) No 1003/2010, (EU) No 1005/2010, (EU) No 1008/2010, (EU) No 1009/2010, (EU) No 19/2011, (EU) No 109/2011, (EU) No 458/2011, (EU) No 65/2012, (EU) No 130/2012, (EU) No 347/2012, (EU) No 351/2012, (EU) No 1230/2012 and (EU) 2015/166' (2019) *Official Journal* L 325, 16 December, pp. 1–40 [Online]. ELI: http://data.europa.eu/eli/reg/2019/2144/oj (Accessed: 1 May 2024).

'Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act)' (2019) *Official Journal* L 151, 7.6.2019, pp. 15–69 [Online]. EI: http://data.europa.eu/eli/reg/2019/881/oj (Accessed: 1 May 2024).

'Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011' (2022) *Official Journal* L 333, 27 December, pp. 1–79 [Online]. ELI: http://data.europa.eu/eli/reg/2022/2554/oj (Accessed: 11 April 2024).

'Regulation (EU) 2023/1230 of the European Parliament and of the Council of 14 June 2023 on machinery and repealing Directive 2006/42/EC of the European Parliament and of the Council and Council Directive 73/361/EEC' (2023) *Official Journal* L 165, 29 June, pp. 1–102 [Online]. ELI: http://data.europa.eu/eli/reg/2023/1230/oj (Accessed: 11 April 2024).

'Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act)' (2024) *Official Journal* L, 2024/1689, 12 July. [Online]. ELI: http://data.europa.eu/eli/reg/2024/1689/oj. (Accessed: 3 October 2024).

'Regulation (EU) 2024/2847 of the European Parliament and of the Council of 23 October 2024 on horizontal cybersecurity requirements for products with digital elements and amending Regulations (EU) No 168/2013 and (EU) 2019/1020 and Directive (EU) 2020/1828 (Cyber Resilience Act)' (2024) *Official Journal* L, 2024/2847, 20 November [Online]. ELI: http://data.europa.eu/eli/reg/2024/2847/oj (Accessed: 24 December 2024).

Robles-Carrillo, M. (2023) 'The European Union strategy for cybersecurity' in Moura Vicente, D., de Vasconcelos Casimiro, S. and Chen, C. (eds.) *The legal challenges of the fourth industrial revolution*. London: Springer Nature, pp. 173-192.

Ruohonen, J. (2022) 'A review of product safety regulations in the European Union', *International Cybersecurity Law Review,* 3, pp. 345–366.

Ruohonen, J., Hyrynsalmi, S. and Leppänen, V. (2016) 'An outlook on the institutional evolution of the European Union cyber security apparatus', *Government Information Quarterly*, 33(4), pp. 746–756.

Salvaggio, S.A. and González, N. (2023) 'The European framework for cybersecurity: strong assets, intricate history', *International Cybersecurity Law Review*, 4, pp. 137–146.

Sander, A. (2024) *CRA & PLD liability rules and software freedom.* Conference talk at elLibre [Online]. Available at: https://propuestas.eslib.re/2024/charlas/cra-pld-liability-rules-software-freedom (Accessed: 25 May 2024).

Schreider, T. and Noakes-Fry, K. (2020) *Cybersecurity law, standards and regulations*. Brookfield: Rothstein Publishing.

Shirey, R. (2007) 'Vulnerability'. *Internet Engineering Task Force RFC 4949 Internet Security Glossary, Version 2* [Online]. Available at: https://datatracker.ietf.org/doc/html/rfc4949 (Accessed: 1 May 2024).

Shostack, A. (2014) *Threat modeling: designing for security.* Indianapolis: Wiley.

Smith, R. (2012) 'A contemporary look at Saltzer and Schroeder's 1975 design principles', *IEEE Security & Privacy*, 10(6), pp. 20–25.

Statista (2024) *Number of internet and social media users worldwide as of January 2024*. Statista [Online]. Available at: https://www.statista.com/statistics/617136/digital-population-worldwide/ (Accessed 1 May 2024).

Townsend, K. (2024) *Vulnerabilities CVE and NVD – A weak and fractured source of vulnerability truth*. SecurityWeek [Online]. Available at: https://www.securityweek.com/cve-and-nvd-a-weak-and-fractured-source-of-vulnerability-truth/ (Accessed 1 May 2024).

Van de Poel, I. (2020) 'Core values and value conflicts in cybersecurity: beyond privacy versus security' in Christen, M., Gordjin, B. and Loi, M. (eds.) *The ethics of cybersecurity*. London: Springer Nature, pp. 45–71.

Vedder, A. (2019) 'Safety, security and ethics' in Vedder, A. et al (eds) *Security and law. Legal and ethical aspects of public security, cyber security and critical infrastructure security*. Cambridge, Antwerp, Chicago: Intersentia, pp. 11-26.

Wang, Z. Sun, L. and Zhu, H. (2020) 'Defining Social Engineering in Cybersecurity,' in *IEEE Access*, v. 8 [Online]. Available at: https://ieeexplore.ieee.org/abstract/document/9087851 (Accessed: 31 January 2025).

Warner, M. (2012) 'Cybersecurity: a pre-history', *Intelligence and National Security*, 27(5), pp. 781–799.

Wikipedia (2025) *API* [Online]. Available at: https://en.wikipedia.org/wiki/API (Accessed: 29 January 2025).

Wikipedia (2025a) *Reverse engineering* [Online]. Available at: https://en.wikipedia.org/wiki/Reverse_engineering (Accessed: 29 January 2025).

Your Europe (2024) *CE marking* [Online]. Available at: https://europa.eu/youreurope/business/product-requirements/labels-markings/ce-marking/index_en.htm (Accessed: 29 January 2025).

Zuboff, S. (2019) *The age of surveillance capitalism: the fight for a human future at the new frontier of power*. New York: PublicAffairs.

Unpacking the NIS 2 Directive: Enhancing EU Cybersecurity for the Digital Age

Eyup Kun

Abstract

The rapid evolution of the digital landscape has increased cybersecurity challenges, necessitating legal interventions to protect critical infrastructure and essential services across the European Union (EU). The EU's Network and Information Systems (NIS 1) Directive (2016/1148) marked the first cross-sectoral legislative effort to address cybersecurity, focusing on essential services such as energy, transport, and banking. However, the Directive's scope and implementation revealed significant gaps, including inconsistent application across Member States and inadequate coverage of newly critical sectors. Recognizing these shortcomings, the EU adopted the NIS 2 Directive (2022/2555), which introduces substantial enhancements to strengthen the cybersecurity framework.

This paper examines the evolution from NIS 1 to NIS 2, highlighting the latter's broader scope, harmonized cybersecurity requirements, improved reporting mechanisms, and stronger supervision and enforcement. While setting minimum harmonization standards, it allows Member States the flexibility to adopt stricter measures aligned with EU law. The NIS 2 Directive also emphasizes cooperative frameworks at national and EU levels to enhance collective resilience against cyber threats.

This Chapter addresses the scope, objectives, and stakeholder responsibilities under NIS 2, including obligations for Member States, public and private entities, and their coordination mechanisms.

1. Introduction: evolution from the NIS Directive to NIS 2 Directive

As the digital landscape evolves, so does the complexity of cyber threats, which pose a significant risk to stability and security across the European Union (EU). Cyber disruptions can lead to substantial repercussions across Member States, thereby requiring EU-level interventions to safeguard the robustness of digital systems (Jacobs, 2023). Recognising the imperative

need to manage cybersecurity, the EU has been at the forefront of establishing comprehensive frameworks to protect its cybersecurity (Carrapico and Barrinha, 2017; Odermatt, 2018).

Nevertheless, cybersecurity, as a relatively nascent field, is not delineated as specific policy area under the EU law. The EU's competence is interpreted in relation to different policy areas (Jacobs, 2023). It falls under shared competence, allowing Member States to create legislation in this field unless the EU itself has already taken action (Jacobs, 2023). Therefore, any legal intervention taken by the EU must follow the principles of proportionality and subsidiarity, which means that the measures should be necessary and more efficiently implemented at the EU, rather than national, level. Moreover, the increasing significance of national security and technological sovereignty adds complexity to this framework, as these matters are primarily under the control of Member States (Chiara, 2024; Liebetrau, 2024). This overlap emphasises the difficulties in expanding the internal market ground of Article (Art.) 114 of the Treaty on the Functioning of the European Union (TFEU) to encompass complex cybersecurity issues, which are increasingly connected with fundamental rights, physical safety, and national security, rather than solely the operation of the internal market (Brandão and Camisão, 2022; Chiara, 2024; Liebetrau, 2024). Thus, although the EU has the competence to create laws, as per Art. 114, the extent and speed at which it can regulate are naturally constrained by these factors.

Considering these challenges, the EU adopted the Network and Information Systems (NIS 1) Directive (2016/1148) to increase the level of cybersecurity. It was the first cross-sectoral legislation aimed at enhancing cybersecurity across the EU. The NIS 1 Directive focused on cybersecurity in such essential services as energy, transport, and banking (enumerated under Annex II of the NIS Directive), which are crucial for the functioning of the economy, society, and digital service providers (namely online marketplaces, online search engines, and cloud computing service providers) under Annex III of the NIS 1 Directive.

In the realm of the rapid expansion of digitalisation and the increasing reliance on information technologies, it became apparent that the NIS 1 Directive needed a substantial update to address emerging challenges and technological dependencies (European Commission, 2020). It became evident that the scope of the NIS 1 Directive did not sufficiently cover all of the sectors now deemed critical due to advanced digitalisation and greater interconnectedness. This was a significant concern as the dependency on

digital platforms and services had escalated, necessitating a broader scope encompassing more sectors and entities (discussed in Section 2.1.). Moreover, the implementation of the NIS 1 Directive revealed inconsistencies across Member States due to varying interpretations of the Directive's criteria for determining responsible actors within it (European Commission, 2020). This resulted in a fragmented approach to cybersecurity, with some critical sectors being under-regulated in certain countries. For instance, significant disparities were noted in the inclusion of healthcare providers and major railway operators under the Directive's scope, leading to an uneven security state across the EU (European Commission, 2020, p. 14)

Considering these changes, the EU adopted the NIS 2 Directive (2022/2555), which, compared to its predecessor, is more comprehensive. It addresses the shortcomings identified in the initial implementation phase of the NIS 1 Directive into the national laws of Member States.

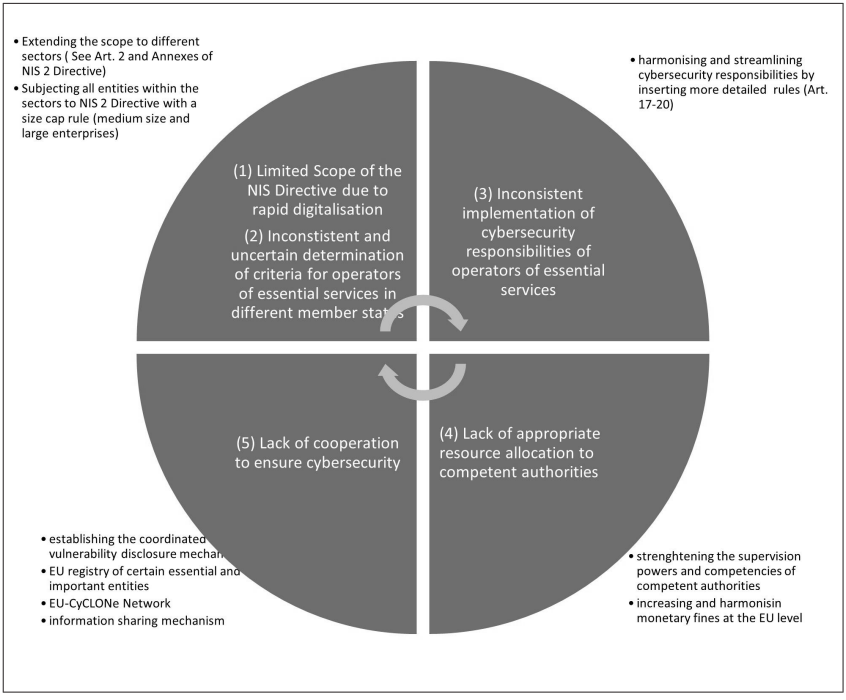

Figure 1: Overview of Challenges of NIS Directive and its Responses in NIS 2 Directive (Source: author)

As illustrated in Figure 1, the evaluation of the NIS 1 Directive underscored the need for systemic and structural changes, prompting the NIS 2 Directive. The NIS 2 Directive introduces several key enhancements aimed at strengthening the EU's cybersecurity framework (Vandezande, 2024). Firstly, it expands the scope to include a broader array of sectors and enterprises, reflecting the current digital reality and the critical nature of various services (Sievers, 2021, p. 2). This adjustment ensures that more entities are covered under the Directive, thereby enhancing the Union's overall security landscape. Secondly, the NIS 2 Directive aims to harmonise the cybersecurity requirements across Member States (Art. 21 NIS 2 Directive). It establishes clearer guidelines and criteria, aimed at minimising the previous ambiguities that led to inconsistent implementations of the NIS 1 Directive (Michels and Walden, 2018; Didenko, 2020). Thirdly, the NIS 2 Directive more strongly emphasises reporting incidents by providing more detailed requirements in such reports (Schmitz-Berndt, 2023). Thus, it requires more stringent and detailed obligations for entities, thus enhancing the resilience and response strategies against cyber threats. Fourthly, the Directive also aims to improve the mechanisms for cooperation both at national and EU levels, ensuring closer coordination when handling cyber incidents and crises. Fifthly, it strengthens the supervision and enforcement mechanisms of competent authorities, among others, by setting administrative fines for the breach of cybersecurity obligations imposed upon private and public actors.

However, it should be borne in mind that the Directive aims for minimum harmonisation in the realm of the EU's cybersecurity (Art. 5), meaning that Member States are given the flexibility to develop or maintain cybersecurity measures that exceed the established minimum requirements of the NIS 2 Directive, provided these enhanced measures are consistent with other obligations under EU law. This approach acknowledges the diverse cybersecurity needs and capabilities of different Member States while ensuring a foundational level of security that supports the collective resilience of the EU's digital sphere.

Due to its very nature (i.e., a Directive), the NIS 2 needs to be transposed to the domestic law of Member States. According to Art. 41, EU Member States are required to adopt and publish any necessary compliance measures by 17 October, 2024, and must begin implementing these measures the following day. Once done, Member States are obliged to notify the European Commission (EC) as soon as possible. In addition, any legislative

or regulatory actions taken by Member States to comply with the Directive must specify that they are referencing it explicitly.

Following this brief overview, the remainder of this Chapter seeks to examine the scope, objective, and responsibilities of different stakeholders (Member States, private and public actors, and the coordination between them at the EU level). For this purpose, Section 2 provides an analysis of the scope and purpose of the NIS 2 Directive. Section 3 analyses the obligations of Member States and the frameworks for cooperation at both national and European levels. Section 4 examines the obligations of the private and public actors recognised as essential and important entities. Finally, Section 5 offers certain conclusions.

2. The scope and objective of the NIS 2 Directive

This section explores four key areas: personal, jurisdictional, and material scope of the NIS 2 Directive, as well as the Directive's underlying aim. Personal scope refers to those who are responsible under the NIS 2 Directive, while jurisdictional scope pertains to how the jurisdictions of Member States are determined, and the material scope concerns what responsibilities the Directive imposes to ensure cybersecurity.

2.1 Personal scope of the NIS 2 Directive

The NIS 2 Directive applies to public and private entities in a sector referred to in Annexes I and II, which are qualified as medium-sized enterprises or those which exceed the threshold for such companies (i.e., those with over 250 employees, an annual turnover of more than 50 million EUR, and/or an annual balance sheet total of over 43 million EUR).

However, there are exceptions to this rule determining the scope. For instance, the NIS 2 Directive applies to entities regardless of the size specified in Annex I (Sectors of High Criticality) and Annex II (Other Critical Sectors), such as providers of public electronic communications networks or of publicly available electronic communications services, trust service providers, top-level domain name registries, and domain name system service providers (Art. 2(2)). This exception arises due to the criticality of the availability of these services for the operations of digital services, regardless of their categorisation as medium-size enterprises.

Moreover, Art.2(6)–(8) provides exceptions for the Directive's application to entities concerned with national security. This exception is due to the EU's lack of competence in relation to national security.

2.1.1 Bifurcation of entities under the NIS 2 Directive: Essential and important entities

Entities covered by the NIS 2 Directive are classified into two categories, "essential" and "important," based on their impact and criticality within their respective sectors (Art. 3). This distinction allows for a nuanced and risk-based approach to cybersecurity, ensuring that entities with the highest impact on cybersecurity are subject to more stringent security measures.

By defining these categories, the NIS 2 Directive not only prioritises where stringent cybersecurity measures are most needed, but also supports a broader goal of fostering a secure, resilient, and EU-wide digital environment. This approach ensures that the most critical services are subject to stringent supervision, while still maintaining a protective stance over other significant sectors. The classification of entities as either essential or important allows for a risk-based approach to their supervision.

Essential entities are those identified as critical to the infrastructure of societal and economic activities. According to Art. 3(1), essential entities include those which exceed the size of medium enterprises and operate within such crucial sectors as transport and digital infrastructure (Annex I). For example, the transport sector covers entities including air carriers, airport managing bodies, and railway undertakings – all of which are crucial for maintaining both freight and passenger mobility across (inter)national boundaries. As another example, digital infrastructure consists of internet exchange point providers, Domain Name System (DNS) service providers, and cloud computing service providers, reflecting the critical nature of maintaining robust digital services and infrastructure.

Important entities, while presumably not on the same critical scale as essential entities, still play significant roles within their sectors. Art. 3(2) (Annexes I and II) outline the scope of sectors which fall into this category. These entities are integral to supporting the functionality of broader societal and economic systems, but may have presumably a lesser direct impact on the availability of the critical services in society. Examples of these include postal and courier services, waste management, the manufacturing sector, and digital providers (online marketplaces, social networking services platforms, and online search engines).

According to recent estimates, the NIS 2 Directive is set to impact over 100,000 entities across the EU (EY, 2023). To establish the list of essential and important entities according to Art. 3(3)–(4), Member States must require those entities to submit specific information to the competent authorities. This includes the entity's name, its address, and current contact details, such as email, IP ranges, and telephone numbers. Additionally, entities must provide details about the relevant sector and subsector to which they belong (Annexes I and II), if applicable. This list shall be established by 17 April, 2025.

2.1.2 The different supervision and enforcement regime for essential and important entities

Indeed, under Arts. 21–24, essential and important entities share the same responsibilities (as discussed in Section 4). The categorisation of essential and important entities under the Directive is relevant for the supervision regime to which these entities are subject. While essential entities are subject to a fully-fledged supervision and enforcement regime (both ex-ante and ex-post), important entities shall be subject to a light ex-post supervisory framework.

Fully-fledged supervision means that competent authorities shall exercise their supervision and enforcement powers regardless of any indication of non-compliance of essential entities under Art. 32. In other words, without any indication of a cybersecurity incident, competent authorities can initiate random checks and on-site inspections for essential entities (Art. 32(a)).

In contrast, ex-post supervision and enforcement means that ex-post supervision by competent authorities may be initiated for important entities upon any indication on the probable non-compliance of those entities brought to the attention of competent authorities (Art. 33).

The underlying objective of this differentiation can be found in Recital 16 of the NIS 2 Directive. According to this Recital, which has an interpretative value despite its non-binding nature, the different supervision regimes to essential and important entities are based on the risk-based approaches and resource-allocation methods of the competent authorities. This approach implies that the risk of cybersecurity incidents occurring in the operations of important entities presumably cause comparably less harm to society than those of essential entities. Regarding the resource allocation of the competent authorities, more can be allocated to the full-fledged supervision and enforcement of essential entities.

2.2 Jurisdictional scope of Member States under the NIS 2 Directive

Art. 26 establishes jurisdictional scope of the Directive. As a main rule, important and essential entities fall within the jurisdiction of the Member States where they were established. However, there are three exceptions for this rule.

The first relates to entities that provide public electronic communication or publicly available electronic communication services. The second concerns digital services, and considers their intrinsic borderless nature. As per Art. 26(1)(b), among others, these entities include a variety of digital service providers, such as DNS providers, cloud computing services, and social media platforms. These entities are subject to the jurisdiction of the Member States where they have their "main establishment".

The definition of "main establishment" is further clarified in Art. 26(2) as the location where key decisions regarding cybersecurity risk management are made. If such a location cannot be determined, the main establishment is where cybersecurity operations are conducted or, failing that, to the establishment with the highest number of employees within the Union. This multi-tiered approach ensures that an entity cannot evade supervision by fragmenting operations across multiple locations. The third exception relates to public administration entities, placing them under the jurisdiction of the Member State that established them, thus aligning with traditional principles of governmental jurisdiction.

The NIS 2 Directive is also applicable entities that were not established in the EU but offer services within it (Art. 26(3)). Such entities must designate a representative in the EU, with jurisdiction falling to the Member State where this representative is located. This provision ensures that entities affecting EU citizens are accountable, even if based outside the Union.

2.3 Material scope of the NIS 2 Directive: data and availability of services as proxies to protect individuals and society

Cybersecurity is defined as the activities required to secure network and information systems, their users, and other people affected by cyber threats under Art. 2(1) of the Cybersecurity Act (EU) 2019/881. Article 6(3) of the NIS 2 Directive borrows the cybersecurity definition from the Cybersecurity Act.

This definition consists of two main components: the activities (1) and the security of network and information systems, their users, and people affected by cyber threats (2).

(1) Activities: There is no specific definition of the activities stipulated under the Cybersecurity Act. Instead, I here use the general definition of "activities". Activities mean actions conducted. More specifically, in the context of cybersecurity, these are all types of actions required to ensure the security of network information. Papakonstantinou (2022) coined the term of "cybersecurity as *praxis*" for the activities that ensure the security of networks and information systems. These measures and actions ensure that network and information systems cover organisational and technical processes for the security of network and information systems.

(2) The security of network and information systems, users, and other people affected by cyber threats: There is no definition of the security of network and information systems in the EU Cybersecurity Act. However, the NIS 2 Directive defines both of these.

Art. 6(1) of the NIS 2 Directive defines "network and information systems" as:

> (a) an electronic communications network within the meaning of Article 2, point (1), of Directive (EU) 2018/1972; (b) any device or group of interconnected or related devices, one or more of which, under a program, perform automatic processing of digital data; or (c) digital data stored, processed, retrieved or transmitted by elements covered under points (a) and (b) for their operation, use, protection, and maintenance.

Additionally, Art. 6(2) states that the "security of network and information systems" means "the ability of network and information systems to resist, at a given level of confidence, any action that compromises the availability, authenticity, integrity, or confidentiality of stored or transmitted or processed data or the related services offered by, or accessible via, those network and information systems". Thus, this security can be roughly defined as "being resilient to cyber threats". Cyber threats are specifically defined in Art. 4(8) of the EU Cybersecurity Act as "any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact network and information systems, the users of such systems and other persons". This component refers to the desired aim of cybersecurity, which is to ensure the security of network and information systems and its impact on its users and natural persons.

Neither the EU Cybersecurity Act nor the NIS 2 Directive clearly define users and other people. However, it is worth mentioning that the users of network and information systems include not only natural persons, but also legal ones, which is one of the ways of differentiating the scope of cybersecurity from data protection.

Cybersecurity is not a goal in and of itself, but rather aims to protect a variety of public and private interests. In so doing, the NIS 2 Directive uses data as proxies to protect these interests. The definition of "cybersecurity" in the EU Cybersecurity Act, in conjunction with the definition of security of network and information systems under the NIS 2 Directive, refers to the protection of data (both personal and non-personal) and the availability of services as proxies for protecting those interests (Brinker, 2024). The inclusion of personal data within the scope of cybersecurity responsibilities, as evidenced by the coordination framework under Art. 35 of the NIS 2 Directive with data protection authorities in addition to the inclusion of personal data into the definition of network and information systems, underscores the dual need to prevent data breaches and mitigate their consequences. Non-personal data are defined as the opposite of personal data, which is any information related to a natural person (Art. 4(1) of the General Data Protection Regulation (EU) 2016/679).[1] Non-personal data, while not directly linked to individual identities, hold significant value for the functioning of services and the broader economy (Pałka, 2023). This data type, encompassing everything from operational data in industrial systems to anonymised datasets used for big-data analytics, is critical for the operational continuity of services across the EU. The NIS 2 Directive's coverage of non-personal data reflects an understanding that the security of such data is important to preventing disruptions and maintaining trust in digital services.

Under the scope of the NIS 2 Directive, both personal and non-personal data play a critical role in cybersecurity. Personal data include such information as customer names, contact details, payment information, and browsing history held by online marketplaces. Such data are directly tied to individuals and must be protected to prevent identity theft, fraud, and privacy violations. On the other hand, non-personal data cover such operational information as product inventories, anonymised user behaviour analytics, pricing algorithms, and logistical information within these mar-

1 For more information about the GDPR, see Chapter 14 'EU Data Protection Law in Action: Introducing the GDPR' by Julia Krämer.

ketplaces. Although these data are not linked to specific individuals, their protection is essential for maintaining the efficiency and continuity of marketplace operations. The disruption or manipulation of non-personal data could lead to supply chain issues, distorted market information, or loss of trust in digital services. Therefore, the NIS 2 Directive's inclusion of both types of data reflects its broad approach to safeguarding critical digital ecosystems.

By imposing uniform cybersecurity responsibilities on all entities within its scope, the NIS 2 Directives minimises the variations in national implementations that previously led to disparities in cybersecurity readiness and response across the EU. This uniformity is crucial for creating a level playing field, ensuring that all critical sectors maintain high standards of data security, thereby enhancing collective cyber defences. The NIS 2 Directive also plays a significant role in bolstering trust among market participants and the public sector regarding cross-border data processing. By clarifying the security obligations for data, the NIS 2 Directive strengthens legal clarity for entities engaged in data processing and outsourcing, particularly in transnational contexts. This clarity is vital for entities relying on digital services that cross national boundaries, as it assures them of the continuous protection of their data under a unified EU-wide cybersecurity regime. Moreover, by encompassing all data types in its cybersecurity mandate, the Directive indirectly discourages data localisation practices that are often adopted as proxies for data security, which aligns with the Free Flow of Non-Personal Data Regulation (Regulation (EU) 2018/1807).

The availability of services is used as another proxy, which is mentioned as part of the security of network information systems under Art. 6(2) of the NIS 2 Directive. This shows the Directive's aim to make available those services that are minimally affected by cyber threats. All in all, the material scope of the Directive is not only the protection of data processed by essential and important entities, but also the continuity of the critical services they provide.

2.4 Objective of the NIS 2 Directive: solving underinvestment problem in cybersecurity

The objective of the NIS 2 Directive, similar to its predecessor (NIS 1), is to incentivise the investment in cybersecurity by private and public actors. There is an underlying assumption of the legal rules for cybersecurity that

more investment means a more secure digital environment. This assumption is predicated on the observation that, without a legal requirement, there is a dearth of investment in cybersecurity (discussed below in terms of underinvestment).

Threats from cyberspace can endanger society and citizens' security or safety (Taddeo, 2013). Significantly, the increased interconnectedness of various devices and systems across industries broadens the scope of cybersecurity policy problems (Lin and Saebeler, 2019). Due to how cybersecurity threats can harm individuals and society rather than organisations themselves, and the ways in which the harm may be dispersed, the firms or entities that use these information systems must take precautions to reduce the risk of cyber incidents. Taking action, on the other hand, has costs. When businesses make decisions, it is believed that they do so based on cost-benefit analyses due to the profit-making nature of their activities (Gordon, Loeb and Lucyshyn, 2014). These analyses are often conducted based on the costs likely to be incurred in the event of a security breach, such as actual harm caused by the breach and reputational damage in the event of exposure (Bauer and van Eeten, 2009). Underinvestment in cybersecurity results from failing to account for negative externalities, such as the costs suffered by other people or enterprises (Frye, 2002). The following statement by the executive of Sony Pictures illustrates the underinvestment issue in the cybersecurity context. The former executive director of Sony Pictures was quoted as saying, "[I]t's a reasonable business decision to take the risk of a security breach", and, in 2015, refused to invest $10 million to avert a possible 1$ million loss (Kostadinov, 2015). In another example, Cortez and Dekker (2022) held semi-structured interviews with 11 Chief (Information) Security Officers in the Benelux region, finding that firms' practises in relation to underinvesting in cybersecurity may be shifting, at least on the margins due to digitalisation during COVID-19 and the increased awareness amongst corporate stakeholders that cybersecurity is a key enabler (and disabler) of business continuity and resilience.

To fix this underinvestment issue, governments should make businesses responsible for reducing the security risks they pose (Clark-Ginsberg and Slayton, 2019). The NIS 2 Directive is a response to this problem as it requires public and private actors to ensure the security of network and information systems during their activities. If they are not compliant with these responsibilities, they can be faced with monetary fines or other sanctions.

Concerning the underinvestment problem and its relation with the adoption of the NIS 1 Directive, Porcedda (2018) described underinvestment as a root cause for the NIS 1 Directive's reason to impose cybersecurity responsibility upon certain private actors. To determine how the NIS 1 Directive (as the predecessor to the NIS 2 Directive) incentivised these actors to invest in cybersecurity, the European Network and Information Security Agency (ENISA) published reports on network and information systems investments in 2020 (ENISA, 2020). According to the report, the average expenditure on network and information system security by operators subject to the NIS 1 Directive was 40% lower than that of their US counterparts. The ENISA also issued a follow-up report in 2021, encompassing all 27 EU Member States and providing new insights into the allocation of network and information system budgets of the operators of essential services (OES)/ digital service providers (DSP) (ENISA, 2021). A survey of 947 organisations designated as OES/DSP across the 27 Member States was used to obtain data. In this second version of the report, in addition to covering all Member States, additional and supplementary questions were asked of the organisations assessed. Overall, 48.9% of the organisations polled said the NIS 1 Directive had a very significant or major impact on their cybersecurity. The fourth version, which included data collected from 1,080 OES/DSPs across all 27 EU Member States, affirmed the role of the NIS 1 Directive in cybersecurity investment in the EU (ENISA, 2023). As the NIS 2 Directive replaces the NIS 1 Directive, the objective to solve the underinvestment problem is still relevant for the former.

3. Responsibilities of Member States and cooperation structures for cybersecurity

This section consists of two parts. The first deals with the roles and responsibilities of Member States under the NIS 2 Directive for cybersecurity. The second concerns cooperation and collaboration within the realm of cybersecurity.

3.1 Responsibilities of Member States

State responsibilities in the realm of cybersecurity reflect the growing recognition that digital infrastructure is as vital to the security as physical

infrastructure. As discussed below, the adoption of cybersecurity strategies by Member States delineates the scope of proactive measures that states foresee to take. Cybersecurity is no longer merely a technical issue, but rather a matter of national resilience, where States play a role in creating protective frameworks. As another role of fostering collaboration between public and private actors to deal with cybersecurity incidents, Member States are tasked with establishing computer security incidents response teams and national cyber crisis management frameworks. These frameworks help States prepare for future cybersecurity incidents and form coordinated responses. A central aspect of state responsibility in cybersecurity is the enforcement of cybersecurity responsibilities by different public and private actors (see Section 4). This implementation is only possible by establishing competent authorities with appropriate enforcement power and competences.

3.1.1 Cybersecurity strategies

First, under Art. 7 of the NIS 2 Directive, each Member State is required to develop a national cybersecurity strategy that clearly outlines the strategic objectives and priorities, especially targeting critical sectors identified in the annexes of the Directive. The strategy must detail the necessary resources and a variety of policy and regulatory measures aimed at achieving and maintaining a robust level of cybersecurity. This includes a comprehensive governance framework to ensure the achievement of these objectives, which involves clear definitions of the roles and responsibilities of key stakeholders, such as national competent authorities, single points of contact, and Computer Security Incident Response Teams (CSIRTs).

The strategy shall establish effective cooperation and coordination both at the national level and with sector-specific authorities. Furthermore, the strategy must feature mechanisms for identifying key assets and assessing risks, policies for improving incident preparedness, response, and recovery, and cooperation between the public and private sectors. It should also list all authorities and stakeholders involved and establish a policy framework for information sharing on cyber and non-cyber risks and incidents among competent authorities.

Raising public awareness about cybersecurity is another critical component, aimed at enhancing the general cybersecurity knowledge of citizens. The strategy is also expected to cover policies related to cybersecurity in ICT supply chains, the inclusion of cybersecurity standards in public

procurement, and the management of vulnerabilities, including promoting coordinated vulnerability disclosure (Art. 12). Additionally, it must address the protection of the public core of the internet, promote the use of advanced cybersecurity technologies, and enhance cybersecurity education, training, and research. The strategy should support voluntary information sharing in accordance with Union law, strengthen cyber resilience and hygiene, particularly in small and medium-sized enterprises, and promote active cyber protection measures.

Member States must notify the EC of their adopted strategies within three months, keeping certain national security information confidential if necessary. They are also obliged to regularly assess and update their strategies at least every five years based on key performance indicators, with support available from the ENISA to ensure alignment with the Directive's requirements and obligations.

3.1.2 National cyber crisis management frameworks

The second requirement is to establish national cyber crisis management frameworks, outlined under Art. 9 of the NIS 2 Directive. These frameworks should be designed so as to handle large-scale cybersecurity incidents and crises effectively. Each Member State is required to designate or establish one or more competent authorities tasked with this critical role. These authorities, known as cyber crisis management authorities, must be equipped with adequate resources to perform their duties efficiently and effectively (Art. 9(1)). To ensure a unified approach to cyber crisis management, these frameworks must align with existing national crisis management systems. When multiple cyber crisis management authorities are established, a clear delineation of responsibilities is necessary, including the designation of a lead authority to coordinate the response to significant cybersecurity incidents and crises (Art. 9(2)). These authorities are also responsible for identifying necessary capabilities, assets, and procedures that can be mobilised in a crisis. Furthermore, each Member State must develop a comprehensive response plan for large-scale cybersecurity incidents and crises. This plan should outline the objectives of national preparedness measures, detail the responsibilities of the cyber crisis management authorities, and describe the procedures for managing cyber crises, including their integration into broader national crisis management frameworks and communication channels (Art. 9(4)). The plan should also include preparedness measures, such as regular exercises and training, and delineate

the roles of relevant public and private stakeholders. Within three months of establishing a cyber crisis management authority, Member States must notify the EC and the European cyber crisis liaison organisation network (EU-CyCLONe) of the authority's identity and any changes thereafter, as well as provide details of their national response plans, while maintaining the necessary discretion for national security reasons.

3.1.3 Establishment of competent authorities and single points of contact for cybersecurity

Under Art. 8 of the NIS 2 Directive, each Member State is mandated to designate or establish one or more competent authorities responsible for overseeing cybersecurity and performing supervisory duties. These authorities play a pivotal role in monitoring the implementation of the Directive at the national level.

Additionally, each Member State is required to designate a single point of contact to streamline communications and enhance cooperation. In cases where a Member State establishes only one competent authority, this entity also assumes the role of the single point of contact. The single point of contact is crucial for ensuring effective liaison functions, facilitating cross-border cooperation with authorities from other Member States, and engaging with the ENISA and EC. This role also extends to fostering cross-sectoral cooperation within the Member State, thus ensuring a cohesive approach to national cybersecurity efforts.

Member States must ensure that their designated competent authorities and single points of contact are equipped with sufficient resources to efficiently and effectively conduct their assigned tasks, thereby achieving the objectives outlined in the Directive. Member States are also required to promptly notify the Commission of the identity of these designated authorities and any changes to their roles or responsibilities. The identity of each competent authority is to be made public, and the EC is tasked with maintaining and publishing a list of all single points of contact to facilitate transparency and accessibility.

3.1.4 Computer Security Incident Response Teams (CSIRTS)

Under the NIS 2 Directive, each Member State is mandated to designate or establish one or more CSIRTs tasked with specific cybersecurity respon-

sibilities. These teams play a crucial role in managing and responding to cybersecurity incidents on a national level, and the scope of their competence must cover at least the sectors, subsectors, and types of entities listed in Annexes I and II of the Directive (Kamara and van den Boom, 2022).

To ensure effective operations under Art. 11, CSIRTs are required to comply with stringent requirements, including maintaining secure and resilient communication and information infrastructures to facilitate robust information exchanges with key stakeholders. CSIRTs' responsibilities include monitoring and analysing cybersecurity threats, vulnerabilities, and incidents within their jurisdictions. They are also tasked with providing timely warnings, alerts, and the dissemination of critical information to relevant entities and stakeholders, aiding in the (near) real-time monitoring of network and information systems (Art. 11(3)(a)). Additionally, CSIRTs respond to incidents and offer necessary assistance to affected entities, undertake forensic data analyses, and contribute to dynamic risk assessments and situational awareness concerning cybersecurity (Art. 11(3)(d)). Furthermore, CSIRTs are pivotal in the proactive scanning of networks to detect vulnerabilities, thus playing a proactive role in securing national and cross-border cyber infrastructures (Art. 11(3)(e)).

For example, under Art. 11 of the NIS 2 Directive, a national CSIRT might work closely with a large online marketplace, such as an e-commerce platform, to maintain secure communication channels. If the marketplace detects unusual activity indicative of a potential cyberattack, such as unauthorised access to customer data, the team would provide immediate support by analysing the incident and offering technical assistance. They would also issue timely alerts to other stakeholders, such as payment processors or logistics providers, to mitigate the broader impact. Additionally, the CSIRT might proactively scan the marketplace's network for vulnerabilities, such as weaknesses in payment gateways or customer databases, and provide guidance on how to strengthen its defences to prevent future incidents.

To bolster their effectiveness, CSIRTs are encouraged to engage in international cooperation and establish cooperative relationships with their counterparts in other countries. This global networking aims to enhance their capability to manage cyber threats more effectively and share critical information under secured protocols, including the traffic light protocol. They also participate in the CSIRTs network, providing mutual assistance and sharing best practices and technologies, thus further strengthening their response to cybersecurity challenges (Art. 11(3)(f)). The Directive also emphasises the importance providing these teams with sufficient resources

and access to secure working environments and redundant systems to ensure the continuity of their services (Art. 11(2)). Moreover, each Member State is required to designate one of its CSIRTS as a coordinator for vulnerability disclosure (Art. 11(3)(g)).

3.1.5 Cooperation at the national level

Under Art. 13 of the NIS 2 Directive, national-level cooperation among various cybersecurity bodies within Member States is crucial. Competent authorities, single points of contact, and CSIRTs are required to work collaboratively to fulfil the Directive's obligations. This includes the sharing and handling of notifications regarding significant incidents, cyber threats, and near misses. It also mandates that these entities not only cooperate internally, but also engage with law enforcement, data protection authorities, and other relevant national regulatory authorities. This integrated approach ensures that all notifications are effectively managed and that consistent information flow is maintained across different regulatory frameworks, thereby enhancing the level of national cybersecurity.

3.2 European vulnerability database and EU-level cooperation

This section discusses two main areas: the European vulnerability database and the EU-level cooperation structures designed in the NIS 2 Directive.

3.2.1 European vulnerability database

Art. 12 of the NIS 2 Directive requires coordinated vulnerability disclosure, achieved through the establishment of a European vulnerability database. The ENISA is tasked with developing and maintaining this database, which will serve as a central resource for registering publicly known vulnerabilities on a voluntary basis, providing access to all stakeholders. It is designed to enhance the security and integrity of ICT systems by including detailed information about each vulnerability, the affected products or services, the severity of the vulnerability, available patches, and, where patches are not available, guidance on mitigating risks. This structured approach to vulnerability disclosure and the centralisation of vulnerability information is aimed at strengthening cybersecurity across the EU by ensuring the timely

and effective communication and management of vulnerabilities, thereby reducing the risk of exploitation and enhancing the overall resilience of ICT infrastructures.

The focus on Art. 12's mandate for a European vulnerability database underscores the EU's commitment to transparency and security in managing ICT vulnerabilities. This database will play a pivotal role in centralising information on known vulnerabilities, thereby facilitating timely access to essential details for stakeholders across the EU. While the database's voluntary nature aims to encourage wide participation, this could be a double-edged sword, as it may limit comprehensive data collection if some stakeholders choose not to participate. Nonetheless, the overall goal is to create a more resilient and secure digital ecosystem by fostering coordinated vulnerability disclosure and information sharing.

3.2.2 EU-level cooperation

The NIS 2 Directive establishes a sophisticated structure for cooperation at both the EU and international levels to enhance the overall cybersecurity posture across Member States. This is articulated through the establishment of the Cooperation Group, the CSIRTs network, and the EU-CyCLONe, each playing a crucial role in facilitating strategic cooperation, information exchange, and coordinated response to cybersecurity incidents and vulnerabilities.

According to Art. 14, the Cooperation Group serves as a platform for strategic cooperation among Member States, fostering the trust and confidence necessary for effective cybersecurity governance. Comprised of representatives from Member States, the EC, and ENISA, the group is tasked with a wide array of responsibilities.

These include providing guidance on the transposition and implementation of the Directive (Art. 14(4)(a)), developing and implementing policies on coordinated vulnerability disclosure (Art. 14(4)(b)), exchanging best practices, and collaborating on emerging cybersecurity policy initiatives (Art. 14(4)(o)). The Group operates under biennial work programmes and includes a variety of participants, including the European External Action Service as an observer, which ensures a comprehensive approach to addressing cybersecurity issues (Art. 14(3)).

The Cooperation Group, through its strategic role, aims to harmonise the Directive's implementation across Member States, promoting a sense of unity in addressing cybersecurity challenges. The challenge here lies in bal-

ancing national interests with EU-level goals, especially in an environment that demands both trust and transparency among the Member States.

The network of national CSIRTs under Art. 15 is a critical component of the EU's cybersecurity infrastructure, promoting swift and effective operational cooperation among Member States. Moreover, it facilitates the exchange of information regarding capabilities, incidents, cyber threats, and vulnerabilities, and also plays a key role in coordinating responses to cross-border cyber incidents. ENISA provides the secretariat for the CSIRTs network, enhancing the support for cooperation among teams (Art. 15(2)). This network ensures that Member States are both informed and prepared to manage and mitigate cybersecurity incidents effectively.

As per Art. 16, EU-CyCLONe is aimed at improving the coordination of large-scale cybersecurity incidents and crises at the operational level. It helps in developing a shared situational awareness and supports decision-making processes during such crises. Composed of representatives from Member States' cyber crisis management authorities and the EC, EU-CyCLONe assesses the impact of large-scale incidents and proposes mitigation measures.

This organisation plays a crucial role in ensuring that Member States are prepared for, and can effectively manage, significant cybersecurity challenges. Under the Directive, EU-CyCLONe's tasks allow for a robust interaction between different cybersecurity bodies within the EU (Art. 16(3)). This includes regular meetings, joint exercises, and continuous information sharing that spans technical details to strategic policies. By fostering an environment where Member States can request assistance, share operational practices, and partake in joint supervisory actions, the Directive ensures that cybersecurity measures are not only unified across the EU, but also adaptable to the evolving nature of cyber threats.

Art. 19 introduces a voluntary peer review system, facilitated by the Cooperation Group with support from the EC, ENISA, and the CSIRTs network.

The system aims to promote shared learning, strengthen mutual trust, and enhance cybersecurity across Member States. The reviews focus on various aspects of cybersecurity, including risk management measures, reporting obligations, competent authorities' capabilities, operational capabilities of CSIRTs, mutual assistance, information-sharing arrangements, and cross-border or sector-specific issues. The methodology and review process are objective, non-discriminatory, transparent, and fair, incorporates both virtual and physical assessments, and ensure that information exchanges

adhere to confidentiality standards and national security protection. The experts are obligated to maintain the confidentiality of sensitive information and disclose any findings to third parties.

Post-review, the experts draft a report summarising their findings and conclusions, including recommendations for improvements. The reviewed Member State can comment on this draft, which is appended to the final report.

Recital 75 of the NIS 2 Directive emphasises that peer reviews should complement existing mechanisms, such as the CSIRTs network peer review system, avoiding the duplication and leveraging of past results. This framework supports the improvement of individual Member States' cybersecurity and fosters a collaborative environment where best practices are shared and collective cybersecurity resilience is bolstered.

4. Responsibilities of important and essential entities for cybersecurity under the NIS 2 Directive

The responsibility for ensuring cybersecurity rests largely with essential and important entities. There are three main responsibilities which these entities must bear. The first directs the managerial board to be personally involved in cybersecurity. The second is risk management responsibility, aimed at mitigating cyber risks arising from the operations of these entities. The third is the reporting of cybersecurity incidents to the competent authorities or CSIRTS, to recipients of their services, as well as to the public, where appropriate. In addition to these responsibilities, the NIS 2 Directive introduces a voluntary information-sharing framework on cybersecurity among these entities. This section analyses these responsibilities and this framework.

4.1 Responsibilities of managerial boards

The NIS 2 Directive addresses concerns related to the involvement of management boards in cybersecurity within essential and important entities. Recognising the limitations in management boards' engagement with cybersecurity issues, the Directive imposes new responsibilities to enhance this engagement and address the identified deficiencies.

Historically, senior management figures, such as chief executive officers (CEOs), chief financial officers (CFOs), and chief information officers

(CIOs) have been primarily responsible for overseeing a firm's cybersecurity strategies, which include assessing and mitigating security breaches. Research has indicated that IT expertise within the board is positively associated with a company's preparedness for cybersecurity incidents (Hartmann and Carmenate, 2021). Studies have shown that CEOs with IT expertise are more likely to detect and report breaches, and the presence of such IT executives as CIOs on the management team correlates with a reduced likelihood of security breaches and better overall preparedness (Haislip et al, 2017). Despite these positive associations, corporate boards continue to be general unprepared to handle cybersecurity incidents. A survey conducted by Cheng et al, (2021) revealed that only a minority of directors have an above-average or excellent awareness of their cybersecurity processes, highlighting a significant gap in effective cybersecurity management at the board level. This ineffectiveness is often compounded by a lack of necessary expertise and inadequate involvement in proactive cybersecurity management, which leads to cybersecurity being treated as a lower priority issue that is often delegated to lower operational levels.

The NIS 2 Directive aims to rectify these shortcomings by explicitly requiring management boards to approve and oversee the cybersecurity risk management measures of their entities. Art. 20(1) mandates that Member States ensure that management bodies of essential and important entities not only approve, but also actively oversee, these risk management measures. Furthermore, to address the expertise gap, Art. 20(2) stipulates that board members must undergo training to enhance their understanding of cybersecurity risks, which should also be regularly encouraged for all employees. Additionally, the Directive strengthens accountability by providing enforcement powers to hold management boards liable for non-compliance with their cybersecurity obligations. According to Arts. 32(6) and 33(5), respectively, natural persons acting as representatives of essential and important entities (likely including members of the management board) can be held personally liable for breaches of the Directive's responsibilities. The specifics of this liability are determined by individual Member States, but the inclusion of such measures underscores the Directive's serious commitment to ensuring management boards' active and knowledgeable involvement in cybersecurity.

In sum, the NIS 2 Directive introduces targeted measures to significantly enhance the role of management boards in cybersecurity, addressing well-documented gaps in involvement and expertise. By mandating direct oversight and accountability of management boards in cybersecurity matters,

coupled with required training for board members, the Directive aims to elevate the strategic importance of cybersecurity within corporate governance structures and ensure a more robust and proactive management of cybersecurity risks.

4.2 Risk management responsibility

The NIS 2 Directive revises the risk management framework established by its predecessor, focusing on enhancing and clarifying the responsibilities of essential and important entities rather than introducing substantial structural changes.

The NIS 2 Directive delineates several key areas of adjustment, primarily aimed at providing a more comprehensive and nuanced understanding of cybersecurity risks and management. First, the NIS 2 Directive modifies the terminology used in its predecessor, changing "Security Requirements" to "Cybersecurity Risk Management Measures". This change, reflected in Art. 21 of the NIS 2 Directive, aims to encapsulate a broader definition of cybersecurity, not only ensuring the security of network and information systems, but also safeguarding the users and other parties impacted by cyber threats (Papakonstantinou, 2022; Biasin and Kamenjasevic, 2022). This aligns with the definitions provided in the EU Cybersecurity Act, which include activities necessary to secure both networks and the broader digital environment from cyber threats.

Article 21(1) of the NIS 2 Directive stipulates that entities must adopt appropriate and proportionate technical, operational, and organisational measures to manage risks to network and information systems. These measures are crucial for maintaining the integrity and security of operations and minimising the impact of any incidents on service recipients and other services. While the emphasis on network and information system security continues from NIS Directive 1, its successor introduces clearer language and requirements, specifically addressing the broader impacts of cybersecurity incidents.

A significant aspect of the Directive involves specific requirements across organisational, technical, and operational measures. Entities are mandated to establish robust governance frameworks that clearly define cybersecurity responsibilities and ensure regular staff training. Additionally, they must develop incident response plans and effectively manage risks associated with third-party service providers. Technical measures require entities to

maintain system security through state-of-the-art technology, enforce strict access control, and engage in continuous monitoring to detect and respond to threats promptly. Operational measures under the NIS 2 Directive include conducting regular risk assessments and developing business continuity plans to ensure resilience in the face of disruptions. It also mandates the regular testing and auditing of cybersecurity measures to ascertain their effectiveness. Furthermore, the Directive encourages entities to adopt cyber hygiene practices, which are vital for mitigating risks from social engineering and other cyber threats.

Art. 21 of the NIS 2 Directive also emphasises the importance of proportional measures in cybersecurity. Moreover, Art. 18(1) specifically considers the costs of implementation, the entity's exposure to risks, and the potential societal and economic impacts of incidents when assessing the proportionality of security measures. This ensures that, while the cybersecurity measures should be robust, they should not necessarily aim for perfection, but rather be proportionate to the risks involved. Furthermore, the Directive aligns with international and European standards, such as ISO 27001, which advocates for an all-hazards approach to security, which is specifically mentioned in Recital 79 of the NIS 2 Directive. This approach is not limited to cyber threats, but also includes other potential risks, such as natural disasters or operational disruptions, thus ensuring comprehensive protection across various scenarios.

Upon conducting a statutory interpretation of the NIS 2 Directive and analysing the cyber kill chain model, Ferguson (2023) observed that the cybersecurity risk management measures outlined in the Directive may have significant limitations in effectively mitigating cyberattacks targeting essential and important entities within EU Member States. This limited efficacy was mainly attributed to the restricted extent of the measures, which notably lack specific methods for targeting the reconnaissance phases of cyberattacks. The Directive does not mandate such key security practices as denial, vulnerability scanning, or threat modelling during reconnaissance phases, which are crucial for anticipating threat actor's tactics (Ferguson, 2023). This leaves essential and important entities at risk of losing information superiority as they prepare for future attack phases, especially the weaponisation phase (Ferguson, 2023). Despite access to threat intelligence, essential and important entities are not required to leverage it effectively, potentially compromising their mitigation capacities.

Regarding risk management responsibility, the EC adopted Implementing Regulation (2024/2690) on cybersecurity measures of the NIS 2 Di-

rective for a variety of important and essential entities (including cloud computing service providers and online marketplaces), according to the mandate given in Art. 21(5) of the Directive. The Implementing Regulation, which is directly applicable and does not need to be implemented in national laws, along with its Annex, establishes comprehensive requirements for cybersecurity measures under Art. 21 of the NIS 2 Directive. The purpose of the Implementing Regulation is to establish uniform cybersecurity standards for digital entities across all Member States. Notably, its Annex, spanning 26 pages, exceeds the length of the Regulation itself. It offers a thorough and detailed explanation of key policies, including the security of network and information systems outlined in Art. 21(2)(a) of the NIS 2 Directive, as well as the incident handling policy specified in Art. 21(2)(b).

In conclusion, compared to its predecessor, the NIS 2 Directive's adjustments primarily function to clarify and slightly extend the responsibilities and requirements for cybersecurity risk management. By emphasising a balanced approach that includes robust protection mechanisms and practical, proportionate measures, the Directive aims to enhance the resilience of network and information systems across the EU. The integration of clearer requirements and the expansion of the scope of risk management reflect a concerted effort to foster a safer and more secure digital environment across Europe.

4.3 Reporting responsibility of essential and important entities

In the NIS 2 Directive, there are three different notification responsibilities imposed upon essential and important entities. These are notifications to competent authorities or CSIRTs, the recipients of the services, and to the public.

4.3.1 Notification to CSIRT or competent authorities

According to Art. 23(1) of the NIS 2 Directive, notification to competent authorities or CSIRT is required for any incident having a significant impact on their services. Not all incidents trigger notification responsibility, but those with severe operational disruption or financial losses for the entity concerned are subject to notification. The parameters of an incident having a significant impact include references to not only organisational harm, but

also to considerable material or non-material losses of legal and natural persons, as per Art. 23(3).

The NIS 2 Directive provides a three-tier approach to notification, with reporting conducted at three-time intervals: an early warning, an incident notification, and final reporting. CSIRTs or competent authorities can request an intermediate report on relevant status updates between incident notification and final reporting, as per Art. 23(4)(c). This approach aims to strike a balance between swift reporting and allowing entities to seek support and draw valuable lessons to improve their resilience to cyber threats. Art. 23(4)(a) sets down the scope of an early warning, which entities must submit within 24 hours after essential and important entities become aware of the incident. Recital 102 of the NIS 2 Directive states that this early warning should not result in the diversion of resources for preparation of early warning.

Art. 23(4)(b) sets forth a second notification, called an incident notification, which must be sent within 72 hours of becoming aware of the incident. This notification should include an update on the elements of early warning, an initial assessment of its severity and impact, and indicators of compromise.

Art. 23(4)(d) outlines the submission of the final report, which includes a detailed description of the incident, its severity and impact, the type of threat or root causes, mitigation measures implemented, and its cross-border impacts. If the incident is still ongoing, essential and important entities must provide a progress (instead of a final) report.

4.3.2 Notification to the recipients of services

There are two different notifications to the recipients of the entities' services: notification of the incidents that significantly impact the provision of their services and communication of a significant cyber threat. Despite the novelty of the notification to the recipients under the NIS 2 Directive, the Directive and its Recitals are notably silent on the underlying objective of these notifications. The question is then what would be the objective of requiring entities to notify their recipients of the incident that have a likely adverse impact on the provision of services? This type of notification serves two different purposes, namely deterrence for the entities from taking inappropriate measures due to reputational damage of the incident, and the mitigation of harms caused to the recipients of services. The former is served through its exposure of the incident and possible negligence of the

entities to their clients. It serves the latter by allowing recipients of services to take appropriate measures to mitigate possible damage.

4.3.3 Notification of the incident to the recipients of services

The NIS 2 Directive outlines three conditions for notification to the recipients of the services under Article 23(1): (1) an incident meeting the requirements of a significant impact, (2) an incident likely to adversely affect the provision of the service, and (3) the notification being deemed appropriate. These recipients can be both natural and legal persons.
The scope of notification in the NIS 2 Directive should include the information to serve the objectives of deterrence and mitigation. It should include information on the extent to which recipients of services should take measures to mitigate damages, the potential impact of the incident on recipients, and the overview of technical and organisational measures to mitigate the incident's impacts.

According to Art. 23(1), notification to recipients of service shall be done without undue delay. There is no specific time limit imposed on entities for notification to recipients, but Member States can either stipulate these or provide discretionary guidelines. The time of notification serves the objective of deterrence and mitigation, ensuring that entities notify recipients as soon as possible to prevent collateral damages.

4.3.4 The communication of significant cyber threats to the recipients of services

Art. 23(2) of the NIS 2 Directive mandates Member States to impose responsibility upon essential and important entities to inform recipients of their services affected by a significant cyber threat of any measures or remedies they can take in response. It also requires entities to inform recipients of the threat itself, if applicable. A "significant" cyber threat is defined as one which could severely impact an entity's network and information systems, causing consequential (non-)material losses. The notification of such threats should be given with best efforts and not relieve entities of their obligation to take immediate measures to prevent or remedy the threat and restore the service's normal security level. The information should be free of charge and written in simple language. This responsibility is unique

to the NIS 2 Directive, as it is related not only to the incident, but also to the significant cyber threat. This type of notification can be justified based on the mitigation objective, allowing essential and important entities to inform recipients of a significant cyber threat without undue delay, thereby enabling them to take appropriate measures to mitigate potential losses.

As an illustration, according to Art. 23(2) of the NIS 2 Directive, if an online marketplace experiences a significant cyber threat, such as a vulnerability that could expose customer payment details, the marketplace must promptly inform its users about the threat. This notification would include clear instructions on steps users can take to protect themselves, such as changing their passwords or monitoring their accounts for suspicious activity. The marketplace would also need to explain the nature of the threat in simple, accessible language and provide this information free of charge. Further to informing its users, the marketplace must still take immediate action to fix the vulnerability and restore normal security levels, ensuring the protection of both the users and platform.

4.3.5 Notification to the incident to the public

The NIS 2 Directive imposes the responsibility to notify the public of cybersecurity incidents in certain circumstances. Indeed, Art. 23(7) states that, after consulting with the entities involved in a cybersecurity incident, the relevant authorities or CSIRTs from other affected Member States can inform the public. They may also require these entities to inform the public if awareness is needed to prevent or manage the incident, or if sharing the information is in the public's interest.

4.3.6 Information sharing on voluntary basis

Information-sharing practices are crucial in cybersecurity, as they help prevent, detect, respond to, or mitigate incidents by raising awareness about, and limiting the spread of, cyber threats (Cormack, 2021; Kolini and Janczewski, 2022). Art. 29 of the NIS 2 Directive requires Member States to ensure that essential and important entities exchange relevant cybersecurity information while respecting the GDPR. Recital 119 emphasises the importance of regular threat and vulnerability intelligence sharing between institutions for the effective detection and prevention strategies.

Entities should be encouraged to pool their expertise and experience at strategic, tactical, and operational levels to strengthen their capacity to analyse, monitor, defend against, and respond to cyber threats effectively. Facilitating voluntary information sharing platforms at the Union level is significant. Thus, Member States should actively promote and encourage participation by relevant entities not covered by this Directive.

Art. 29(2) foresees the conclusion of information-sharing arrangements when potentially sensitive information is exchanged, including between the cybersecurity service providers of important and essential entities. Art. 29(3) specifies the scope of these arrangements, specifying operational elements, content, and conditions of information sharing. Member States may impose conditions on information provided by competent authorities or CSIRTs. Art. 7(2)(h) of the NIS 2 Directive requires Member States to support the application of such arrangements, and essential and important entities must notify competent authorities when participating in, or withdrawing from, information-sharing arrangements (Art. 29(4)).

In addition to these, the Directive also stipulates voluntary notification of cyber threats and near misses by essential and important entities under Art. 30(1). It also opens a room for the notification of significant incidents, cyber threats, and near misses by other entities outside the Directive's scope. This provision seeks to obtain a comprehensive situational picture of cybersecurity in the EU without imposing obligations to other entities.

5. Conclusion

The NIS 2 Directive aims to strengthen cybersecurity in the EU by making structural changes to the NIS 1 Directive. It promotes investment in cybersecurity by both private and public entities, recognising that allocating resources for cybersecurity measures is essential for protecting the digital landscape.

A significant challenge for the Directive is the extension of the scope of entities responsible for ensuring cybersecurity. The new categorisation of important and essential entities eliminates the distinction between OESs and DSPs, and subjects all important and essential entities to the same provisions. However, there is a difference in the supervision and oversight regime, with essential entities being subject to full-fledged supervision and important entities only requiring demonstration of compliance ex-post.

The NIS 2 Directive takes a data agnostic approach to cybersecurity, covering all types of data processed by essential and important entities.

It also requires Member States to develop national cybersecurity strategies, outlining strategic objectives, priorities, and resources, as well as establishing effective cooperation and coordination mechanisms between public and private sectors. The Directive establishes a new cybersecurity framework, which includes coordinated vulnerability disclosure and the establishment of a European vulnerability database. The ENISA is made responsible for maintaining this database, which seeks to enhance the security and integrity of ICT systems.

The NIS 2 Directive also establishes a cooperation structure at the EU level, with the Cooperation Group, CSIRTs network, and EU-CyCLONe playing crucial roles in facilitating strategic cooperation, information exchanges, and coordinated responses to cybersecurity incidents and vulnerabilities.

Essential and important entities have responsibilities for network and information system security, including involving the managerial board in cybersecurity, mitigating cyber risks, and reporting incidents to authorities. The NIS 2 Directive introduces a voluntary information-sharing framework to address limitations in engagement with cybersecurity issues. Furthermore, it aims to enhance network and information system resilience by clarifying cybersecurity risk management responsibilities and expanding the scope. It includes notification responsibilities for entities to competent authorities, recipients of services, and the public. Timely and appropriate notifications serve deterrence and mitigation purposes, and collaboration and voluntary information sharing platforms at the Union level are encouraged.

Overall, the NIS 2 Directive aims to strengthen cybersecurity in the EU by addressing the ineffectiveness of cybersecurity management, expanding the scope of entities responsible for cybersecurity, and establishing frameworks for cooperation, information sharing, and incident reporting. It emphasises the importance of investment in cybersecurity and the protection of critical sectors.

Acknowledgements

This research has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101057844 (iFLOWS Project).

References

Bauer, J.M. and van Eeten, M.J.G. (2009) 'Cybersecurity: stakeholder incentives, externalities, and policy options', *Telecommunications Policy*, 33(10–11), pp. 706–719.

Biasin, E. and Kamenjasevic, E. (2022) 'Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive Proposals', *International Cybersecurity Law Review*, 3, pp. 163-180.

Brandão, A.P. and Camisão, I. (2022) 'Playing the market card: The Commission's strategy to shape EU cybersecurity policy', *JCMS: Journal of Common Market Studies*, 60(5), pp. 1335–1355.

Brinker, N. (2024) 'Identification and demarcation – a general definition and method to address information technology in European IT security law', *Computer Law & Security Review*, 52, 105927 [Online]. Available at: https://doi.org/10.1016/j.clsr.2023.105927 (Accessed: 5 February 2025).

Carrapico, H. and Barrinha, A. (2017) 'The EU as a coherent (cyber)security actor?', *JCMS: Journal of Common Market Studies*, 55(6), pp. 1254–1272.

Cheng, J.Y.-J., Groysberg, B., Healy, P. and Vijayaraghavan, R. (2021) 'directors' perceptions of board effectiveness and internal operations', *Management Science*, 67(10), pp. 6399–6420.

Chiara, P.G. (2024) 'Towards a right to cybersecurity in EU law? The challenges ahead', *Computer Law & Security Review*, 53, 105961 [Online]. Available at: https://doi.org/10.1016/j.clsr.2024.105961 (Accessed: 5 February 2025).

Clark-Ginsberg, A. and Slayton, R. (2019) 'Regulating risks within complex sociotechnical systems: evidence from critical infrastructure cybersecurity standards', *Science and Public Policy*, 46(3), pp. 339–346.

'Commission Implementing Regulation (EU) 2024/2690 of 17 October 2024 laying down rules for the application of Directive (EU) 2022/2555 as regards technical and methodological requirements of cybersecurity risk-management measures and further specification of the cases in which an incident is considered to be significant with regard to DNS service providers, TLD name registries, cloud computing service providers, data centre service providers, content delivery network providers, managed service providers, managed security service providers, providers of online market places, of online search engines and of social networking services platforms, and trust service providers (Text with EEA relevance)' (2024) *Official Journal* L [Online]. Available at: https://eur-lex.europa.eu/eli/reg_impl/2024/2690/oj/eng (Accessed: 21 January 2025).

Cormack, A. (2021) 'NISD2: a common framework for information sharing among network defenders', *SCRIPTed: A Journal of Law, Technology and Society*, 18(1), pp. 83–98.

Cortez, E.K. and Dekker, M. (2022) 'A corporate governance approach to cybersecurity risk disclosure', *European Journal of Risk Regulation*, 13(3), pp. 1–23.

Didenko, A.N. (2020) 'Cybersecurity regulation in the financial sector: prospects of legal harmonization in the European Union and beyond', *Uniform Law Review*, 25(1), pp. 125–167.

'Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive) (Text with EEA relevance)' (2022) *Official Journal* L 333, 27 December, pp. 80–152 [Online]. Available at: http://data.europa.eu/eli/dir/2022/2555/oj/eng (Accessed: 18 April 2024).

ENISA (2020) *NIS investments report 2020*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/nis-investments (Accessed: 7 April 2022).

ENISA (2021) *NIS investments report 2021*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/nis-investments-2021 (Accessed: 5 October 2022).

ENISA (2023) *NIS investments report 2023*. ENISA [Online]. Available at: https://www.enisa.europa.eu/publications/nis-investments-2023 (Accessed: 18 April 2024).

European Commission (2020). *Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union*. European Commission [Online]. Available at: https://digital-strategy.ec.europa.eu/en/library/impact-assessment-proposal-directive-measures-high-common-level-cybersecurity-across-union (Accessed: 18 April 2024).

EY (2023) *Five things to know if your company falls under the scope of NIS2*. EY [Online]. Available at: https://www.ey.com/en_dk/cybersecurity/five-things-to-know-if-your-company-falls-under-the-scope-of-nis2 (Accessed: 18 April 2024).

Ferguson, D.D.S. (2023) 'The outcome efficacy of the entity risk management requirements of the NIS 2 Directive', *International Cybersecurity Law Review*, 4(4), pp. 371–386.

Frye, E. (2002) 'The tragedy of the cybercommons: overcoming fundamental vulnerabilities to critical infrastructures in a networked world', *The Business Lawyer*, 58(1), pp. 349–382.

Gordon, L.A., Loeb, M.P. and Lucyshyn, W. (2014) 'Cybersecurity investments in the private sector: the role of governments', *Georgetown Journal of International Affairs*, 15(SI), pp. 79–88.

Haislip, J., Lim, J.H. and Pinsker, R. (2017) 'Do the roles of the CEO and CFO differ when it comes to data security breaches?', in *AMCIS 2017 – America's Conference on Information Systems: A Tradition of Innovation* [Online]. Available at: https://scholars.ttu.edu/en/publications/do-the-roles-of-the-ceo-and-cfo-differ-when-it-comes-to-data-secu (Accessed: 16 November 2022).

Hartmann, C.C. and Carmenate, J. (2021) 'Academic research on the role of corporate governance and IT expertise in addressing cybersecurity breaches: implications for practice, policy, and research', *Current Issues in Auditing*, 15(2), pp. A9–A23.

Jacobs, B. (2023) 'A comparative study of EU and US regulatory approaches to cybersecurity in space', *Air and Space Law*, 48(4/5) [Online]. Available at: https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\AILA\AILA2023052.pdf (Accessed: 10 April 2024).

Kamara, I. and van den Boom, J. (2022) *Computer Security Incident Response Teams in the reformed Network and Information Security Directive: good practices*. Den Haag: National Cybersecurity Centre.

Kolini, F. and Janczewski, L.J. (2022) 'Exploring incentives and challenges for Cybersecurity Intelligence Sharing (CIS) across organizations: a systematic review', *Communications of the Association for Information Systems*, 50(1), pp. 86–121.

Kostadinov, D. (2015) *How harmful can a data breach be?* Infosec Resources [Online]. Available at: https://resources.infosecinstitute.com/topic/the-cost-of-a-data-breach-how-harmful-can-a-data-breach-be/ (Accessed: 4 October 2022).

Liebetrau, T. (2024) 'Problematising EU cybersecurity: exploring how the single market functions as a security practice', *JCMS: Journal of Common Market Studies*, 62(3), pp. 705–724. Available at: https://doi.org/10.1111/jcms.13523.

Lin, W.C. and Saebeler, D. (2019) 'Ris-based v. compliance-based utility cybersecurity – a false dichotomy?, *Energy Law Journal*, 40, pp. 243-282.

Michels, J.D. and Walden, I. (2018) 'How safe is safe enough? Improving cybersecurity in Europe's critical infrastructure under the NIS Directive'. *SSRN* [Online]. Available at: https://papers.ssrn.com/abstract=3297470 (Accessed: 18 April 2024).

Odermatt, J. (2018) 'The European Union as a cybersecurity actor' in *Research Handbook on the EU's Common Foreign and Security Policy*. Edward Elgar Publishing, pp. 354–373.

Pałka, P. (2023) 'Harmed while anonymous: beyond the personal/non-personal distinction in data governance', *Technology and Regulation*, 2023, pp. 22–34.

Papakonstantinou, V. (2022) 'Cybersecurity as praxis and as a state: the EU law path towards acknowledgement of a new right to cybersecurity?', *Computer Law & Security Review*, 44, 105653 [Online]. Available at: https://doi.org/10.1016/j.clsr.2022.105653 (Accessed: 5 February 2025).

Porcedda, M.G. (2018) 'Patching the patchwork: appraising the EU regulatory framework on cyber security breaches', *Computer Law and Security Review*, 34(5), pp. 1077–1098.

'Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union (Text with EEA relevance)' (2018) *Official Journal* L 303, 28 November, pp. 59–68 [Online]. Available at: http://data.europa.eu/eli/reg/2018/1807/oj/eng (Accessed: 24 April 2024).

Schmitz-Berndt, S. (2023) 'Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS 2 Directive', *Journal of Cybersecurity*, 9(1), p.tyad009 [Online]. Available at: https://doi.org/10.1093/cybsec/tyad009 (Accessed: 5 February 2025).

Sievers, T. (2021) 'Proposal for a NIS directive 2.0: companies covered by the extended scope of application and their obligations', *International Cybersecurity Law Review*, 2(2), pp. 223–231.

Taddeo, M. (2013) 'Cyber security and individual rights, striking the right balance', *Philosophy & Technology*, 26, pp. 353–356.

Vandezande, N. (2024) 'Cybersecurity in the EU: how the NIS2-directive stacks up against its predecessor', *Computer Law & Security Review*, 52, p.105890. Available at: https://doi.org/10.1016/j.clsr.2023.105890.

Author Biographies

Dr. Adelaida Afilipoaie

Adelaida is a senior researcher at imec-SMIT, Vrije Universiteit Brussel in the Media Economic & Policy Unit. She conducted her PhD on the regulatory frameworks at the EU and Member States level, and their ability to address online platform power. During her PhD Adelaida contributed to two European studies on media plurality and diversity online and on the implementation of the AVMSD, both for the European Commission. Currently, she is a postdoctoral researcher for the EU Horizon Europe funded Fair MusE (Promoting Fairness of the Music Ecosystem in a Platform-Dominated and Post-Pandemic Europe) and the WEAVE (FWO) ALGEPI (understanding ALGorithmic gatekeepers to promote EPIstemic welfare). In parallel, Adelaida is coordinating the Belgian research team in the Council of Canada funded GMICP (Global Media and Internet Concentration Project) and contributes to various research projects on the topics of discoverability and prominence of European content in the cultural and creative industries.

Valerie Albus

Valerie Albus is a PhD Researcher at the European University Institute in Florence, Italy. Her doctoral research explores how EU regulation shapes the role of online service providers for the purpose of criminal law enforcement. Valerie holds an undergraduate degree in French and European Law from the Université Catholique de Lille and an LLM (cum laude) in European Law from Leiden University. She has professional experience in legal academia (EUI and Max-Planck-Society), legal consultancy, and working for international organisations. Valerie was a trainee in the Legal Service of the European Commission (2019-2020) and in the cabinet of President O'Leary at the European Court of Human Rights (2023-2024). She is the author of several publications in the areas of EU digital regulation, criminal law, and human rights law.

Dr. Lucie Antoine

Lucie Antoine is a post-doctoral researcher at Ludwig Maximilian University in Munich. Her research focuses on traditional intellectual property law

with a focus on copyright law as well as on data- and technology-related questions from a private law perspective, including the protection of personal data.

Lena Auler

Lena Auler is a research assistant at Mainzer Medieninstitut and a doctoral candidate at the Department of Law at Johannes Gutenberg University of Mainz, Germany. She earned her law degree from the University of Mainz with a specialisation in media and communications law. She is especially interested in the law of social media.

Dr. Jascha Bareis

Jascha Bareis is a Political scientist, STS and Media scholar. His passion lies at the crossroads of questions of normativity, political communication and future studies. Currently, he analyzes and comments on the politics of AI, hype, tech oligarchy, and the field of autonomous weapons. He is just about to start his post-doc at the university of Fribourg, joining the HUMAN-IST institute to research the performativity of AI.

Prof. Dr. Catrien Bijleveld

Catrien Bijleveld is a Professor of Research Methods in Criminology at VU Amsterdam, and the director of the Netherlands Institute for the Study of Crime and Law Enforcement (NSCR) since 2014. She is also a member of the Royal Netherlands Academy of Arts and Sciences and was appointed to the Netherlands Scientific Council for Government Policy in 2019.

Professor Bijleveld's work focuses mainly on criminal careers, and she has conducted experimental research into the effectiveness of interventions, juvenile sex offenders, historical trends and the intergenerational transmission of delinquent behaviour.

Jorge Constantino

Jorge Constantino graduated in August 2022 (Cum Laude) with a master's in International Technology Law at Vrije Universiteit Amsterdam (VU Amsterdam) and previously graduated in 2015 with a Bachelor of Laws at Queensland University of Technology (Australia). He is a qualified lawyer with the High Court of Australia and admitted to the Supreme Court of Queensland. He has practiced in the areas of human rights, administrative and constitutional law, as well as migration and criminal law. He is also

a Ph.D. candidate at TU Delft's Faculty of Technology, Policy and Management and a member of the AI Futures Lab at TU Delft.

Dr. Max van Drunen

Max van Drunen is a postdoctoral researcher at the University of Amsterdam, Institute for Information Law. His research focuses on the regulation of technologies used to create and distribute information, such as news recommender systems, generative artificial intelligence, and targeted political advertising.

Rita Gsenger

Rita Gsenger is a research associate in the Research Group "Norm Setting and Decision-Making Processes" at the Weizenbaum Institute for the Networked Society in Berlin. She is a PhD candidate at the Institute of Journalism and Communication Studies at Free University Berlin under Prof. Dr. Christoph Neuberger. Her research focuses on issues of platform regulation, content moderation, evidence-based regulation, and the structural background of disinformation and conspiracy theories, as well as their countermeasures.

Prisca von Hagen

Prisca von Hagen is a research associate at the Weizenbaum Institute in the research group "Norm Setting and Decision Processes". Her research focuses on issues of data protection and data economy law and their interface. For this, she especially examines the development of current data legislation. As a doctoral candidate at Humboldt University Berlin, she deals with information on product characteristics in contracts for digital content and services.

Liza Herrmann

Liza Herrmann, is a PhD student and Junior Research Fellow at the Max Planck Institute for Innovation and Competition, Munich, in the Department of Intellectual Property and Competition Law under the supervision of Prof. Dr. Josef Drexl, LL.M. (Berkeley) and enrolled at the Ludwig-Maximilians-Universität Munich. She studied law at the Humboldt University of Berlin and the University of Geneva, specialising in international law. Her research focuses on competition law, with an emphasis on emerging issues in the digital economy and IT law, in particular bots.

Julia Krämer

Julia Krämer is a PhD candidate in Empirical Legal Studies in the Department of Law and Business at the Erasmus School of Law. She completed her bachelor's degree at the University of Amsterdam and holds an LL.M. from the University of Mannheim. Her research focusses on the quantitative analysis of law and Data Protection Law. Her PhD project explores whether and how mobile platforms are able to implement and foster the goals of privacy regulation, with a special focus on the role of app stores.

Eyup Kun

Eyup Kun is a doctoral researcher in KU Leuven Center for IT and IP Law since February 2021. He conducts his doctoral research on the intersection of cybersecurity and data protection law in the digital economy in addition to his involvement in iFLOWS and ENSURESEC project, which are funded by European Union Horizon 2020 Programme.

Eyup Kun graduated from Istanbul University, Faculty of Law. He is a Turkish qualified lawyer since 2019. He completed his master studies at the London School of Economics and Political Science (the LSE) with the specialisation of information technology, media and communications law in 2020. During his master studies, he was involved in several projects related to the intersection between data protection and other fundamental rights. After graduating from the LSE, he worked as a trainee at the Data Protection Unit at the Council of Europe. During this assignment, he mainly worked on the guidelines on the facial recognition technologies adopted by the Council of Europe in January 2021.

Dr. Lucas Lasota

Dr. Lucas Lasota – MA, PhD, is an Associated Researcher at the Weizenbaum Institute and at the Martin Luther University Halle-Wittenberg, He is also Lecturer at the Humboldt University of Berlin and Legal Programme Manager at the Free Software Foundation Europe. His research focuses on regulatory measures of digital technologies and their impact on individual and collective rights, as well as on internet governance, telecommunications and international contract law.

Lisa Markschies

Lisa Markschies works as a research assistant at Humboldt University of Berlin. In addition, she is currently an associate researcher in the research group "Norm Setting and Decision Processes" at the Weizenbaum Institute.

Due to her legal background, she is particularly interested in how the law is influenced by new technologies, focusing on issues of data and intellectual property law. As part of her dissertation project, Lisa is conducting research on access rights to electronic health data. She participates in the cross-university graduate school "Law of the Information Society" which comprises of a select group of PhD students from all over Germany.

Prof. Dr. Heritiana Ranaivoson

Heritiana Ranaivoson is Research Professor at imec-SMIT-VUB in the Media Economic & Policy Unit. Previously he got a PhD in Economics (Université Paris 1, Panthéon-Sorbonne) and was associate researcher at Mines ParisTech. Having led several research projects funded by public (e.g. European Commission (H2020, Horizon Europe, study contracts), the Unesco) or private (e.g. Google) organizations; he is currently coordinator for the WEAVE (FWO) ALGEPI (understanding ALGorithmic gatekeepers to promote EPIstemic welfare) research project and Work Package leader for both EU Horizon Europe projects Fair MusE (Promoting Fairness of the Music Ecosystem in a Platform-Dominated and Post-Pandemic Europe) and CresCine (Increasing the international competitiveness of the film industry in small European markets). He has published extensively in the fields of cultural and media diversity, media innovation, online platforms, and the role of recommender systems in cultural industries. His latest co-edited book is 'European Audiovisual Policy in Transition' (2023) at Routledge.

Nik Roeingh

Nik is a legal trainee at the Berlin Court of Appeal (Kammergericht) and a research associate at the German Research Institute for Public Administration, where he coordinates the project "Data-Driven Fulfillment of Public Tasks." He studied law in Leipzig, Münster, and Paris and is currently pursuing his doctorate under the supervision of Professor Mario Martini on business-to-government data sharing obligations.

Prof. Dr. Hannah Ruschemeier

Hannah Ruschemeier is Juniorprofessor (tenure W3) for Public Law, Data Protection Law and Law of Digitalisation at the FernUniversität Hagen. She is an associated researcher at CAIS NRW, digtale_kultur, board member of RAILS e.V. and academic advisory board member for user rights. She is particularly interested in collective dimensions of rights, privacy, technical

driven inequalities, data power, new interferences with fundamental rights, surveillance, regulation of technology, legal theory.

Dr. *Pascal Schneiders*

Pascal Schneiders is a postdoctoral researcher at the Johannes Gutenberg University of Mainz, Department of Communication. His research interests include the platformisation of the news ecosystem and its implications from a user and regulatory perspective.

Marie-Therese Sekwenz

Marie-Therese Sekwenz is a PhD candidate at TU Delft's Faculty of Technology, Policy and Management and a Deputy Director of the university's AI Futures Lab. As part of the Lab community, she explores questions at the intersection of rights and compliance with them in the context of digital technologies. Her research focuses on content moderation, platform governance and regulation, artificial intelligence (AI), and the design of socio-technical and legal systems.

In addition to her academic work, Marie-Therese is an active journalist with the Austrian Broadcasting Corporation (ORF), contributing to cultural and documentary radio formats such as Diagonal and Radiokolleg.

Previously, she contributed to research projects at the Leibniz Institute for Media Research | Hans-Bredow-Institut (HBI) and the Vienna University of Economics and Business (WU Wien), where she also completed her studies. She spent a semester abroad at the Graduate School of Management in St. Petersburg and holds an interdisciplinary academic background in law, information systems, and economics.

Lisa Völzmann

Lisa is a DPhil candidate in Socio-Legal Studies at the University of Oxford, conducting legal and empirical research on data access and use rights of EU institutions, bodies and agencies. In addition, she is a Guest Lecturer in European and German Constitutional Law at University College London and a Tutor in Competition Law and Policy at Oxford. Lisa holds a law degree with honors from Humboldt University of Berlin and has previously worked as a Research Assistant at the Weizenbaum Institute and PricewaterhouseCoopers.

David Wagner

David Wagner is an attorney at Spirit Legal Rechtsanwaltsgesellschaft mbH in Frankfurt, Germany, where he advises clients on data protection, technology and competition law, with particular expertise in anonymization and data access. He uses his practical legal experience in his research at the University of the Federal Armed Forces in Munich within the research cluster 'ANIGED', where he investigates the legal implications of various anonymization techniques.

Abbreviations and Acronyms

ADM	Algorithmic Decision-making Systems
AI	Artificial Intelligence
ALTAI	Assessment List for Trustworthy AI
API	Application Programming Interfaces
Art.	Article
Art29WP	Article 29 Working Party
AVMSD	Audiovisual Media Services Directive
B2B	Business-to-business
B2C	Business-to-consumer
B2G	Business-to-government
BBC	British Broadcasting Corporation
BKA	Bundeskriminalamt
BkartA	German Federal Cartel Office (in German: Bundeskartellamt)
BverfG	German Federal Constitutional Court (in German: Bundesverfassungsgericht)
CC	Creative Commons
CCTV	Closed Circuit Television
CCW	Certain Conventional Weapons
CEN	European Committee for Standardization
CENELEC	European Committee for Electrotechnical Standardization
cf.	Confer (Latin) for compare
CFR	Charter of Fundamental Rights
CJEU	Court of Justice of the European Union
CMPF	Centre for Media Pluralism and Media Freedom
CPSs	Core platform services
CR4	Concentration Ration 4
CRA	Cyber Resilience Act
CSIRTS	Computer Security Incident Response Teams
DA	Data Act

DCDSM	Directive on Copyright in the Digital Single Market
DG COMP	Directorates-General for Competition
DG CONNECT	Communications Networks, Content and Technology
DGA	Data Governance Act
DMA	Digital Markets Act
DNS	Domain Name System
DPD	Data Protection Directive
DSA	Digital Service Act
DSC	Digital Services Coordinator
DSP	Digital Service Provider
ECHR	European Convention on Human Rights
ECJ	European Court of Justice
ECSC	European Coal and Steel Community
Ed.	Edition
ed./eds.	editor/editors
EDPB	European Data Protection Board
EGE	European Group on Ethics in Science and New Technologies
EHDS	European Health Data Space
EHR	Electronic Health Record
ELS	Empirical Legal Studies
EMFA	European Media Freedom Act
ERGA	European Regulators Group for Audiovisual Media Services
et seq.	and what follows
ETSI	European Telecommunications Standards Institute
EU	European Union
EC	European Commission
EU-CyCLONe	European Commission and the European cyber crisis liaison organization network
EUI	European University Institute
FCAS	Future Combat Air System
FIDA	Financial Data Access Regulation
FLOPs	Floating Point Operations per Second
FOSS	Free and Open Source Software

FRAND	Fair, Reasonable and Non Discriminatory terms
FSM	Freiwillige Selbstkontrolle Multimedia-Diensteanbieter
G2B	Government-to-Business
GDPR	General Data Protection Regulation
GeschGehG	German Trade Secrets Protection Act (in German: Geschäftsgeheimnisschutzgesetz)
GG	Basic Law for the Federal Republic of Germany (in German: Grundgesetz)
GWB	German Competition Act (in German: Gesetz gegen Wettbewerbsbeschränkungen)
HHI	Herfindahl-Hirschman Index
HLEG	High-Level Expert Group
HVD	High Value Datasets
ICT	Information and communications technology
IoT	Internet of Things
Lit.	Littera (Latin for 'letter')
LLM	Large Language Model
ML	Machine Learning
MPM	Media Plurality Monitor
NCA	National Competition Authority
NetzDG	Netzwerkdurchsetzungsgesetz
NGO	Non-Governmental Organisation
NIS	Network and Information Systems
NLF	New Legislative Framework
NRA	National Regulatory Authority
ODC	Open Data Commons
ODD	Open Data Directive
OECD	Organisation for Economic Co-operation and Development
OESs	Operators of Essential Services
OJEU	Official Journal of the European Union
PAR	Political Advertising
PIMS	Personal Information Management Systems
PSM	Public Service Media
RDAOs	Recognized Data Altruism Organizations

SGB	German Social Codes (in German: Sozialgesetzbuch)
SMEs	Small and medium-sized enterprises
SyRI	System Risico Indicatie
TCO Regulation	Regulation (EU) 2021/784 on addressing the dissemination of terrorist content online
TEHDAS	Towards the European Health Data Space
TEU	Treaty on the European Union
TFEU	Treaty of the Functioning of the European Union
TINA	There-is-no-alternative
TWFD	Television Without Frontiers Directive
U.S	United States of America
VLOP	Very Large Online Platform
VLOSE	Very Large Search Engines
VSP	Video Sharing Platform