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).