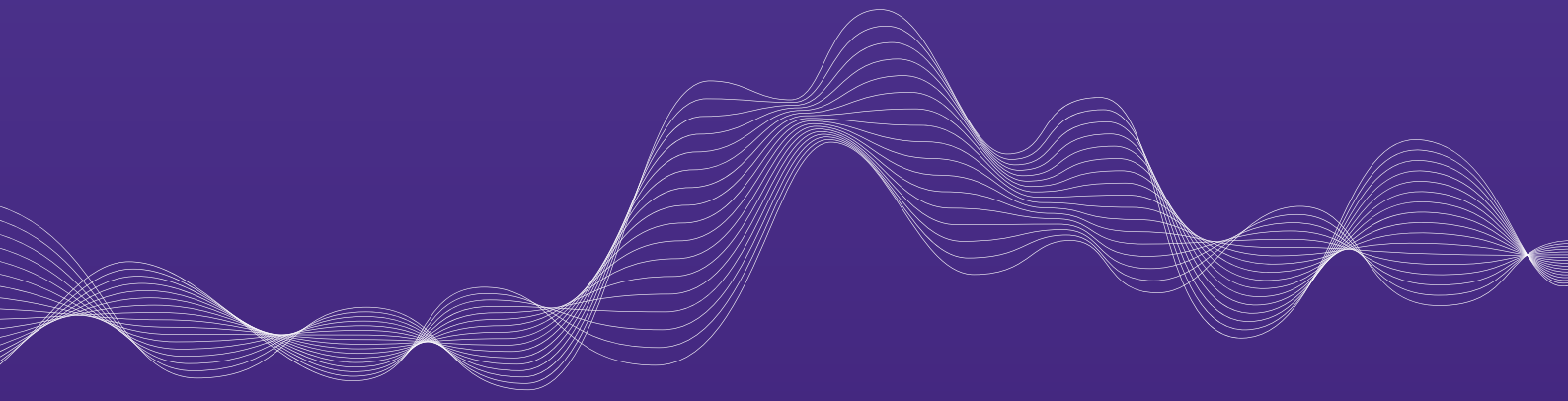
OBSERVATORY ON INFORMATION AND DEMOCRACY

GOVERNING INFORMATION ECOSYSTEMS: LEGISLATION AND REGULATION



An initiative by: FORUM ON INFORMATION AND DEMOCRACY

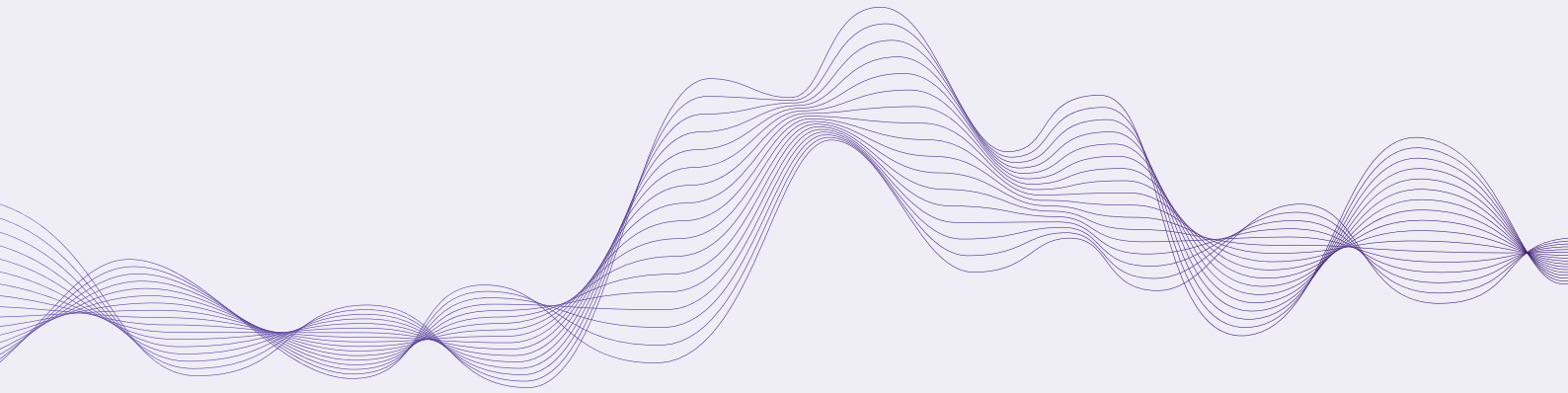
1 Introduction 2

2 Types of Governance Approaches 2

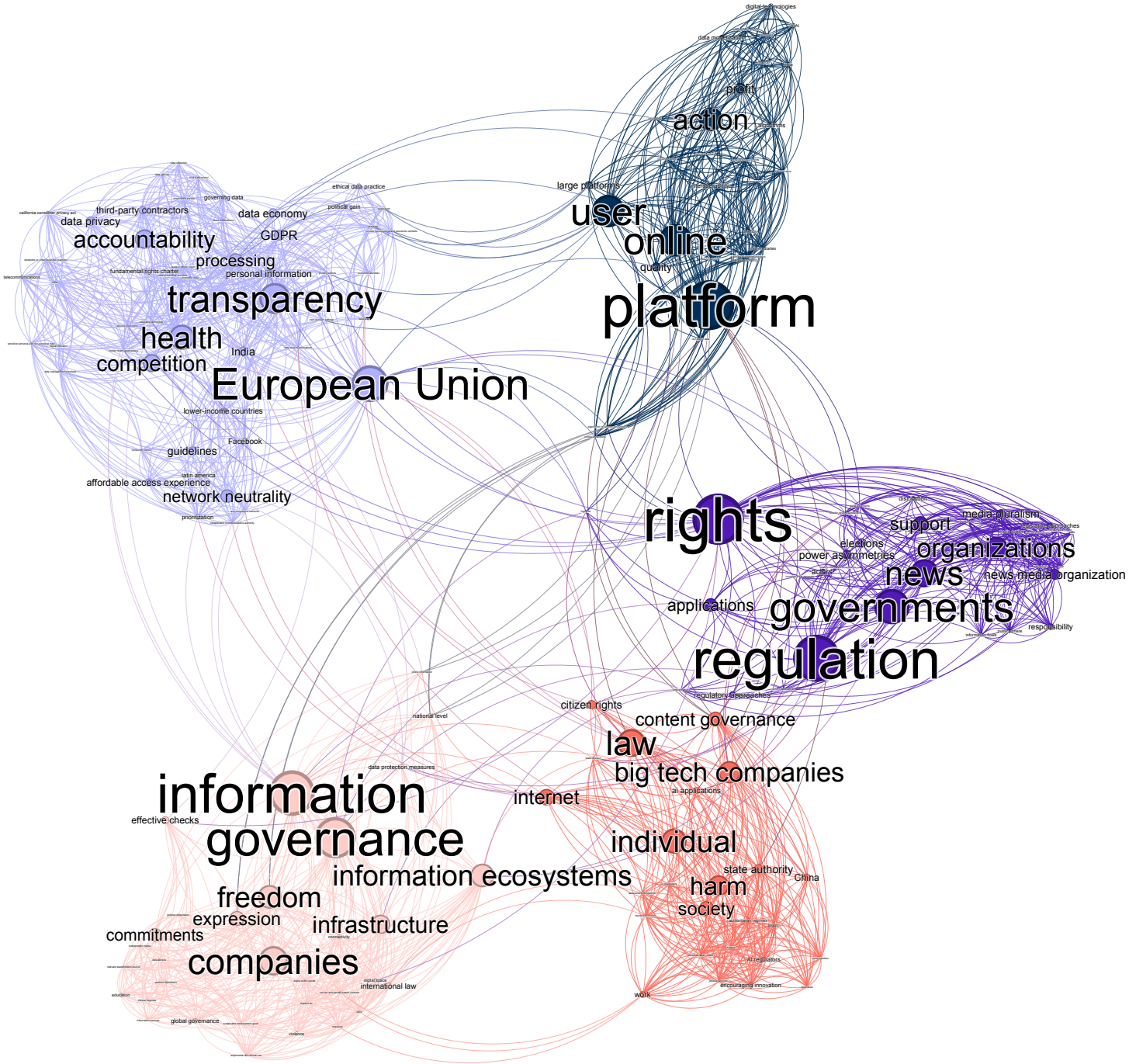
3 Global Governance of Information Ecosystems 4

4 Governance Approaches Applied at Regional and National Levels 6
- **4.1** Governing Network Infrastructure 6
- **4.2** Privacy and Data Protection Governance 8
- **4.3** Governing Digital Platforms 11
- **4.4** Governing AI Systems 15
- **4.5** Governing News Media 17

5 Chapter Summary 20



How to cite this document: Mansell, R., Durach, F., Kettemann, M., Lenoir, T., Procter, R., Tripathi, G., and Tucker, E. (2025) 'Chapter 6: Governing Information Ecosystems: Legislation and Regulation' in Information Ecosystems and Troubled Democracy: A Global Synthesis of the State of Knowledge on New Media, AI and Data Governance. International Observatory on Information and Democracy. Paris.



This map represents a statistical summary of the thematic content of this chapter. The network graph represents relations between the words in the chapter, placing them closer to each other the more they are related. The bigger the node, the more present the word is, signalling its role in defining what the report is about. The colors represent words that are closely related to each other and can be interpreted as a topic.

The map is generated by the OID on the basis of the chapter's text using GarganText – developed by the CNRS Institute of Complex Systems. Starting from a co-occurrence matrix generated from chapter's text, GarganText forms a network where words are connected if they are likely to occur together. Clustering is conducted based on the Louvain community detection method, and the visualization is generated using the Force Atlas 2 algorithm.

Link to the interactive map here

This chapter provides an account of selected legislative and regulatory tools that are available to governments to mitigate the harms of mis- and disinformation and to govern the way mainly big tech companies operate.[1]

The research synthesis focuses on:

- **What types of governance approaches are available?** This briefly discusses voluntary governance that relies on corporate self-regulation and anticipatory co-regulatory and direct state regulatory approaches as well as remedial approaches such as competition/anti-trust measures.
- **What approaches to information ecosystems governance are being promoted at the global level?** This highlights principles that are being established for governing information ecosystems and the emphasis given to human rights protections.
- **What are some of the legislative, regulatory and judicial approaches to governing information ecosystems?** This explains governance approaches applied at regional or national levels. Anticipatory and remedial approaches are discussed: network neutrality policies aiming to open the digital infrastructure; privacy and data protection measures; digital platform regulation; and the regulation of AI systems and news media.

This chapter emphasizes normative goals and rules embodied in selected governance approaches, providing an insight into tensions between these goals and rules and their implementation in view of the interests of different actors.

Chapter 7 examines how governance practices are being deployed to combat mis- and disinformation to strengthen the health of information ecosystems. Chapter 8 critically examines alternative data governance practices aimed at resisting injustices, biases and the harms of big tech-enabled datafication practices.

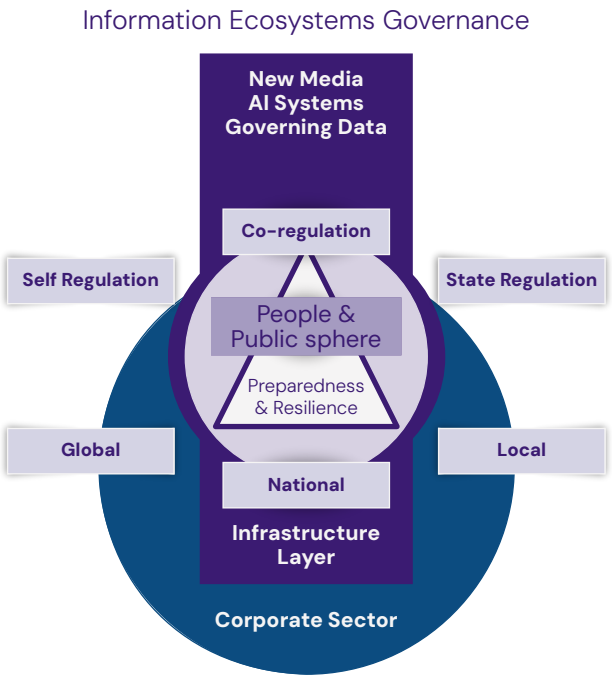
[1] For background reading, see Flew (2021). A comprehensive analysis of research in this area is beyond the scope of this report. See Appendix: Methodology for details of literature review process.

1 Introduction

Governance of information ecosystems is concerned with both the role of governments to cultivate 'systems, institutions, and norms that enable quality and useful information to flourish',[2] and also the corporate actors that supply the digital technologies that are implicated in the spread of mis- and disinformation. 'Governance' is understood here broadly to encompass patterns of rules that underpin social orders.[3]

The focus in this chapter is on interdependent systems and the multiple interactions of information flows, technology and communication infrastructures, norms and practices of public and private institutions. Governance approaches are complicated by the fact that information ecosystems are composed of layers, each with its own conditions and actors, both public and private.[4] These layers – infrastructure and applications – in this report, support news media and AI systems and the way data is governed (see Figure 6.1).

Figure 6.1
Simplified view of the governance of information ecosystems



Source: Authors of this report

Figure 6.1 locates the preparedness and resilience of people and their communities at the center of information ecosystems, indicating that governance arrangements – principles and institutions – are put in place globally, regionally or nationally through state regulations, co-regulatory measures involving states and the private sector, and the self-regulatory initiatives of companies that supply the information ecosystems infrastructure layer and support the applications such as hosting news media content. In this chapter we look principally at the governance of corporate actors (recognizing that in some countries state ownership plays a crucial role, and that local, municipal and community civil society actors are also taking initiatives to govern information ecosystems).

2 Types of Governance Approaches

Voluntary governance measures rely on self-regulation by the tech company owners whose platforms host and circulate content, and by the companies that invest in and operate the underlying infrastructure, including the internet.[5] In this case private actors are expected to commit voluntarily to more stringent standards of practice, consistent with norms and values agreed internationally, regionally and nationally. Power asymmetries due to the monopolistic practices of many of these companies result in clashes between business interests and the public interest. Self-regulation may be intended, for instance, to protect the integrity of elections and the health of democracies, but it is limited due to its voluntary nature and the

[2] Radsch (2023a).
[3] 'Governance' may refer to formal rules initiated by states, corporate self-regulation or co-regulation as well as informal rules and norms put in place individually or collectively. See Puppis *et al.* (2024) on multiple ways in which the term 'governance' is used and criticized in the literature.
[4] The layers of information ecosystems can be depicted in many different ways. See van Dijck (2020), for example, a depiction of the components of digital platforms as a tree structure with roots and branches organized differently in the in the European Union and the United States.
[5] Kokshagina *et al.* (2023), supported by the European Commission.

possible interference with business interests (i.e., to maximize and monetize user online engagement) or by indifference to the public's interest (i.e., in the protection of human rights or the maintenance of healthy information ecosystems).[6]

Most digital platforms employ some form of content governance. They claim that their practices embody fundamental human rights protections, including freedom of expression and privacy protection. Typically, they have no dedicated policy specifically regarding mis- and disinformation, yet it is these big tech companies that decide how mis- and disinformation are addressed.[7] Recent efforts to achieve international consensus on what is expected of corporate self-regulatory governance are discussed in Section 3 of this chapter. Governance approaches applied at regional and national levels to network infrastructure, and for privacy and data protection, digital platform and AI systems governance and news media regulation are discussed in Section 4.

States are primarily responsible for acting to protect human rights and fundamental freedoms, including in the digital environment. They have a *negative obligation* not to violate rights – including the rights of digital companies. They also have a *positive obligation* to protect human rights and implement them in practice. Every intervention is therefore a balancing act that must be assessed in each specific context.[8] While governance in the form of state and co-regulation can address certain illegal acts, most mis- and disinformation cannot simply be banned because much of it is not illegal per se.[9]

When voluntary self-regulation does not address concerns about the way the corporate sector is operating, *anticipatory governance* measures are used. These introduce legislative obligations that must be adhered to by the companies developing and operating components of information ecosystems. They may take the form of *co-regulation* (state and corporate), which is becoming common as concerns about the power of digital platforms and other data intermediaries are growing, and voluntary mis- and disinformation countermeasures are deemed insufficient to mitigate harms.[10] This approach aims to correct the power asymmetry between the owners of digital platforms and other actors in the ecosystem. Typically, co-regulation takes the form of regulations applied to dominant firms to establish norms and rules for their behavior.[11] It is regarded as a potentially balanced option – between the interests of the public and the interests of companies in succeeding in the commercial market. When the states legislate to set up co-regulatory arrangements, this can also involve participation by the private sector and some form of civil society representation in decision-making processes.[12]

Anticipatory governance in this form is seen in some regions as more flexible and inclusive than direct state regulation. This is because co-regulation is said to leave less room for abuse and discretionary measures on the part of the state.[13] *State regulation* involves governments enacting legislation that grants them the authority to decide how information ecosystems should be structured and managed, which can result in rights-infringing measures and partisanship.

In addition, a remedial form of governance led by the state in the form of competition/anti-trust measures is becoming more common. This is premised on the view that competing infrastructure and service providers is consistent with the public interest. The state can also undertake other remedial actions, such as legislating changes in ownership arrangements for data or news organizations.

[6] De Blasio & Selva (2021).
[7] See Chapter 2 for news media and Chapter 3 for AI systems.
[8] Tenove (2020), funded by the Social Sciences and Humanities Research Council (SSHRC) of Canada.
[9] For an introduction to various forms of regulation, see Brown & Marsden (2023).
[10] Self-regulation was still the preferred approach in 2021 in the Czech Republic, which addresses problems of mis- and disinformation through intelligence strategies; see De Blasio & Selva (2021).
[11] Pickard (2020b).
[12] See De Blasio & Selva (2021) on state/industry co-regulatory bodies, technical measures and codes of conduct.
[13] Dittrich (2019); Durach *et al.* (2020).

3 Global Governance of Information Ecosystems

Concerns about an 'information crisis', political polarization, harms to individuals and groups and the destabilization of democracies in the wake of datafication for profit have led to global initiatives to address these concerns. Concluding that declining trust in major institutions globally is partly due to failure to provide reliable information, in 2023 the United Nations proposed a voluntary code of conduct relating to the integrity of information ecosystems (see Table 6.1):

> All stakeholders should refrain from using, supporting or amplifying disinformation and hate speech for any purpose, including to pursue political, military or other strategic goals, incite violence, undermine democratic processes or target civilian populations, vulnerable groups, communities or individuals.[14]

UNESCO's governance initiative takes the form of *Guidelines for the Governance of Digital Platforms*. It establishes voluntary principles and guidelines for duties, responsibilities and roles for stakeholders, with the aim of safeguarding freedom of expression, access to information and other basic human rights (see Table 6.1). It also sets out guidance for policy makers for addressing hate speech through education.[15]

Table 6.1
Governing information ecosystems

Principles for information integrity: United Nations	Principles for governing digital platforms: UNESCO
• Commitment to information integrity • Respect for human rights • Support for independent media • Increased transparency • User empowerment • Strengthened research and data access • Scaled-up responses • Stronger disincentives • Enhanced trust and safetY	• Platform owners to conduct human rights due diligence • Platform owners should adhere to international human rights standards, including in platform design, content moderation and content curation • Platform operations are transparent • Platform companies make available information accessible • Platform owners are accountable to relevant stakeholders

Source: UN (2023a) and UNESCO (2023b)

Other intergovernmental organizations have stepped up efforts to mitigate threats associated with mis- and disinformation. For example, the OECD observed in 2024 that:

> What makes content-specific regulatory responses particularly complex is not only that defining what content may be restricted without infringing upon freedom of expression is difficult, but also that illiberal regimes can co-opt laws to combat disinformation developed in countries with effective checks and balances to legitimise their own antidemocratic practices.[16]

The OECD is working towards a framework that would help to enhance the transparency, accountability and plurality of information sources; foster societal resilience; upgrade governance measures; and encourage institutional arrangements that uphold the integrity of the information space. Bilateral initiatives aim to form coalitions among like-minded countries, for example a United States-led effort aimed at protecting democracies from the disinformation campaigns of foreign governments.[17]

[14] UN (2023a).
[15] UNESCO (2023b). The Guidelines were produced through a multistakeholder consultation, gathering more than 10,000 comments from 134 countries; see also UNESCO (2023a), a multi-stakeholder consultation that received 10,000 comments from 123 countries.
[16] OECD (2024).
[17] Wintour (2024), announced in April 2024, and signed by Canada, the United Kingdom and the United States.

The framing of the impact of digital platforms and their technologies, including AI systems, on information ecosystems in governance contexts depends on 'political decisions about normative issues',[18] reflecting the interconnected nature of digital technologies and societal norms. Developing rules for news media, digital platforms and AI is a key means of exercising normative influence over global regulation, and all these initiatives are framed by international human rights rules, even if the best means of institutionalizing these rules is contested.[19] At the global level, these contests among stakeholders – public and private, individual and collective – played out in deliberations that led in 2024 to the United Nations' *Pact for the Future*, setting out 'guiding principles', which, among others, embrace 'full respect for international law', 'the pursuit and enjoyment of human rights and fundamental freedoms for all' and 'the responsible and ethical use of science, technology of innovation, guided by the principles of equity and solidarity'.[20] Annex I is a *Global Digital Compact* that sets out five objectives:

1. Close all digital divides and accelerate progress across the Sustainable Development Goals;
2. Expand inclusion in and benefits from the digital economy for all;
3. Foster an inclusive, open, safe and secure digital space that respects, protects and promote human rights;
4. Advance responsible, equitable and interoperable data governance approaches;
5. Enhance international governance of artificial intelligence for the benefit of humanity.[21]

The actions include addressing connectivity and digital divides, addressing digital literacy, skills and capacities, promoting digital public goods and digital public infrastructure, expanding inclusion in the digital economy and promoting the 'free flow of information and ideas', calling on digital technology companies to respect international human rights and principles.[22]

Regarding digital trust and safety, the Compact states that:

> We must urgently counter and address all forms of violence, including sexual and gender-based violence, which occurs through or is amplified by the use of technology, all forms of hate speech and discrimination, misinformation and disinformation, cyberbullying and child sexual exploitation and abuse. We will establish and maintain robust risk mitigation and redress measures that also protect privacy and freedom of expression.[23]

The Compact explicitly refers to information integrity:

> We will work together to promote information integrity, tolerance and respect in the digital space, as well as to protect the integrity of democratic processes. We will strengthen international cooperation to address the challenge of misinformation and disinformation and hate speech online and mitigate the risks of information manipulation in a manner consistent with international law.[24]

In this context, specific commitments to be achieved by 2030 include: 'digital media and information literacy curricula', promoting 'diverse and resilient information ecosystems', including the strengthening of independent and public media as well as supporting journalists and media workers, and providing, promoting and facilitating 'access to and dissemination of independent, fact-based, timely, targeted, clear, accessible, multilingual and science-based information', along with other commitments.[25] Other issues addressed under other objectives include data privacy and security, standards, data flows and AI.

[18] Erman & Furendal (2022, p. 267), supported by the Marianne and Marcus Wallenberg Foundation and Swedish Research Council (Vetenskapsrådet).
[19] Roberts *et al.* (2024).
[20] UN (2024b, pp. 57-58). For the full list of guiding principles and commitments, see pp. 58-60.
[21] UN (2024b, pp. 40-41).
[22] UN (2024b, pp. 41-56).
[23] UN (2024b, p. 48).
[24] UN (2024b, p. 49).
[25] UN (2024b, p. 49).

These statements of commitments necessarily are voluntary and have less traction than the governance rules that are introduced at national level by states or by regions and through the self-regulatory initiatives of globally operating companies.

4 Governance Approaches Applied at Regional and National Levels

This section explains governance approaches that are developed and applied at regional or national levels, although they are informed by commitments to voluntary principles that are agreed at the global level. We start with a selection of both anticipatory and remedial approaches to governance in areas that are expected to impact on the health of information ecosystems, beginning with network neutrality measures designed to secure an open internet (Section 4.1). We then review privacy and data protection measures (Section 4.2), digital platform regulation (Section 4.3), AI systems regulation (Section 4.4) and finally, approaches to news media regulation (Section 4.5).

4.1 GOVERNING NETWORK INFRASTRUCTURE

Internet connectivity and access are central to how people experience information ecosystems. While we cannot address all the features of governance in this area, network neutrality policies and regulations concerning what is known as 'zero rating' are central to how those who do have connections and affordable access experience information ecosystems. This form of anticipatory governance typically involves legislation and co-regulation, but it can also involve the state acting authoritatively under legislation that permits it to set rules for internet access and use. Whether network neutrality rules are adhered to conditions whether and how people can generate and amplify the circulation of all kinds of information, including mis- and disinformation, and what information they encounter online.

Network neutrality is the principle that internet service providers (ISPs) should treat all data (information) that flows through their networks without discrimination. This open internet principle is controversial because it impacts on the equality of access to data and online information.[26] The principle emerged in the Global North, and it intersects with zero-rating practices that are now common in many countries in the Global Majority World — ISPs offer access to certain services, and data usage does not count against a cap on the data used to access those services. This means that owing to a desire to minimize costs, users may restrict their access to information to a limited number of platforms.

Approaches to network neutrality and zero rating in India. Network neutrality and zero rating became critical policy issues in *India*, attracting intense scrutiny from online content firms and ISPs. The Telecom Regulatory Authority of *India* (TRAI) consulted on network neutrality in 2016 and 2017, after a #SaveTheInternet campaign by activists against Facebook's Internet.org. Facebook aimed to provide low-cost and subsidized access to a few selected services to lower-income countries in Asia and Africa. This zero-rating service raised concerns about fairness and competition, because it would give preferential treatment to certain services over others.

Network neutrality debates focused on traffic management practices, that is, the prioritization of certain types of internet traffic over others, potentially disadvantaging

[26] For a discussion, see Baranes (2014); Bauer & Knieps (2018); Economides & Hermalin (2012); Hildebrandt & Wiewiorra (2024); Jordan (2017); Marsden (2016); Marsden & Brown (2023); Menon (2021); Pickard & Berman (2019); Winseck & Pooley (2017); Wu (2003); Yoo (2024). For a literature review, see Lee & Shin (2016).

some users or competing services. The conflict is between those calling for an open internet, where all data is treated equally, and the ISPs that claim they need to manage network traffic under conditions of congestion and to block illegal content. TRAI banned discriminatory tariffs in 2016, effectively prohibiting zero-rating service offerings like Facebook's Free Basics.[27]

In *India*'s diverse socio-economic context, where internet access is a critical developmental tool, its policy of ensuring equal access by banning a two-tiered internet illustrates how a balance may need to be struck between equity and innovation in service provision. The Cellular Operators Association of India (COAI) suggests that the policy is limiting the introduction of lower-cost access that might help to bridge the digital divide.[28]

Network neutrality and zero-rating issues are widely discussed in *South Africa*, *South Korea* and *Latin America* in relation to the public value of the internet, and where digital activism aims to resist Facebook's Free Basics service.[29] In jurisdictions allowing zero rating, regulatory bodies, such as the Independent Communications Authority of South Africa (ICASA), provide guidelines to try to align these practices with public interest goals, for example to enhance educational and public health access to information or to prevent anti-competitive behavior.

In the *United States*, net neutrality policy is in regulatory flux. The Federal Communications Commission established strong net neutrality rules in 2015 so that ISPs could not discriminate between preferred online service providers. A Pew Research Center survey found that when network neutrality rules were in place, a majority of Americans reported that they either understood or supported the policy even though its enforcement was inconsistent and impacted on the quality of service they experienced online.[30] Network neutrality was repealed in the United States in 2017, reinstated in 2024 and then blocked by the federal court. There is some evidence that without net neutrality rules, there has been an increase in ISP data throttling and prioritization, which can be argued to disadvantage smaller content providers and reduce consumer choice.

The *European Union*'s Open Internet Access Regulation provides rules on net neutrality across member states, with the Body of European Regulators for Electronic Communications (BEREC) setting guidelines requiring that ISPs do not favor specific service providers. These indicate that zero-rating practices must not undermine net neutrality.[31] Here, too, the policy is controversial; although there is a high compliance rate, critics argue that the policy allows for subtle traffic prioritization that is discriminatory.

Techniques for closing off internet access, whether via zero rating, throttling traffic or other means of fragmenting the internet, are also used widely.[32] Strong measures include internet shutdowns and social media blocking during elections, with political unrest and protests occurring in countries as diverse as *Belarus*, *Iran*, *Myanmar*, *Turkey*, *Vietnam* and *Zimbabwe*.[33] Interference by authoritarian regimes includes restrictions on access to information, such as *China*'s Great Firewall, heavily regulated 'national internets' and using intrusive content governance measures to favor or censor political speech or for surveillance,[34] such as, for example, *Iran*'s initiative to create a 'national information network', requiring websites and services to locate servers inside the country and increasing the cost of global internet traffic.[35]

[27] Eisenach (2015); Mukerjee (2016); Prasad (2018). For a more extensive treatment of zero rating, to give a sense of its scope and the debate around whether it addresses exclusion problems or unjustly reduces access to information, see Gerpott (2018); Hoskins (2024); Jaunaux & Lebourges (2019); Krämer & Peitz (2018); Mattelart (2023).
[28] Menon (2021).
[29] Nothias (2020); Robb & Hawthorne (2019); Shahin (2019); Shin & Lee (2017).
[30] Greenstein *et al.* (2016); Program for Public Consultation (2022); Vogels & Anderson (2019).
[31] BEREC (2024a, b).
[32] Boas (2006); Howard & Hussain (2013); Kalathil & Boas (2003); Shahbaz *et al.* (2022).
[33] Akser & Baybars (2023); Mare (2020); Sinpeng (2020); Ryng *et al.* (2022), supported in part by the Office of the United Nations High Commissioner for Human Rights (OHCHR).
[34] Keremoğlu & Weidmann (2020), funded by the German National Science Foundation (DFG, Deutsche Forschungsgemeinschaft).
[35] Motamedi (2024).

Debates in this area concerning the infrastructure layer highlight the need for adaptable and context-sensitive regulation so that the benefits of digital inclusion and access to diverse sources of information are balanced against risks of market distortions. One strategy is to require ISPs to disclose their data management practices and zero-rating agreements publicly, and to include civil society and industry in policy making. Decisions are increasingly influenced by efforts to achieve internet or digital sovereignty, which is understood differently depending on a country's political and economic context.[36]

4.2 PRIVACY AND DATA PROTECTION GOVERNANCE

The collection and processing of sensitive personal and non-personal data on an industrial scale in the data economy by big tech companies means that governance rules are being updated to mitigate risks of privacy infringements and harms resulting from identity exposure. Specific rules apply for different types of data depending on their sensitivity and the risks associated with their misuse, with the aim of increasing transparency and accountability for data use.[37] In this area we find a mix of anticipatory and remedial governance measures.

In the United States the capacity of digital platforms to collect, process and make data generated online available to third parties without user consent is subject to privacy protection legislation at the federal level, with the Children's Online Privacy Protection Act (COPPA) of 1998 updated in 2013 to govern the collection of information about minors, addressing issues of parental consent, confidentiality and security, with safe harbor provisions and rules for data retention and deletion.[38] There is no single federal law to govern data privacy, but federal laws apply to data and telecommunications, health information, credit, financial and marketing information. There are multiple state-level laws, including the California Consumer Privacy Act (CCPA). The Federal Trade Commission (FTC) functions as a regulator to constrain unfair or 'deceptive or unfair business practices and from unfair methods of competition', and takes action to enforce privacy laws.[39]

- In the *United States*, the CCPA is seen as the most stringent privacy law. It requires businesses to disclose the categories and specific pieces of personal information they collect at or before the point of collection. It asserts the consumer's right to know about the personal information that is collected and when it is sold or shared with third parties. This model broadened the concept of data 'sale', potentially encompassing many types of data transactions not typically considered sales, and requiring businesses to reevaluate their data practices.[40]

- In the *United States*, the Health Insurance Portability and Accountability Act (HIPAA) was introduced in 1996 with data privacy and security provisions for safeguarding medical information. The HIPAA, while comprehensive, does not fully address the complexities of new technologies and the digitization of health records. Mobile health applications and wearable technology are generating vast amounts of health-related data that can fall outside the scope of this legislation. This underscores the need for continuous enhancement of legal frameworks to keep pace with technological advances and societal changes. Data protection becomes even more complex when sensitive topics, such as access to abortion data, become an issue, and the handling of, for example, abortion data, comes under intense scrutiny. The reversal of *Roe v. Wade* has heightened concerns about the privacy and security of reproductive health data. The protection of such sensitive data is crucial in preventing data misuse and discrimination, and in ensuring that individuals' privacy rights are upheld.[41]

[36] Afina *et al.* (2024); Kokas (2022); Kumar & Thussu (2023); Stefanija & Pierson (2023).
[37] Kerber (2020).
[38] US Congress (2013).
[39] See FTC website https://www.ftc.gov/about-ftc and see Kira *et al.* (2021) for an overview, supported by the Global Challenges Research Fund (GCRF), UK and the Omidyar Network.
[40] US State of California (2018).
[41] Dellinger & Pell (2024); Roth (2022); US Congress (1996a).

- The *European Union*'s General Data Protection Regulation (GDPR) references fundamental rights enshrined in Articles 7 and 8 of its Fundamental Rights Charter, and is among the most comprehensive regulation worldwide.[42] Implemented in May 2018, it sets out requirements for companies and organizations that collect, store and manage personal data. It applies uniformly across all sectors, but has specific provisions for some types of data-processing activities. For example, Article 9 imposes stricter conditions on the processing of special categories of personal data such as health information, biometric data and data revealing racial or ethnic origin.

A shift in tech company behavior was recorded when data collectors were required to disclose their data handling practices and undergo regular audits to ensure compliance with legal standards.[43]

Compliance with the GDPR. Google has faced significant challenges in complying with the GDPR. The stringent demands for increased transparency and data handling accountability compelled the company to overhaul its privacy policies and practices. It revised its privacy policies to make them more understandable and accessible to users, simplifying the language and providing clearer explanations of what data is collected and how it is used. The policies now include detailed descriptions of privacy controls that users can access to manage their personal information, aiming to ensure users have a better understanding and greater control over their data. Google introduced more granular privacy controls in user account settings, allowing users to more easily review and modify privacy options. A proactive 'Privacy Checkup' tool was rolled out that guides users through their privacy settings, aiming to help them make better informed decisions about their data.[44]

Questions remain about whether the regulation goes far enough to ensure data privacy, and tech companies are frequently charged with data breaches and with unauthorized tracking of users online. For example, a case has been brought under European Union competition policy anti-trust rules law against Alphabet Inc. for Google's alleged tracking of users. In June 2024, action by the European Center for Digital Rights (NYOB), a privacy advocacy group, resulted in Google being scrutinized under European Union anti-trust law for unauthorized user tracking by its Chrome web browser.[45] Privacy controls on platforms such as Facebook have also been criticized for their use of so-called 'dark patterns' – 'tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something' all create opportunities for unauthorized data collection that are opaque to the user.[46] Alleged infringements of privacy can take a long time to resolve. For example, the *Irish* Data Protection Commission's 2019 investigation into whether Google uses sensitive personal data about race, health or political preferences to target ads stalled. The Irish Council for Civil Liberties then asked the Irish High Court to force an investigation, but this request was denied, although the Data Protection Commission did start an investigation in early 2024.[47]

The complexity of data collection practices and the volume of data pose significant challenges for achieving true transparency, and data protection authorities are struggling to keep pace with multiple cases before the courts. The power asymmetry between large tech companies and their users can leave the latter unaware of the full extent

[42] EC (2016b).
[43] Linden *et al.* (2020), supported in part by the National Science Foundation (NSF), US.
[44] See Houser & Voss (2018); Murtaza & Salman (2019); Waldman (2020).
[45] See Halpern *et al.* (2024).
[46] See Brignull (2023, p. np).
[47] See Murgia (2019); O'Faolain (2024).

and implications of data collection and data monetization; targeted advertising and the misuse of data for political gain mean that the GDPR is not a panacea for all data economy issues. Vigilance and a commitment to ethical data practice are essential to protect user privacy and maintain public trust.

While the GDPR has served as a template in several jurisdictions,[48] others have varied approaches, reflecting their unique socio-political and economic contexts:

- In *African countries* measures are being taken to introduce privacy protection and data protection legislation. A data protection law was put in place in *Cape Verde* in 2001. As of the end of 2023, 35 countries had enacted legislation, with three others pending, although a review indicates that in some cases countries introduce exemptions for national security reasons. While the GDPR in Europe also provides exemptions, the issue in African countries is the robustness of the institutional protection of human rights.[49]

- *Brazil*'s General Personal Data Protection Law (LGPD, Lei Geral de Proteção de Dados) mirrors the GDPR's comprehensive scope while incorporating elements tailored to the country's environment. The LGPD emphasizes principles of transparency, purpose limitation and data minimization, aiming to balance the protection of personal data with the facilitation of economic activities.[50]

- *China*'s approach to data protection, exemplified by the Cybersecurity Law and Personal Information Protection Law (PIPL), is tied to its broader strategy to balance the imperatives of economic growth and national security, reflecting its socio-political and economic landscape.[51] It is argued in the critical literature that the main emphasis of the country's data laws is on treating data as a 'new factor of production', which does not acknowledge people's epistemic rights, that is, their right to know.[52]

- In *India*, a Draft Personal Data Protection Act (DPDPA) 2023 was proposed in 2018 after a landmark Supreme Court judgment – *Puttaswamy vs. Union of India* in 2017 – and passed in 2023. The DPDPA mirrors aspects of the GDPR, and is aimed at 'the processing of digital personal data in a manner that recognises both the right of individuals to protect their personal data and the need to process such personal data for lawful purposes'. In some sectors, such as financial technology (fintech), sectoral regulations apply. For example, the Reserve Bank of India plays an important role in regulating the financial services industry, establishing and enforcing self-regulatory guidelines, and penalizing and suspending bank licenses that do not comply with its data protection guidelines and 'know your customer' norms.[53]

- *Japan* has updated its Act on the Protection of Personal Information (APPI) several times after its introduction in 2003, and achieved GDPR compliance a year before the European Union's legislation came into force. Further amendments have expanded the scope of individual rights, provided for stricter consent requirements, made data breach notifications mandatory, and limited the types of data that can be provided to third parties.[54]

These rules illustrate that approaches to governing data to secure privacy protection differ considerably because they are tailored to the concerns and inequalities in specific political and economic contexts. It is therefore important to differentiate between approaches in the

[48] Bryant (2021).
[49] Andere & Kathure (2024); Ndemo & Thegeya (2023); South Africa Government (2024).
[50] Government of Brazil (2018).
[51] He (2023); US-China Commission (2022); Voss & Pernot-Leplay (2024).
[52] Chin (2024)
[53] Government of India (2023, p. 1); *Justice K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors* (2017); for an overview of trends in data governance, see also Punia *et al.* (2022).
[54] Abdulrauf & Dube (2024); Coos (2022) provides a comprehensive overview of data privacy laws in Africa.

higher-income countries and the middle- and lower-income countries.[55] Data protection and privacy legislation can share common themes, such as provisions for consent and attention to data subject rights, although this legislation differs in scope and specific provisions, such as data localization.

For instance, in the *European Union*, the GDPR mandates strict consent requirements and robust data subject rights, influencing global data protection standards with its comprehensive and extraterritorial reach. In contrast, in the *United States*, the CCPA, while also emphasizing consumer rights and transparency, introduces a unique private right of action and provisions tailored to California's legislative context. *India*'s DPDPA incorporates stringent data localization requirements, reflecting an emphasis on digital sovereignty, local data control and geopolitical considerations. Each of these legislative approaches plays a role in shaping the practices of data privacy and individual rights protection and the standards that are adhered to.[56]

Defining responsible parties. Under the GDPR, responsible parties are clearly defined as either 'data controllers' or 'data processors'. A data controller determines the purposes and means of processing personal data, while a data processor is responsible for processing data on behalf of the controller. This distinction is crucial for accountability as it clarifies who is responsible for ensuring compliance with the GDPR, and who will be liable if something goes wrong. In India, the DPDPA introduces the concept of data fiduciary and data processor, where data fiduciaries are akin to data controllers under the GDPR and are tasked with exercising due diligence in the processing and securing of personal data.

Governing data is a delicate endeavor for policy makers. It involves a struggle to manage the balance between the need for data security and privacy and the benefits of data utilization (for sector applications, e.g., health, finance, environment monitoring or for monetization purposes). By implementing specialized governance measures, enhancing transparency and promoting public awareness, the aim is to safeguard sensitive personal data against misuse. The diverse parties involved in data collection – from tech giants and startups to governments and third-party contractors – presents unique challenges in achieving effective governance that can assure accountability, fairness and transparency in how data is collected and used.[57]

4.3 GOVERNING DIGITAL PLATFORMS

Both anticipatory and remedial forms of governance are being applied in many countries to moderate the behavior of the big tech companies, with measures being put in place to establish rules for digital platform operation when it is found to be inconsistent with human rights standards and/or to be anti-competitive. This section highlights how these measures impact on the problem of mis- and disinformation, but does not address the full complement of governance measures being introduced in regions around the world.

The *European Union* introduced measures dedicated to countering mis- and disinformation with an Action Plan in 2018. This was centered around improving capabilities to detect, analyze and expose mis- and disinformation. The aim was to strengthen coordinated responses, mobilize the private sector, raise awareness and increase societal resilience. A Code of Practice on Online Disinformation was put in place (and strengthened in 2022). The Code commits industry to address mis- and disinformation, political advertising and the integrity of services, and aims to empower consumers and the research community.[58] It operates under the

[55] Sampath (2021).
[56] Park (2020).
[57] Dolata *et al.* (2022).
[58] EC (2018, 2022e); early signatories were Facebook, Google, Twitter and Mozilla, and parts of the advertising industry, followed by Microsoft and TikTok; see also Saurwein & Spencer-Smith (2020). For criticisms of the Code, see Culloty (2021); Monti (2020); Nenadić *et al.* (2023); Pamment (2020).

supervision of the European Commission, and has inspired other countries to take similar action.[59] A permanent monitoring mechanism – the European Digital Media Observatory – was established as a hub for fact-checkers and for those studying mis- and disinformation issues.[60]

A wider European Union regulatory framework has been put in place to strengthen digital governance, including the Digital Services Act (DSA) and the Digital Markets Act (DMA).[61] These rules share a foundation in human rights aiming to safeguard citizen rights, and this legislative package is shaping content governance approaches at the national level.[62]

Horizontal human rights. The DSA sets limits to the terms and conditions of platforms to govern the interactions between users and platforms — including the degree to which algorithmic recommender systems are used. Article 14 mandates that platforms must consider user interests in content moderation and complaint handling, referencing fundamental rights, such as freedom of expression. Very large online platforms (VLOPs) are required to respect fundamental rights due to the 'systemic risks' they present, based on comprehensive risk analyses and mitigation strategies. Article 34(1) obligates platforms to consider users' fundamental rights among other factors when evaluating risks.[63]

The DSA is 'a horizontal framework for regulatory oversight, accountability and transparency of platforms and search engines'.[64] Many of its measures apply to digital platforms and intermediaries with more than 45 million users per month in the European Union.[65] The Act's provisions govern the algorithms used in automated content moderation, with binding obligations to remove illegal content, safeguards to respect freedom of expression and substantial penalties for failure to comply. VLOPs and search engines must adhere to a benchmark for processing valid notifications for removal of illegal hate speech in less than 24 hours. If a platform considers that content is not compliant with its terms and conditions, it may proceed with deletion or restriction. The aim is to create a safer digital space within which the fundamental rights of all users of digital services are protected.[66] These legislative measures combine 'internal market, fundamental rights and geopolitical motivations, primarily in relation to emerging technologies'.[67]

The DMA addresses the monopolistic behavior of the largest digital platforms with the aim of establishing a 'level playing field', that is, a contestable market, by constraining the practices of companies with gatekeeping power and that offer 'core' platform services. The overall goal is to promote 'innovation, high quality of digital products and services, fair and competitive prices, as well as high quality and choice for end users in the digital sector'[68] by addressing imbalances in bargaining power and unfair (monopolistic) practices so that greater choice is available to platform users. There are sanctions against platform self-preferencing, the largest gatekeepers must enable the interoperability of services, and there are other measures aimed at achieving a balance between business and individual (or collective) interests.

[59] DiGi (2022); Wilding (2021).
[60] European Digital Media Observatory: https://edmo.eu.
[61] EC (2022a, c). For the Data Governance Act, see EC (2022d) and for the Data Act, see EC (2023); see also Akman (2022); Botta (2021); Broughton Micova & Jacques (2020); Galantino (2023); Just (2022); Mansell (2021); Moreno Belloso & Petit (2023); Nenadić *et al.* (2023).
[62] Church & Pehlivan (2023), authors affiliated with Linklaters, a law firm, with offices in London and Madrid. The large tech companies are also subject to national law with binding measures, such as the German Network Enforcement Act 2017, the French Organic Law No. 2018-1201, and Hungarian legislation; see German Law Archive (2017); Government of France (2018); Stolton & Makszimov (2020).
[63] Defined as platforms with more than 45 million users per month.
[64] Nenadić *et al.* (2023, p. 8).
[65] Turillazzi *et al.* (2023).
[66] EC (2022c); Reyna (2024).
[67] Broeders *et al.* (2023, p. 1272), funded by the Dutch Ministry of Foreign Affairs (BZ, Ministerie van Buitenlandse Zaken); see also Mansell (2021).
[68] EC (2022a, para. 106). See also Brown & Marsden (2023); Crémer *et al.* (2019).

Competition/anti-trust legislation provides tools that are applied ex post to mitigate harms. Remedial remedies can include corporate divestment, fines and behavioral requirements. Competition law is seen as a means of leveling the market and diffusing gatekeeper power, although the gatekeeping power of big tech companies is generally treated as a 'natural' outcome of technological innovation.

Competition law applies in the European Union, and cases have been brought against Google's search and advertising practices, Google's and Apple's app store rules for participation, Meta's data collection and processing practices, and Amazon, for its treatment of companies that use its online marketplace.[69] The Treaty on the Functioning of the European Union (TFEU) applies to the conduct of 'gatekeepers'. The scope tends to be limited to cases where the dominance of specific markets can be evidenced through lengthy investigation, although the criteria for establishing market dominance are slowly being modified.[70] For example, in Germany, non-price issues, such as access to data, have been treated as a potential criterion for determining market power, and member states are introducing modifications to enable them to bring actions against digital platforms more easily.[71]

The digital platforms have faced few efforts in the *United States* to curtail their market power until recently, allowing them to refine their business models to maximize user engagement and monetize data for profit. This has enabled them to acquire or suppress competitors, favor their own products and services, and downplay or disavow responsibility for harms linked to data collection, processing and monetization operations. The companies insist that they are providing their customers with convenient ways to access digital content and to buy goods online consistent with their individual preferences. However, more aggressive application of anti-trust law was encouraged under the Biden Administration, with cases being brought against the platforms by the Department of Justice and the FTC as they pursue more vigorous efforts to limit platform monopolistic behavior.[72] Proposals for sector-specific legislation, with some echoes of European Union approaches, are considered from time to time at the federal level to tackle big tech power. These have not been signed into law, but they call for prohibitions on large platforms giving preference to their own products, encourage interoperability and restrict platform use of non-public data, with penalties and injunctions.

In the United States there is much debate about the spread of viral mis- and disinformation and the consequences of content governance practices.[73] The First Amendment speech rights protections have led to controversy around the need for content governance.[74] Legislative proposals aimed at curtailing the circulation of content deemed to be harmful typically fail to attract sufficient congressional support. Digital platforms benefit from Section 230 of the Telecommunications Act of 1996.[75] Providers or users of interactive computer services are not treated as 'publishers' or 'speakers' of any information provided by another content provider. They therefore have broad immunity from liability for the content they host. Debates about how platform immunity might be circumscribed are highly politicized. Proposals to combat 'fake' information are met with 'free market' arguments and the claims that competition will eliminate problems.

This report does not cover all the cases seeking to curtail the big tech companies' power. However, it is important to note that when there are successful cases confirming their monopoly power, this could have a substantial long-term impact. One example is a court ruling in August 2024 that Google was a monopolist in the general search text ad market. However, it was not found to be a monopolist in the search ads market, that is, based on the signals

[69] Nicoli & Iosifidis (2023).
[70] EC (2012, Articles 101, 102).
[71] Just (2018, 2022).
[72] FTC (2024); see also Stigler Committee (2019); Wu (2018).
[73] Flew (2021).
[74] Forum on Information and Democracy (2024d).
[75] US Congress (1996b).

provided by users' online interactions and the company's algorithms.[76] At the time of writing the judgment was under appeal. If it stands, it could open the door to further action, from breaking up monopolies to forcing companies such as Meta, Apple and Amazon to change their behavior, for example to modify their algorithms or make them provide support to the news media industry.[77]

None of these judgments changes the overarching commitment to rapid innovation in digital technologies, including the use of opaque algorithms and generative AI (GenAI) for profit, which, in the *United States* at least, remains a powerful mobilizer of investment in future generations of data monetization strategies.[78] An argument gaining some ground is that the scale of digital platform adoption has reached a point where they have become essential public services and should be subject to the same regulations as public utilities (as privately, publicly, cooperatively or municipally owned) that operate as 'natural monopolies'. However, whether digital platforms such as Meta meet the threshold for being classified as an 'essential service' is disputed, and some argue that treating them in this way could entrench their monopolistic position.

Much of the literature on big tech governance focuses on the *United States* and *Europe* (and increasingly on *China*). Other countries also have legislation. We mention only a small sample of instances here, where measures are being taken to combat mis- and disinformation.[79]

Country measures to legislate to limit mis- and disinformation. Between 2011 and 2022, 78 countries had passed sector-specific laws designed to limit the spread of online mis- and disinformation. Some focus on improving transparency and accountability and increasing media and information literacy. Others focus on criminalizing the creation and distribution of content, which, in authoritarian states, paves the way for subjective evaluations of what constitutes 'fake news', leading to the abuse and undermining of freedom of expression, including press freedom.[80] National legislation aimed at combating mis- and disinformation includes the *Malaysian* Anti Fake-News Act 2018, the *Singapore* Protection from Online Falsehoods and Manipulation Act 2019, the *Russian* fake news law, the *Bangladesh* Digital Security Bill Act, and several laws in *China*.[81]

These laws tend to position digital platform owners or states as arbiters of 'truth', which can lead to abuses of basic freedoms.[82] Legal initiatives also face lobbying by the big tech firms. For example, in *Brazil*, work on a law on AI initially proposed in 2019 had not been adopted at the time writing in late 2024 due to successful lobbying by big tech companies. The draft calls explicitly for the 'development, implementation and use of Artificial intelligence in *Brazil* … based on integrity of information through the protection and promotion of reliability, accuracy and consistency of information'.[83] In authoritarian regimes, when digital platforms provide spaces for political activism – including by opposition parties – this is problematic from a rights-based perspective, and is illustrated by the experience of *Southeast Asian* states, where state authority is maintained through a combination of political pressure and internet controls.[84]

[76] This general search ad market excludes display ads, retargeted display ads and non-search social media ads, that is, ads that rely on 'indirect signals to decipher a users' latent intent' based on a user's past online interactions (US District Court, 2024, p. 168).
[77] Radsch (2024).
[78] This is addressed in Chapter 8.
[79] Pickard (2022a).
[80] Lim & Bradshaw (2023).
[81] Dittrich (2019); Malaysia Government (2018); Repnikova (2018); Reuters (2019); Richter (2019); Singapore Statutes (2019).
[82] Dittrich (2019).
[83] Government of Brazil (2023); our translation.
[84] Sinpeng (2020).

4.4 GOVERNING AI SYSTEMS

Regulators and policy makers face substantial challenges in defining rules for content governance enabled by AI systems in the light of the challenge of balancing the potential benefits to be gained from encouraging innovation against the risk of harm to individuals, businesses and society from the lack of regulation to protect them.[85] International bodies such as the Council of Europe, the OECD and the United Nations, and its agency, UNESCO, are active in defining principles and standards designed to protect human rights against the negative impacts of AI systems.[86] Every intervention intended to uphold human rights norms is therefore a balancing act that must be assessed in each context.

Differences in approaches are apparent in AI governance initiatives announced by the United States and the European Union in 2023. President Biden's 2023 Executive Order on Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence emphasizes the obligations of AI developers of 'dual-use' foundation models to show that these will not lead to violations of federal laws on civil rights, discrimination, etc.[87] In contrast, the European Union's AI Act of 2024 takes a wider view that includes obligations on the part of AI developers to actively protect human rights.[88]

Before the emergence of AI-related regulation, the components of information ecosystems were already regulated at various levels: international law, regional standards and national laws. Recent initiatives to regulate the impact on AI on societies have started to home in on transparency requirements, training data disclosures and risk assessment obligations. Normative approaches include the United Nations resolution, 'Seizing the opportunities of safe, secure and trustworthy artificial intelligence systems for sustainable development', the OECD's Recommendation of the Council on Artificial Intelligence, UNESCO's Recommendation on the Ethics of AI, the G20 AI Principles, the G7 Hiroshima Process, including principles for GenAI, the AI Safety Summit Declaration in Bletchley, the Council of Europe Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law, and the Executive Order in the United States. The European Union's AI Act enters into force in 2025.[89] Many of these aim to guard against the risks and harms of mis- and disinformation.

Policy makers and their regulatory institutions face two connected challenges when developing rules for governing the impacts of AI on information ecosystems.[90] First, 'AI' is not a static product that can be regulated once, and regulatory approaches need to focus on the evolution of AI systems during their whole lifecycle, that is, throughout the design, development and deployment phases. Second, the impacts of the use of AI systems are seen as being more determinative of regulatory needs than abstract characteristics of a system (which are bound to change). For this reason, most regulatory approaches involve risk-based approaches that are used to define AI systems requirements based on the level of risk a system is judged to pose.[91] The aim of risk-based approaches is therefore seen by some as 'not primarily to manage risk but instead to ensure legislative proportionality' that will avoid stifling innovation.[92] An example of this is the European Union's AI Act of 2024, which classifies AI applications into different risk categories, with more extensive obligations for higher-risk applications.

[85] For reviews of research on the governance of algorithms and AI, see Gritsenko *et al.* (2022), supported by NOS-HS (Joint Committee for Nordic research councils in the Humanities and Social Sciences); Crawford (2021); and for resources on legal approaches, see Custers & Fosch-Villaronga (2022); De Bruyne & Vanleenhove (2021); Księżak & Wojtczak (2023); see also Bullock *et al.* (2022).

[86] Bello y Villarino (2023). Professional societies, such as the Institute of Electrical and Electronics Engineers (IEEE) are very active in this domain, especially in relation to Electronic Warfare (EW). See, for example, Koene *et al.* (2018).

[87] US Executive Order (2023, para. k). The dual-use foundation model is defined as an 'AI model that is trained on broad data; generally uses self-supervision; contains at least tens of billions of parameters; is applicable across a wide range of contexts; and that exhibits, or could be easily modified to exhibit, high levels of performance at tasks that pose a serious risk to security, national economic security, national public health or safety, or any combination of those matters…'

[88] European Commission (2024b); Larsen & Küspert (2024).

[89] Council of Europe (2024); G7 (2023); G20 (2019); OECD (2022c); UK DSIT (2023); UNESCO (2022c); UN (2024c); see also EC (2024c), agreed March 2024; US Executive Order (2023).

[90] De Gregorio (2023).

[91] Cole (2024).

[92] Mahler (2022, p. 247).

AI system risk categories. In the *first category*, certain AI systems are deemed so risky as to be 'unacceptable': an AI-based Aassessment of individuals' behavior by government agencies, that is, when they influence the 'free will' of users or contain 'social scoring'. Under the AI Act's scope, their use is prohibited in the European Union.

The *next* category includes 'high-risk' AI systems, which are listed in Annexes II and III of the Act. Annex II features a list of existing European Union regulations that require a 'conformity assessment' for products that bear specific risks. If an AI component is part of these products or the product 'itself', it is considered a 'high-risk' AI system. For the list in Annex III, the context of use is more relevant, that is, it is not the AI system itself that is considered risky, but the domain in which it is applied. Eight domains are named in which certain AI systems are 'high risk', such as those involved in decisions about access to education or employment. A particularly large number of applications that are considered 'high risk' are those involved in law enforcement or migration. If an AI system falls into this category, manufacturers and users must adhere to compliance obligations, such as having risk governance and quality management systems in place, and registering the AI system with the European Commission.[93]

The *third* category includes 'low-risk' AI systems, for which the Act requires 'only' transparency obligations and thus, significantly fewer requirements than for those in the 'high-risk' category. This means that providers of AI systems that (1) interact with humans, (2) are used for emotion or biometrics recognition, or (3) that generate 'deepfakes' must notify their users that the content was generated by AI.

Not regulated by the AI Act are 'risk-free' AI systems that include, for example, spam filters for email programs. Here, the risk for users is considered so small that no regulation is envisaged. For emerging AI systems not previously addressed, the AI Act stipulates that they must be categorized as 'high-risk' AI systems if they can negatively affect fundamental rights. This classification imposes substantial compliance duties on both providers and users of these AI systems. Article 13 requires providers of 'high-risk' AI systems to transparently outline the risks these systems pose to fundamental rights when employed, and Article 14(2) mandates human oversight of 'high-risk' AI systems to safeguard fundamental rights.

The AI Act also references fundamental rights at various points. These often serve to clarify the broader context and rationale for specific provisions at European Union level, highlighting the potential of AI systems to impact fundamental rights. For instance, recitals (legislative texts) address the risks of AI systems being used for manipulative or exploitative practices. One criticism voiced against regulating only primary uses of AI models, mainly exercised through quality assurance of their training data, is that risks of secondary use, where a model used in an AI system is applied in a way that its developers did not intend, may go undetected. A solution would be to focus on the concept of purpose limitation for AI models, which would leverage existing data protection approaches.[94] Some researchers are encouraging more stringent AI systems rules, arguing that law makers should learn from both ineffective and missing regulations during the early days of social media, when they failed to address the underlying business model that led platforms to prioritize the data-driven monetization of user attention.[95]

Many other regions and countries are putting strategies and governance frameworks in place.[96] Despite the fact that AI systems are largely developed by companies in the Global North and China, organizations in African countries, Latin America and Asia are

[93] Annexes I and III of the Act refer to harmonization with European Union legislation and listed high-risk AI systems requiring third-party conformity assessment.

[94] Mühlhoff & Ruschemeier (2024).

[95] Sanders & Schneider (2024); and there are calls for standards, see Lewkowiz & Sarf (2024); Schwartz *et al.* (2022), although some argue that companies will use voluntary standards to evade regulations on AI systems development (Han *et al.*, 2022).

[96] For a comprehensive review of AI systems regulation in emerging economies, see Findlay *et al.* (2023).

developing applications using large data sets and machine translation tools, and there are calls for the localized development of AI applications.[97]

- The *African Union* agreed a Continental Artificial Intelligence Strategy in July 2024. A review of the state of AI regulation in Africa in 2024 indicates that AI governance measures face challenges of 'weak institutional frameworks, limited judicial capacity, lack of expertise from policymakers, fragmented laws, and poor enforcement mechanisms, where laws, even if existing, are seldom applied'.[99]

- There are calls to reframe debates about AI governance in Global Majority regions to acknowledge power asymmetries and to recognize that the aim to develop 'responsible AI' governance frameworks still allows powerful companies to 'diffuse accountability, evade liability, and disregard rights'.[100]

- Discussions around AI governance typically exclude 'marginalized communities and groups including women, racial and sexual minorities, small producers, workers, and Indigenous communities'.[101]

- It has been pointed out that debates around ethical issues and requirements to ensure that AI systems are 'explainable' are rooted in Western perspectives – for example, in *sub-Saharan African countries*, where local informal savings and lending practices are common, AI tools to assess creditworthiness exclude these practices.[102]

- In *China*, some argue that academic input into shaping AI regulation is considerable, and that the emphasis is on strong binding regulations.[103]

Clearly uniform approaches to governing AI systems and tackling mis- and disinformation are not viable.[104] And when AI governance turns to ethical considerations, scholars in Global Majority World countries point to the bias of debates towards the interests of the Global North, which neglect approaches that differ from those adopted in *Europe* or the *United States*.[105] Proposed AI legislation in *Brazil*, for example, follows the European Union's AI Act in adopting a risk-based approach with a list of prohibited applications. It differs, however, in guaranteeing individual rights accompanied by judicial and administrative mechanisms to enforce these rights. These include the right to contestation and human intervention, emphasizing due process for people affected by automated decisions.[106]

Frameworks are being developed that transcend national boundaries and address the international implications of AI systems, beyond regional normative approaches and global commitments to sustainable and accountable AI. However, so far no organization has succeeded in taking the lead in driving the development of AI systems in a way that is based on international solidarity and inclusive participation.

4.5 GOVERNING NEWS MEDIA

Rule-based governance arrangements have implications for the way the news media is regulated, especially since what counts as news, what is a news media organization, and journalism profession norms and practices are changing, or at being least contested, in many countries.[107]

Legacy and online news media are intertwined in the data economy. The governance of data, digital platforms and AI influences the health of

[97] Okolo (2023).
[98] African Union (2024).
[99] Tech Hive Advisory Center for Law & Innovation (2024, p. 21).
[100] Gurumurthy & Bharthur (2023, p. 2).
[101] Gurumurthy & Bharthur (2023, p. 3).
[102] Effoduh (2024).
[103] Zhu (2022), supported by the Finnish National Agency for Education.
[104] Kakkar (2023).
[105] Gunkel *et al.* (2024); the need to differentiate between countries is illustrated by a comparison of AI systems in Senegal and Cambodia (Heng *et al.*, 2022).
[106] Government of Brazil (2023); Mendes & Kira (2023).
[107] See Section 4.1, Chapter 2 for a discussion of changing journalism practices.

information ecosystems. Verifiable news and informed public opinion are essential for democracy to function, and this requires high-quality public debate and deliberation and accountable representation. When mis- and disinformation circulate and the digital platforms operate in ways that depart from human rights expectations, there is no doubt that this contributes to democratic fragility.[108]

The news media are expected to preserve and maximize diversity and a plurality of voices in the public sphere within the framework of internationally agreed rights and responsibilities. Yet news media outlets face the challenge of declining levels of trust, some people are actively turning away from the news, there is a deficit of media pluralism, a growing dependence of news media organizations on digital platforms, increasing concentration in the news media industry in many countries, and absent or weak editorial independence.

News media regulation can backfire when it is used as a pretext to consolidate state power and control over information flows, which leads to censorship and repression or more subtle forms of leverage that hold news media organizations in check.

- In *Cuba*, the state maintains control over the mass media (also dominating artistic and intellectual affairs) by prohibiting private (legacy and online) media outlets under the 2019 Constitution, which classes them as being funded by 'enemies of the state'.[109]

- In *Hungary*, the use of media laws, efforts to control regulatory bodies and a concentrated media market have helped to consolidate domination by the ruling party.[110]

- When Apartheid ended in 1994 in *South Africa*, new governance arrangements for the media were introduced. The 1996 Constitution gave unprecedented levels of freedom to media organizations, emphasizing the priority to build an ethical, independent and publicly accountable news media, and moving from media self-regulation to co-regulation.[111] Yet there are complaints that the news media serves the interests of an elite, that disadvantaged community voices are not represented, and that the public broadcaster, South African Broadcasting Corporation (SABC), lacks independence. SABC is criticized for being too soft on the elected government, and debate focuses on whether the news media should be more critical of the democratic government or protect democracy by supporting it.[112]

- In *Turkey*, the government has sought to foster a favorable news media by leveraging structural, legislative and illegal measures to benefit the ruling party. After a failed coup in 2016, a restructuring of the media system led to greater repression through certain measures, including economic incentives, structural support for favoring the ruling party and control of regulatory bodies.[113]

- In *Venezuela*, a legal reorganization under the Hugo Chávez government (1999-2013) shifted the media system from private dominance (opposing the government) to state dominance (supporting the government), without alleviating the political and economic pressures on news media organizations. Under Nicolás Maduro (2013-19), the news media experienced further government pressures.[114]

- *Vietnam* and *Singapore* have implemented media regulations, including censorship, ownership controls, personnel management and other repressive instruments. Vietnam's approach is coercive while in Singapore, political norms are enforced implicitly by embedding stakeholders with financial interests in the media system.[115]

[108] Pickard (2022a, b); Tambini (2021); Tenove (2020).
[109] Garcia Santamaria & Salojärvi (2020); Romeu (2023).
[110] Polyák (2019).
[111] Wasserman (2020b).
[112] Wasserman (2020b).
[113] Akser & Baybars (2023).
[114] Gracia Santamaria & Salojärvi (2020).
[115] Haenig & Ji (2024), supported by the National Social Science Fund of China.

Repressive measures infringe on human rights, and they also create a space to produce mis- and disinformation and its circulation through both legacy and online news media.

In addition to political pressure, many news media organizations are dependent on digital platforms to circulate their news, and many news organizations are facing financial pressures, which leads to questions about their independence.[116] Declining advertising revenues can prevent news media organizations from fulfilling their democratic function, reduce media pluralism and contribute to perceptions that the news media industry is untrustworthy.

Power asymmetries between news media organizations and the big tech owners of digital platforms are visible in multiple regions. There have been clashes among the platforms, news organizations and regulators in *Australia*, *Canada* and the *European Union*, for example.[117] One remedy is to compensate publishers for the content that platforms host, since platforms derive substantial economic value from featuring news on their sites, although this can lead to the largest news media organizations benefiting disproportionately.[118] There are also disputes about the scale of compensation, especially among economists who argue that the digital platforms do not 'free ride' on the news media, and that payments by platforms to the publishers would inhibit innovation, among other reasons.[119] Other means of financially supporting news media, such as introducing taxes on digital advertising, are also being proposed.[120]

In the Global North and Global Majority World countries, there are moves to empower smaller news organizations to bargain collectively with big tech companies. Other measures include influencing the production, distribution and monetization of news content – for example, sometimes using their own apps on a subscription basis (mainly viable for the largest providers) by setting up paywalls or membership programs, creating their own real-time advertising marketing capability, or launching cooperative news organizations.[121]

Public service media (PSM) (including those permitted to attract advertising) are rarely economically sustainable without subsidies, concessions and/or protections that involve direct government financial support, license revenue, technical assistance and collaborative strategic programming and advocacy.[122] If news media are treated as 'a public good', this can help to maintain independent PSM organizations.[123] In countries where PSM is reasonably shielded from political pressure, these news organizations are a vital component of a healthy information ecosystem.[124] In countries where governments pressure news media organizations, both privately owned outlets and PSM often fail to meet normative expectations.[125]

In some countries and regions action is being taken to try to promote news media pluralism and media freedom and to counter mis- and disinformation.[126] For example, the *European Union* introduced a Democracy Action Plan in 2020, which included measures to promote free and fair elections, strengthen media freedom and counter mis- and disinformation.[127]

[116] Wasserman (2018); see also Chapter 2 for discussion of news media independence.

[117] Marshall (2023); Meese & Hurcombe (2021), funded by the Australian Research Council (ARC); Hermida (2023); see Section 2, Chapter 2 for more details on news media concentration.

[118] Flew (2023); Flew & Martin (2022).

[119] Lesh (2023); in early 2024 it was estimated that the platforms in the United States would owe news publishers annually between USD 11.9 and 13.9 billion – the methodology is explained in Mateen *et al.* (2023), two authors affiliated with the Brattle Group, US.

[120] Radsch (2022).

[121] Grover & Baik (2024); MacKenzie *et al.* (2023); Marshall (2023); Poell *et al.* (2023).

[122] Radsch (2022).

[123] UNESCO (2022d).

[124] Michalis & D'Arma (2024).

[125] Farahat (2021).

[126] Paal (2017).

[127] EC (2020b).

The Media Freedom Act. In the European Union, the Media Freedom Act aims to protect journalists' work, secure the independence of public media and increase the transparency of private media ownership. It requires a fair allocation of state advertising revenue to news media producers and aims to secure media freedom. The Act obliges member states to implement media concentration assessments (although it neither prevents media concentration nor sets a threshold). Article 22 introduces a 'media pluralism test', requiring member states to examine media mergers based on the implications for media pluralism and editorial independence, as well as market competition assessments. This is a substantial shift away from the previous hands-off approach to regulating media pluralism.[128]

The news media in Western democracies have been largely self-governing to protect their independence. The freedoms enjoyed by the news media historically have never been absolute in any country, and the privileges and duties of the journalism profession have varied across the world. In response to changes in the relations between news organizations, the platforms and state actors engaged in producing and circulating news, it is essential that human rights standards provide guidance on normative expectations, even if there are deviations in practice.[129]

5 Chapter Summary

This chapter has described the approaches applied by national governments (or regions) to govern the growing complexity of information ecosystems. These are spread across a spectrum, of hard and soft touch regulation: from voluntary corporate self-governance to co-regulation (state and corporate) to direct state intervention. All the components of information ecosystems, from the network infrastructure to the service applications layer, are subject to norms and rules that condition how they operate. These are expected to be consistent with broad principles, including for how data is collected and processed. We have presented the features of selected governance arrangements that are being put in place (and in some cases, resisted) around the world that influence information integrity and the health of information ecosystems.

There is broad agreement that states have a duty to act to protect human rights and fundamental freedoms. This includes a negative obligation not to violate rights – including those of big tech companies. States also have a positive obligation to protect human rights and implement them. This means that every aspect of governance involves a balancing act, with an outcome that varies with each context.

The synthesis of research in this chapter shows that:

- On the infrastructure layer of information ecosystems, network neutrality policies and 'zero-rating' regulations are central to how those who have connections and affordable access experience these ecosystems. These policies and others, such as internet shutdowns and social media blocking during elections or political unrest, contribute to fragmenting the internet and curbing access to information in many regions of the world. These policies and practices are informed by state ambitions to achieve digital sovereignty and corporate interests in profit.

- Governing how data is produced and used is increasingly controversial because of the lack of transparency in corporate data collection and monetization, targeted advertising and the

[128] EC (2024b, p. 3). The Act excludes user-generated content unless it is uploaded for financial or other consideration, purely private correspondence and services that do not have 'provision of programmes or press publications as their principal purpose', corporate communication and informational or promotional materials, but it includes freelancers. See also Brogi *et al.* (2023); Centre on Media Pluralism *et al.* (2022).

[129] Tambini (2021).

misuse of data for political gain. Legislation, such as the European Union's GDPR, is not a panacea for all data economy issues. It is important to attend to how approaches in higher-income and middle- and lower-income countries differ.

- Approaches to governing big tech-owned digital platforms, such as the European Union's Digital Services and Digital Markets Acts (and codes of practice to counter mis- and disinformation), have achieved prominence in debates about how to limit the spread of online mis- and disinformation. These place obligations on the largest platforms to take down illegal or suppress harmful mis- and disinformation. Governance measures vary significantly around the world regarding the penalties or criminalization of those who produce and circulate mis- and disinformation.

- AI systems governance focuses on balancing the potential benefits to be gained from encouraging innovation against the risk of harm to individuals, businesses and society from a lack of regulation. The European Union's AI Act shows how AI applications can be classified into risk categories, but homogeneous approaches to governing AI systems and tackling mis- and disinformation are unlikely to be viable. Frameworks are being developed that transcend national boundaries aimed at increasing transparency and accountability. So far, no organization has succeeded in taking the lead in driving the development of AI systems that are based on international solidarity and inclusive participation.

- Verifiable news and informed public opinion are essential if the public sphere is to provide a space for democratic participation. Regulatory measures applied to legacy and online news media can backfire when they are a pretext to consolidate state power and control information flows, leading to censorship or leverage over news media organizations. While news media freedom has never been absolute, and the privileges enjoyed by journalists and news media organizations vary throughout the world, human rights principles should guide normative expectations, even when there are deviations in practice.

Research is needed:

- To monitor the voluntary and anticipatory or remedial governance measures that are being introduced globally in response to the strategies and practices of big tech companies, and to systematically track corporate lobbying that frames governance in these companies' interests.

- To monitor the implementation of governance measures, whether they uphold fundamental human rights and whether they are effective in helping people navigate information ecosystems to be resilient to mis- and disinformation. It is essential to differentiate between normative goals and principles being articulated on a global level, and how these are translated into practice at local, country and regional levels over time.

- To assess the implementation of network neutrality policies in different contexts and their consequences.

- To examine how specific types of customer contracts restrict people's ability to access information and to participate in an informed way in information ecosystems.

- To examine systematically and on an ongoing basis the extent to which privacy and data protection, platform regulation, AI systems and news media governance are aligned with individuals' interests and the collective interest. Research must be inclusive of the experience of the Global Majority World.

References

- Abdulrauf, L. A., & Dube, H. (Eds) (2024). *Data Privacy Law in Africa: Emerging Perspectives*. Pretoria University Law Press.
- Afina, Y., Buchser, M., Krasodomski, A., Rowe, J., Sun, N., & Wilkinson, R. (2024). *Towards a Global Approach to Digital Platform Regulation: Preserving Openness Amid the Push for Internet Sovereignty*. Chatham House, Royal Institute of International Affairs.
- African Union. (2024). Continental Artificial Intelligence Strategy: Harnessing AI for Africa's development and prosperity. African Union Press Release, 9 August. https://au.int/en/documents/20240809/continental-artificial-intelligence-strategy#:~:text=The%20Continental%20AI%20Strategy%20calls,inclusive%20and%20responsible%20AI%20development
- Akman, P. (2022). Regulating competition in digital platform markets: A critical assessment of the famework and approach of the EU Digital Markets Act. *European Law Review*, 47(2022), 85-114. https://dialnet.unirioja.es/servlet/articulo?codigo=8320879
- Akser, M., & Baybars, B. (2023). Repressed media and illiberal politics in Turkey: The persistence of fear. *Southeast European and Black Sea Studies*, 23(1), 159-177. https://doi.org/10.1080/14683857.2022.2088647
- Andere, B., & Kathure, M. (2024). *Strengthening Data Protection in Africa: Key Issues for Implementation*. Access Now. www.accessnow.org/wp-content/uploads/2024/01/Strengthening-data-protection-in-Africa-key-issues-for-implementation-updated.pdf
- Baranes, E. (2014). The interplay between network investment and content quality: Implications to net neutrality on the Internet. *Information Economics and Policy*, 28, 57-69. https://doi.org/10.1016/j.infoecopol.2014.07.002
- Bauer, J. M., & Knieps, G. (2018). Complementary innovation and network neutrality. *Telecommunications Policy*, 42(2), 172-183. https://doi.org/10.1016/j.telpol.2017.11.006
- Bello y Villarino, J.-M. (2023). Global standard-setting for artificial intelligence: Para-regulating international law for AI? *The Australian Year Book of International Law Online*. https://brill.com/view/journals/auso/41/1/article-p157_7.xml
- BEREC (Body of European Regulators for Electronic Communications). (2024a). *BEREC Guidelines on the Implementation by National Regulators of European Net Neutrality Rules*. www.berec.europa.eu/en/document-categories/berec/regulatory-best-practices/guidelines/berec-guidelines-on-the-implementation-by-national-regulators-of-european-net-neutrality-rules
- BEREC. (2024b). What is zero-rating? www.berec.europa.eu/en/what-is-zero-rating
- Boas, T. C. (2006). Weaving the Authoritarian Web: The Control of Internet Use in Nondemocratic Regimes. In J. Zysman & A. Newman (Eds), *How Revolutionary Was the Digital Revolution? National Responses, Market Transitions and Global Technology* (pp. 361-378). Stanford University Press.
- Botta, M. (2021). Sector regulation of digital platforms in Europe: Uno, Nessuno e Centomila. *Journal of European Competition Law & Practice*, 12(7), 500-512. https://doi.org/10.1093/jeclap/lpab046
- Brignull, H. (2023). *Deceptive Patterns: Exposing the Tricks Tech Companies Use to Control You*. Testimonium Ltd.
- Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative power Europe to the test of its geopolitical ambitions. *JCMS: Journal of Common Market Studies*, 61(5), 1261-1280. https://doi.org/10.1111/jcms.13462
- Brogi, E., Borges, D., Carlini, R., Nenadic, I., *et al.* (2023). *The European Media Freedom Act: Media Freedom, Freedom of Expression and Pluralism*. European Parliament's Committee on Civil Liberties, Justice and Home Affairs, PE 747.930.
- Broughton Micova, S. B., & Jacques, S. (2020). The functions of data in the competition between audiovisual media and video sharing platforms foradvertising. *Journal of Information Policy*, 10, 514-548. https://doi.org/10.5325/jinfopoli.10.2020.0514
- Brown, I., & Marsden, C. T. (2023). *Regulating Code: Good Governance and Better Regulation in the Information Age*. MIT Press.
- Bryant, M. (2021). Is Facebook leading us on a journey to the metaverse? *The Observer*, 26 September. www.theguardian.com/technology/2021/sep/26/is-facebook-leading-us-on-a-journey-to-the-metaverse
- Bullock, J. B., Chen, Y.-C., Himmelreich, J., Hudson, V. M., *et al.* (2022). *The Oxford Handbook of AI Governance*. Oxford University Press.
- Centre on Media Pluralism, Media Freedom, CITI, KU Leuven, *et al.* (2022). *Study on Media Plurality and Diversity Online: Final Report*. European Commission, LC-01637953.
- Chin, Y. C. (2024). Right to Data Access in the Digital Era: The Case of China. In M. Aslama Horowitz. H. Niemeinen, K. Lehtisaari, & A. D'Arma (Eds), *Epistemic Rights in the Era of Digital Disruption* (pp. 187-201). Springer International Publishing.
- Church, P., & Pehlivan, C. N. (2023). The Digital Services Act (DSA): A new era for online harms and intermediary liability. *Global Privacy Law Review*, 4(1), 1-7. https://kluwerlawonline.com/api/Product/CitationPDFURL?file=Journals\GPLR\GPLR2023005.pdf
- Cole, M. D. (2024). AI regulation and governance on a global scale: An overview of international, regional and national instruments. *Journal of AI Law and Regulation*, 1(1), 126-142. https://doi.org/10.21552/aire/2024/1/16

- Coos, A. (2022). Data protection in Japan: All you need to know about APPI. Endpoint Protector Blog, 5 April. www.endpointprotector.com/blog/data-protection-in-japan-appi
- Council of Europe. (2024). *Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law*. 133rd Meeting, 17 May 2024, CM(2024)52-final.
- Crawford, K. (2021). *The Atlas of AI: Power, Politics, and the Planetary Costs of Artificial Intelligence*. Yale University Press.
- Crémer, J., de Montjoye, Y.-A., & Schweitzer, H. (2019). *Competition Policy for the Digital Era: Final Report*. European Commission DG Competition.
- Culloty, E. (2021). Désinformation sur la migration: UN problème de longue date au dimensions technologiques nouvelles. In M. McAuliffe & A. Triandafyllidou (Eds), *Rapport État de la Migration Dans Le Monde* (pp. 229-245). Organisation internationale pour les migrations (OIM).
- Custers, B., & Fosch-Villaronga, E. (Eds) (2022). *Law and Artificial Intelligence: Regulating AI and Applying AI in Legal Practice*. T.M.C. Asser Press.
- De Blasio, E., & Selva, D. (2021). Who is responsible for disinformation? European approaches to social platforms' accountability in the post-truth era. *American Behavioral Scientist*, 65(6), 825-846. https://doi.org/10.1177/0002764221989784
- De Bruyne, J., & Vanleenhove, C. (Eds) (2021). *Artificial Intelligence and the Law*. Intersentia.
- De Gregorio, G. (2023). The normative power of artificial intelligence. Indiana Journal of Global Legal Studies 55, 30(2). https://ssrn.com/abstract=4436287
- Dellinger, J., & Pell, S. (2024). Bodies of evidence: The criminalization of abortion and surveillance of women in a post-DOBBS world. *Duke Journal of Constitutional Law & Public Policy*, 19, 1-99. http://dx.doi.org/10.2139/ssrn.4599445
- DiGi (Digital Industry Group). (2022). *Australian Code of Practice on Disinformation and Misinformation*. https://digi.org.au/disinformation-code
- Dittrich, P.-J. (2019). *Tackling the Spread of Disinformation: Why a Co-Regulatory Approach Is the Right Way Forward for the EU*. Bertelsmann Stiftung Policy Paper 12, Hertie School, Jacques Delors Centre.
- Dolata, M., Feuerriegel, S., & Schwabe, G. (2022). A sociotechnical view of algorithmic fairness. *Information Systems Journal*, 32(4), 754-818. https://doi.org/10.1111/isj.12370
- Durach, F., Bârgăoanu, A., & Nastasiu, C. (2020). Tackling disinformation: EU regulation of the digital space. *Romanian Journal of European Affairs*, 20(1), 5-20. https://papers.ssrn.com/abstract=3650780
- EC (European Commission). (2012). *Consolidated Version of the Treaty on the Functioning of the European Union (TFEU)*. C326/47. www.legislation.gov.uk/eut/teec/contents
- EC. (2016b). *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Processing of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)*. OJ L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679
- EC. (2018). *Communication – Tackling Online Disinformation: A European Approach*. COM(2018) 236 final. https://digital-strategy.ec.europa.eu/en/library/communication-tackling-online-disinformation-european-approach
- EC. (2022a). *Contestable and Fair Markets in the Digital Sector and Amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act), PE/17/2022/REV/1*. Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022. https://eur-lex.europa.eu/eli/reg/2022/1925/oj
- EC. (2020b). *Communication on the European Democracy Action Plan*. COM(2020) 790 final. www.europeansources.info/record/communication-on-the-european-democracy-action-plan
- EC. (2022c). *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)*. https://eur-lex.europa.eu/eli/reg/2022/2065/oj
- EC. (2022d). *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)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022R0868
- EC. (2022e). *The Strengthened Code of Practice on Disinformation 2022*. https://digital-strategy.ec.europa.eu/en/library/2022-strengthened-code-practice-disinformation
- EC. (2023). *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)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202302854
- EC. (2024b). *Regulation (EU) 2024/1083 Establishing a Common Framework for Media Service (European Media Freedom Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401083
- EC. (2024c). *Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 Laying Down Harmonised Rules on Artificial Intelligence (Artificial Intelligence Act)*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L_202401689
- Economides, N., & Hermalin, B. E. (2012). The economics of network neutrality. *The RAND Journal of Economics*, 43(4), 602-629. www.jstor.org/stable/41723347
- Effoduh, J. O. (2024). A Global South perspective on explainable AI. Carnegie Endowment for International Peace, 30 April. https://carnegieendowment.org/2024/04/30/global-south-perspective-on-explainable-ai-pub-92333

- Eisenach, J. A. (2015). *The Economics of Zero Rating*. NERA Economic Consulting, US.
- Erman, E., & Furendal, M. (2022). The global governance of artificial intelligence: Some normative concerns. *Moral Philosophy and Politics*, 9(2), 267-291. https://doi.org/10.1515/mopp-2020-0046
- Farahat, M. (2021). *Egypt Digital Rights Landscape Report*. Institute for Development Studies, Sussex.
- Findlay, M., Ong, L. M., & Zhang, W. (Eds) (2023). Elgar Companion to Regulating AI and Big Data in Emerging Economies. Edward Elgar Publishing.
- Flew, T. (2021). *Regulating Platforms*. Polity Press.
- Flew, T. (2023). Mediated trust and artificial intelligence. *Emerging Media*, 1(1), 22-29. https://doi.org/10.1177/27523543231188793
- Flew, T., & Martin, F. R. (Eds) (2022). *Digital Platform Regulation: Global Perspectives on Internet Governance*. Springer International.
- Forum on Information and Democracy. (2024d). US Supreme Court Decision on social media regulation, uncertainty remains! Unpacking Current Developments in the Information Space, Insight Nr. 2. https://informationdemocracy.org/wp-content/uploads/2024/09/FID-Insight-Nr-2-US-Supreme-Court-Decision-on-social-media-regulation.pdf
- FTC (Federal Trade Commission). (2024). FTC launches inquiry into generative AI investments and partnerships. Federal Trade Commission News, 25 January. www.ftc.gov/news-events/news/press-releases/2024/01/ftc-launches-inquiry-generative-ai-investments-partnerships
- G7. (2023). *Hiroshima Process International Guiding Principles for Organizations Developing Advanced AI Systems*. G7 2023 Hiroshima Summit. https://www.mofa.go.jp/files/100573471.pdf
- G20. (2019). *G20 Ministerial Statement on Trade and Digital Economy, Annex G20 AI Principles*. https://wp.oecd.ai/app/uploads/2021/06/G20-AI-Principles.pdf
- Galantino, S. (2023). How will the EU Digital Services Act affect the regulation of disinformation? *SCRIPTed: A Journal of Law, Technology and Society*, 20(1), 89-129. https://script-ed.org/wp-content/uploads/2023/02/Sharon-Galantino_February-2023.pdf?d=05112024
- German Law Archive. (2017). *Network Enforcement Act (Netzdurchsetzunggesetz, NetzDG)*. Government of Germany.
- Gerpott, T. J. (2018). Zero-rating arrangements of mobile Internet access service providers – An analysis of main factors shaping the need for regulatory interventions. *Telecommunications Policy*, 42(6), 489-500. https://doi.org/10.1016/j.telpol.2018.03.003
- Government of Brazil. (2018). *Lei Geral de Proteção de Dados Pessoais* (LGPD).
- Government of Brazil. (2023). Projeto de Lei 2338/2023, *Dispõe sobre o uso da Inteligência Artificial*. Internal Temporary Commission on Artificial Intelligence in Brazil.
- Government of France. (2018). *Regarding the Fight Against Information Manipulation*. Organic Law No. 2018-1201 of 22 December 2018.
- Government of India. (2023). *The Digital Personal Data Protection Act*, 2023.
- Garcia Santamaria, S., & Salojärvi, V. (2020). Media in Authoritarian Contexts: A Logics Approach to Journalistic Professional Resistance in Cuba and Venezuela. In X. Orchard, S. Garcia Santamaria, J. Brambila, & J. Lugo-Ocando (Eds), *Media & Governance in Latin America: Towards Plurality of Voices* (pp. 97-116). Peter Lang.
- Greenstein, S., Peitz, M., & Valletti, T. (2016). Net neutrality: A fast lane to understanding the trade-offs. *Journal of Economic Perspectives*, 30(2), 127-150. https://doi.org/10.1257/jep.30.2.127
- Gritsenko, D., Markham, A., Pötzsch, H., & Wijermars, M. (2022). Algorithms, contexts, governance: An introduction to the special issue. *New Media & Society*, 24(4), 835-844. https://doi.org/10.1177/14614448221079037
- Grover, R., & Baik, J. (2024). Platforms as templates: Emerging datafication dynamics in digital news outlets' datawalls. *The Information Society*, 40(4), 260-276. https://doi.org/10.1080/01972243.2024.2350015
- Gunkel, D. J., Ali, S. M., Paragi, B., Daly, A. C., *et al.* (2024). The (Un)bearable Whiteness of AI Ethics. In D. J. Gunkel (Ed.), *Handbook on the Ethics of Artificial Intelligence* (pp. 218-231). Edward Elgar Publishing.
- Gurumurthy, A., & Bharthur, D. (2023). *Reframing AI Governance through a Political Economy Lens*. IT for Change. https://itforchange.net/index.php/reframing-ai-governance-through-a-political-economy-lens
- Haenig, M. A., & Ji, X. (2024). A tale of two Southeast Asian states: Media governance and authoritarian regimes in Singapore and Vietnam. *Asian Review of Political Economy*, 3(4), 1-23. https://doi.org/10.1007/s44216-024-00024-6
- Halpern, H., Brown, G., Kagan, O., Li, L., & Avramenko, A. (2024). Google accused of privacy breaches over alleged Chrome tracking. GRC World Forums, 14 June. www.grcworldforums.com/risk/google-accused-of-privacy-breaches-over-alleged-chrome-tracking/9675.article
- Han, T. A., Lenaerts, T., Santos, F. C., & Pereira, L. M. (2022). Voluntary safety commitments provide an escape from over-regulation in AI development. *Technology in Society*, 68(2022), 1-14. https://doi.org/10.1016/j.techsoc.2021.101843
- He, A. (2023). *State-Centric Data Governance in China*. CIGI Papers No. 282. CIGI (Centre for International Governance Innovation), Canada.
- Heng, S., Tsilionis, K., Scharff, C., & Wautelet, Y. (2022). Understanding AI ecosystems in the Global South: The cases of Senegal and Cambodia. *International Journal of Information Management*, 64(2022), 1-18. https://doi.org/10.1016/j.ijinfomgt.2021.102454

- Hermida, A. (2023). Journalism prepares for a post-search, post-social future. Nieman Lab. www.niemanlab.org/2023/12/journalism-prepares-for-a-post-search-post-social-future
- Hildebrandt, C., & Wiewiorra, L. (2024). The past, present, and future of (net) neutrality: A state of knowledge review and research agenda. *Journal of Information Technology*, 39(1), 167-193. https://doi.org/10.1177/02683962231170891
- Hoskins, G. T. (2024). Far right > digital rights: The precarity of free expression, internet access, net neutrality and data privacy in Bolsonaro's Brazil. *Javnost – The Public*, 31(2), 309-326. https://doi.org/10.1080/13183222.2024.2346704
- Houser, K., & Voss, W. G. (2018). GDPR: The end of Google and Facebook or a new paradigm in data privacy? *Richmond Journal of Law & Technology*, 25(1), 1-109. https://jolt.richmond.edu/files/2018/11/Houser_Voss-FE.pdf
- Howard, P. N., & Hussain, M. M. (2013). Democracy's Fourth Wave? Digital Media and the Arab Spring. Oxford University Press.
- Justice *K.S. Puttaswamy (Retd.) & Anr. vs. Union of India & Ors* (Judge Bench Civil Writ Petition, Case (2017) 10SCC 1, AIR 2017 SC 4161 2017). https://privacylibrary.ccgnlud.org/case/justice-ks-puttaswamy-ors-vs-union-of-india-ors#:~:text=Case%20Brief&text=The%20nine%20Judge%20Bench%20in,of%20dignity%2C%20autonomy%20and%20liberty.
- Jaunaux, L., & Lebourges, M. (2019). Zero rating and end-users' freedom of choice: An economic analysis. *Digital Policy, Regulation and Governance*, 21(2), 115-128. https://doi.org/10.1108/DPRG-06-2018-0030
- Jordan, S. (2017). Evaluating zero-rating and associated throttling practices under the Open Internet Order. *Journal of Information Policy*, 7, 450-507. https://doi.org/10.5325/jinfopoli.7.2017.0450
- Just, N. (2018). Governing online platforms: Competition policy in times of platformization. *Telecommunications Policy*, 42(5), 386–394. https://doi.org/10.1016/j.telpol.2018.02.006
- Just, N. (2022). Which is to be master? Competition law or regulation in platform markets. *International Journal of Communication*, 16(2022), 504-524. https://ijoc.org/index.php/ijoc/article/view/13095/3657
- Kakkar, J. M. (2023). Tackling Misinformation in Emerging Economies and the Global South: Exploring Approaches for the Indian Context. In F. Fukuyama & M. Schaake (Eds), *Digital Technologies in Emerging Countries* (pp. 48-62). Cyber Policy Centre, Freeman Spogli Institute and Stanford Law School, Stanford University.
- Kalathil, S., & Boas, T. C. (2003). *Open Networks, Closed Regimes: The Impact of the Internet on Authoritarian Rule*. Carnegie Endowment for International Peace.
- Kerber, W. (2020). *From (Horizontal and Sectoral) Data Access Solutions towards Data Governance Systems*. Joint Discussion Paper No. 40-2020. Series in Economics. Universities of Aachen, Gießen, Göttingen Kassel, Marburg, Siegen.
- Keremoğlu, E., & Weidmann, N. B. (2020). How dictators control the internet: A review essay. *Comparative Political Studies*, 53(10-11), 1690-1703. https://doi.org/10.1177/0010414020912278
- Kira, B., Sinha, V., & Srinivasan, S. (2021). Regulating digital ecosystems: Bridging the gap between competition policy and data protection. *Industrial and Corporate Change*, 30(5), 1337-1360. https://academic.oup.com/icc/article/30/5/1337/6356942
- Koene, A., Smith, A. L., Egawa, T., Mandalh, S., & Hatada, Y. (2018). IEEE P70xx, establishing standards for ethical technology. *Proceedings of KDD*. https://doi.org/10.1145/nnnnnnn.nnnnnnn
- Kokas, A. (2022). Becoming a Cyber Sovereign: China's Politics of Data Governance. In A. Kokas, *Trafficking Data: How China Is Winning the Battle for Digital Sovereignty* (pp. 51-C53.P72). Oxford Academic.
- Kokshagina, O., Reinecke, P. C., & Karanasios, S. (2023). To regulate or not to regulate: Unravelling institutional tussles around the regulation of algorithmic control of digital platforms. *Journal of Information Technology*, 38(2), 160-179. https://doi.org/10.1177/02683962221114408
- Krämer, J., & Peitz, M. (2018). A fresh look at zero-rating. *Telecommunications Policy*, 42(7), 501-513. https://doi.org/10.1016/j.telpol.2018.06.005
- Księżak, P., & Wojtczak, S. (2023). *Toward a Conceptual Network for the Private Law of Artificial Intelligence* (Vol. 51). Springer International Publishing.
- Kumar, A., & Thussu, D. (2023). Media, digital sovereignty and geopolitics: The case of the TikTok ban in India. *Media, Culture & Society*, 45(8), 1583-1599. https://doi.org/10.1177/01634437231174351
- Larsen, B. C., & Küspert, S. (2024). Regulating general-purpose AI: Areas of convergence and divergence across the EU and the US. Brookings Institution Research, 21 May. www.brookings.edu/articles/regulating-general-purpose-ai-areas-of-convergence-and-divergence-across-the-eu-and-the-us
- Lee, D., & Shin, D.-H. (2016). The effects of network neutrality on the incentive to discriminate, invest, and innovate: a literature review. *info*, 18(3), 42-57. https://doi.org/10.1108/info-12-2015-0053
- Lesh, M. (2023). *Breaking the News? Should Digital Platforms Be Required to Fund News Publishers?* IEA Discussion paper No. 119. Institute of Economic Affairs.
- Lewkowiz, G., & Sarf, R. (2024). Taking technical standardization of fundamental rights seriously for trustworthy artificial intelligence. *La Revue des Juristes de Sciences Po*, 25, 42-46. https://centreperelman.be//content/uploads/2024/03/GL-RS-AI-Technical-standards-and-fundamental-rights.pdf
- Lim, G., & Bradshaw, S. (2023). *Chilling Legislation: Tracking the Impact of 'Fake News' Laws on Press Freedom Internationally*. Center for International Media Assistance.

- Linden, T., Khandelwal, R., Harkous, H., & Fawaz, K. (2020). The privacy policy landscape after the GDPR. ArXiv. https://doi.org/10.48550/arXiv.1809.083696
- MacKenzie, D., Caliskan, K., & Rommerskirchen, C. (2023). The longest second: Header bidding and the material politics of online advertising. *Economy and Society*, 52(3), 554-578. https://doi.org/10.1080/03085147.2023.2238463
- Mahler, T. (2022). Between Risk Management and Proportionality: The Risk-Based Approach in the EU's Artificial Intelligence Act Proposal. In L. Colonna & S. Greenstein (Eds), *Law in the Era of Artificial Intelligence: Nordic Yearbook of Law and Informatics 2020-2021* (pp. 247-270). The Swedish Law and Informatics Research Institute.
- Malaysia Government. (2018). *Anti-Fake News Bill 2018*.
- Mansell, R. (2021). European Responses to (US) Digital Platform Dominance. In D. Y. Jin (Ed.), *The Routledge Handbook of Digital Media and Globalization* (pp. 141-149). Routledge.
- Mare, A. (2020). State-ordered internet shutdowns and digital authoritarianism in Zimbabwe. *International Journal of Communication*, 14(2020), 4244-4263. https://ijoc.org/index.php/ijoc/article/view/11494
- Marsden, C. T. (2016). Comparative case studies in implementing net neutrality: A critical analysis of zero rating. SCRIPTed: *A Journal of Law, Technology & Society*, 13(1), 1-39. https://doi.org/10.2966/scrip.130116.1
- Marsden, C. T., & Brown, I. (2023). App stores, antitrust and their links to net neutrality: A review of the European policy and academic debate leading to the EU Digital Markets Act. *Internet Policy Review*, 12(1), 1-27. https://policyreview.info/articles/analysis/app-stores-antitrust-net-neutrality-eu-digital-markets-act
- Marshall, S. (2023). We get past 'post-platform'. Nieman Lab. www.niemanlab.org/2023/12/we-get-past-post-platform
- Mateen, H., Tabakovic, H., Holder, P., & Schiffrin, A. (2023). *Paying for News: What Google and Meta Owe Publishers*. Initiative for Policy Dialogue, Columbia University. http://dx.doi.org/10.2139/ssrn.4704237
- Mattelart, T. (2023). US Digital Platforms in the Global South: A Critical Review of an Emerging Research Field. In P. Bouquillion, C. Ithurbide, & T. Mattelart (Eds), *Digital Platforms and the Global South: Reconfiguring Power Relations in the Cultural Industries* (pp. 18-36). Routledge.
- Meese, J., & Hurcombe, E. (2021). Facebook, news media and platform dependency: The institutional impacts of news distribution on social platforms. *New Media & Society*, 23(8), 2367-2384. https://doi.org/10.1177/1461444820926472
- Mendes, L. S., & Kira, B. (2023). The road to regulation of artificial intelligence: The Brazilian experience. *Internet Policy Review*, 21 December. https://policyreview.info/articles/news/road-regulation-artificial-intelligence-brazilian-experience/1737
- Menon, S. (2021). An institutional analysis of TMP regulation in India. *Review of Policy Research*, 38(3), 300-325. https://doi.org/10.1111/ropr.12425
- Michalis, M., & D'Arma, A. (2024). Public Service Media: From Epistemic Rights to Justice. In M. A. Horowitz, H. Nieminen, K. Lehtisaari, & A. D'Arma (Ed.), *Epistemic Rights in the Era of Digital Disruption* (pp. 97-109). Springer International Publishing.
- Monti, M. (2020). The EU Code of Practice on Disinformation and the Risk of the Privatisation of Censorship. In S. Giusti & E. Piras (Eds), *Democracy and Fake News: Information Manipulation and Post-Truth Politics* (pp. 214-225). Routledge.
- Moreno Belloso, N., & Petit, N. (2023). The EU Digital Markets Act (DMA): A competition hand in a regulatory glove. *European Law Review*, 48(4), 391-421. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4411743
- Motamedi, M. (2024). Iran unveils plan for tighter internet rules to promote local platforms. Al Jazeera, 24 February. www.aljazeera.com/news/2024/2/24/iran-unveils-plan-for-tighter-internet-rules-to-promote-local-platforms
- Mühlhoff, R., & Ruschemeier, H. (2024). Regulating AI with purpose limitation for models. Journal of AI Law and Regulation, 1(1), 24-39. https://doi.org/10.21552/aire/2024/1/5
- Mukerjee, S. (2016). Net neutrality, Facebook, and India's battle to #SaveTheInternet. *Communication and the Public*, 1(3), 356-361. https://doi.org/10.1177/2057047316665850
- Murgia, M. (2019). Google accused of secretly feeding personal data to advertisers. *The Financial Times*. www.ft.com/content/e3e1697e-ce57-11e9-99a4-b5ded7a7fe3f
- Murtaza, G., & Salman, S. (2019). GDPR fine imposed upon Google: An analysis. Manuscript. Brown University. https://cs.brown.edu/courses/csci2390/2019/assign/gdpr/ssalman1-gmurtaza-google.pdf
- Ndemo, B., & Thegeya, A. (2023). A Prototype Data Governance Framework for Africa. In B. Ndemo, N. Ndung'u, S. Odhiambo, & A. Shimeles (Eds), *Data Governance and Policy in Africa* (pp. 9-29). Springer.
- Nenadić, I., Brogi, E., & Bleyer-Simon, K. (2023). *Structural Indicators to Assess Effectiveness of the EU's Code of Practice on Disinformation*. RSC Working Paper 2023/34. European University Institute.
- Nicoli, N., & Iosifidis, P. (2023). EU digital economy competition policy: From ex-post to ex-ante. The case of Alphabet, Amazon, Apple, and Meta. *Global Media and China*, 8(1), 24-38. https://doi.org/10.1177/20594364231152673
- Nothias, T. (2020). Access granted: Facebook's free basics in Africa. *Media, Culture & Society*, 42(3), 329-348. https://doi.org/10.1177/0163443719890530
- O'Faolain, A. (2024). Court dismisses claim data watchdog failed to investigate alleged breach by Google. *The Irish Times*, 24 June. www.irishtimes.com/crime-law/courts/2024/06/24/court-dismisses-claim-data-watchdog-failed-to-investigate-alleged-breach-by-google
- OECD (Organisation for Economic Co-operation and Development). (2022c). *Recommendation of the Council on Artificial Intelligence*. https://oecd.ai/en/assets/files/OECD-LEGAL-0449-en.pdf

- OECD. (2024). *Facts not Fakes: Tackling Disinformation, Strengthening Information Integrity*. www.oecd.org/en/publications/facts-not-fakes-tackling-disinformation-strengthening-information-integrity_d909ff7a-en.html
- Okolo, C. T. (2023). AI in the Global South: Opportunities and challenges towards more inclusive governance. Brookings Institution Commentary, 1 November. www.brookings.edu/articles/ai-in-the-global-south-opportunities-and-challenges-towards-more-inclusive-governance
- Paal, B. (2017). Current issues and recent developments on media concentration in the context of competition law and media law. *Journal of Intellectual Property Law and Practice*, 12(7), 610-616. https://academic.oup.com/jiplp/article-abstract/12/7/610/3916940
- Pamment, J. (2020). *EU Code of Practice on Disinformation: Briefing Note for the New European Commission*. Working Paper. Carnegie Endowment for International Peace.
- Park, G. (2020). The changing wind of data privacy law: A comparative study of the European Union's General Data Protection Regulation and the 2018 California Consumer Privacy Act. *UC Irvine Law Review*, 10(4), 1455-1489. https://escholarship.org/content/qt8562f0v0/qt8562f0v0.pdf
- Pickard, V. (2020b). Monopoly Control over Digital Infrastructures. In V. Pickard, *Democracy without Journalism? Confronting the Misinformation Society* (pp. 104-135). Oxford University Press.
- Pickard, V. (2022a). Can Journalism Survive in the Age of Platform Monopolies? Confronting Facebook's Negative Externalities. In T. Flew & F. R. Martin (Eds), *Digital Platform Regulation: Global Perspectives on Internet Governance* (pp. 23-42). Palgrave Macmillan.
- Pickard, V. (2022b). Democratizing the platforms: Promises and perils of public utility regulation. *Media Development*, 68(3), 6-10. www.asc.upenn.edu/sites/default/files/2022-10/Democratizing%20the%20platforms%20-%20Victor%20Pickard.pdf
- Pickard, V., & Berman, D. E. (2019). *After Net Neutrality: A New Deal for the Digital Age*. Yale University Press.
- Poell, T., Nieborg, D. B., & Duffy, B. E. (2023). Spaces of negotiation: Analyzing platform power in the news industry. *Digital Journalism*, 11(8), 1391-1409. https://doi.org/10.1080/21670811.2022.2103011
- Polyák, G. (2019). Media in Hungary: Three Pillars of an Illiberal Democracy. In E. Połońska & C. Beckett (Eds), *Public Service Broadcasting and Media Systems in Troubled European Democracies* (pp. 279-303). Palgrave Macmillan.
- Prasad, R. (2018). Ascendant India, digital India: How net neutrality advocates defeated Facebook's Free Basics. *Media, Culture & Society*, 40(3), 415-431. https://doi.org/10.1177/0163443717736117
- Program for Public Consultation. (2022). Three-in-four voters favor reinstating net neutrality. School of Public Policy, University of Maryland. https://publicconsultation.org/united-states/three-in-four-voters-favor-reinstating-net-neutrality
- Punia, S., Mohan, S., Kakkar, J. M., & Bhandari, V. (Eds) (2022). *Emerging Trends in Data Governance*. National Law University, Delhi Press.
- Puppis, M., Mansell, R., & Van den Bulck, H. (Eds) (2024). *Handbook of Media and Communication Governance*. Edward Elgar Publishing.
- Radsch, C. C. (2022). *Making Big Tech Pay for the News They Use*. Center for International Media Assistance US.
- Radsch, C. C. (2023a). Envisioning a healthy information ecosystem. CDT (Center for Democracy and Technology), 2 June. https://cdt.org/insights/from-our-fellows-envisioning-a-healthy-information-ecosystem
- Radsch, C. C. (2024). The must-carry solution for the media's Google problem. *Washington Monthly*, 22 August. https://washingtonmonthly.com/2024/08/22/the-must-carry-solution-for-the-medias-google-problem
- Repnikova, M. (2018). China's lessons for fighting fake news. *Foreign Policy*, 6 September. https://foreignpolicy.com/2018/09/06/chinas-lessons-for-fighting-fake-news
- Reuters. (2019). China seeks to root out fake news and deepfakes with new online content rules. 29 November. www.reuters.com/article/idUSKBN1Y30VT
- Reyna, A. (2024). DMA and DSA *effective* enforcement – Key to success. *Journal of Antitrust Enforcement*, 12(2), 320-324. https://doi.org/10.1093/jaenfo/jnae018
- Richter, A. (2019). *Disinformation in the Media under Russian Law*. European Audiovisual Observatory.
- Robb, G., & Hawthorne, R. (2019). Net neutrality and market power: The case of South Africa. *Telecommunications Policy*, 43(9), 1-15. https://doi.org/10.1016/j.telpol.2019.03.003
- Roberts, H., Hine, E., Taddeo, M., & Floridi, L. (2024). Global AI governance: Barriers and pathways forward. *International Affairs*, 100(3), 1275-1286. https://doi.org/10.1093/ia/iiae073
- Romeu, A. (2023). New digital law tightens clampdown on press freedom in Cuba. Reporters Without Borders. https://rsf.org/en/new-digital-law-tightens-clampdown-press-freedom-cuba
- Roth, E. (2022). Google results for abortion clinics are misleading and politically fraught. *The Verge*, 16 August. www.theverge.com/2022/8/16/23307850/google-maps-results-abortion-clinics-crisis-pregnancy-centers
- Ryng, J., Guicherd, G., Saman, J. A., Choudhury, P., & Kellett, A. (2022). Internet shutdowns: A human rights issue. The RUSI Journal, 167(4-5), 50-63. https://doi.org/10.1080/03071847.2022.2156234
- Sampath, P. G. (2021). Governing artificial intelligence in an age of inequality. *Global Policy*, 12(S6), 21-31. https://doi.org/10.1111/1758-5899.12940

- Sanders, N. E., & Schneider, B. (2024). Let's not make the same mistakes with AI that we made with social media. *MIT Technology Review*, 13 March. www.technologyreview.com/2024/03/13/1089729/lets-not-make-the-same-mistakes-with-ai-that-we-made-with-social-media
- Saurwein, F., & Spencer-Smith, C. (2020). Combating disinformation on social media: Multilevel governance and distributed accountability in Europe. *Digital Journalism*, 8(6), 820-841. https://doi.org/10.1080/21670811.2020.1765401
- Schwartz, R., Vassilev, A., Greene, K., Perine, L., Burt, A., & Hall, P. (2022). *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*, US National Institute of Standards and Technology.
- Shahbaz, A., Funk, A., & Vesteinsson, K. (2022). *Countering an Authoritarian Overhaul of the Internet*. Freedom House.
- Shahin, S. (2019). Facing up to Facebook: How digital activism, independent regulation, and mass media foiled a neoliberal threat to net neutrality. *Information, Communication & Society*, 22(1), 1-17. https://doi.org/10.1080/1369118X.2017.1340494
- Shin, D.-H., & Lee, M.-K. (2017). Public value mapping of network neutrality: Public values and net neutrality in Korea. *Telecommunications Policy*, 41(3), 208-224. https://doi.org/10.1016/j.telpol.2016.12.012
- Singapore Statutes. (2019). *Protection from Online Falsehoods and Manipulation Act 2019*. Government of Singapore.
- Sinpeng, A. (2020). Digital media, political authoritarianism, and internet controls in Southeast Asia. *Media, Culture & Society*, 42(1), 25-39. https://doi.org/10.1177/0163443719884052
- South Africa Government. (2024). *National Policy on Data and Cloud*. Communications & Digital Technologies Department, Republic of South Africa.
- Stefanija, A. P., & Pierson, J. (2023). Algorithmic governmentality, digital sovereignty, and agency affordances: Extending the possible fields of action. *Weizenbaum Journal of the Digital Society*, 3(2), 1-30. https://doi.org/10.34669/WI.WJDS/3.2.2
- Stigler Committee. (2019). *Stigler Committee on Digital Platforms: Final Report*. Stigler Center for the Study of the Economy and the State, University of Chicago Booth School of Business.
- Stolton, S., & Makszimov, V. (2020). Orbán to rule by decree with new powers to 'silence critics'. Euractiv, 30 March. www.euractiv.com/section/global-europe/news/orban-to-rule-by-decree-with-new-powers-to-silence-critics
- Tambini, D. (2021). Media Freedom. Polity.
- Tech Hive Advisory Center for Law & Innovation. (2024). *State of AI Regulation in Africa: Trends and Developments Report*. www.techhiveadvisory.africa/report/state-of-ai-regulation-in-africa-trends-and-developments
- Tenove, C. (2020). Protecting democracy from disinformation: Normative threats and policy responses. *The International Journal of Press/Politics*, 25(3), 517-537. https://doi.org/10.1177/1940161220918740
- Turillazzi, A., Taddeo, M., Floridi, L., & Casolari, F. (2023). The Digital Services Act: An analysis of its ethical, legal, and social implications. *Law, Innovation and Technology*, 15(1), 83-106. https://doi.org/10.1080/17579961.2023.2184136
- UK DSIT (Department for Science, Innovation & Technology). (2023). *The Bletchley Declaration by Countries Attending the AI Safety Summit, 1-2 November 2023*. www.gov.uk/government/publications/ai-safety-summit-2023-the-bletchley-declaration/the-bletchley-declaration-by-countries-attending-the-ai-safety-summit-1-2-november-2023
- UN (United Nations). (2023a). *Information Integrity on Digital Platforms*. Our Common Agenda, Policy Brief 8. www.un.org/sites/un2.un.org/files/our-common-agenda-policy-brief-information-integrity-en.pdf
- UN. (2024b). *Pact for the Future, Global Digital Compact, and Declaration on Future Generations*. www.un.org/sites/un2.un.org/files/sotf-pact_for_the_future_adopted.pdf
- UN. (2024c). *Seizing the Opportunities of Safe, Secure and Trustworthy Artificial Intelligence Systems for Sustainable Development*. United Nations General Assembly A/78/L.49.
- UNESCO. (2022a). *Global Standards for Media and Information Literacy Curricula Development Guidelines*. www.unesco.org/sites/default/files/medias/files/2022/02/Global Standards for Media and Information Literacy Curricula Development Guidelines_EN.pdf?hub=750
- UNESCO. (2022c). *Recommendation on the Ethics of Artificial Intelligence*. SHS/BIO/PI/2021/1. https://unesdoc.unesco.org/ark:/48223/pf0000381137
- UNESCO. (2022d). *World Trends in Freedom of Expression and Media Development: Global Report 2021/22*.
- UNESCO. (2023a). *Addressing Hate Speech Through Education: A Guide for Policy Makers*. https://unesdoc.unesco.org/ark:/48223/pf0000384872
- UNESCO. (2023b). *Guidelines for the Governance of Digital Platforms: Safeguarding Freedom of Expression and Access to Information through a Multi-stakeholder Approach*. https://unesdoc.unesco.org/ark:/48223/pf0000387339
- US Congress. (1996a). Health Insurance Portability and Accountability Act (HIPAA). UPub. L. 104-191. https://www.govinfo.gov/content/pkg/PLAW-104publ191/pdf/PLAW-104publ191.pdf
- US Congress. (1996b). *Telecommunications Act of 1996, Section 230 Protection for Private Blocking and Screening of Offensive Material*. Pub. LA. 104-104. https://www.govinfo.gov/app/details/PLAW-104publ104#:~:text=An%20act%20to%20promote%20competition,deployment%20of%20new%20telecommunications%20technologies.
- US Congress. (2013). *Children's Online Privacy Protection Act 1998*. U15 USC 6501-6505, Federal Trade Commission Amendment. https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa
- US District Court. (2024). *US v. Google*. United States District Court for the District of Columbia, Case No. 20-cv-3010 (APM), 5 August. https://www.texasattorneygeneral.gov/sites/default/files/images/press/Google%20Search%20Engine%20Monopoly%20Ruling.pdf

- US Executive Order. (2023). *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. The White House. www.whitehouse.gov/briefing-room/presidential-actions/2023/10/30/executive-order-on-the-safe-secure-and-trustworthy-development-and-use-of-artificial-intelligence
- US State of California. (2018). *California Consumer Privacy Act (CCPA)*. State of California Department of Justice. https://oag.ca.gov/privacy/ccpa
- US-China Commission. (2022). *China's Evolving Data Governance Regime*. US-China Economic and Security Review Commission.
- van Dijck, J. (2020). Seeing the forest for the trees: Visualizing platformization and its governance. *New Media & Society*, 23(9), 2801–2819. https://doi.org/10.1177/1461444820940293
- Vogels, E. A., & Anderson, M. (2019). *Americans and Digital Knowledge*. Pew Research Center, US.
- Voss, W. G., & Pernot-Leplay, E. (2024). China data flows and power in the era of Chinese big tech. *Northwestern Journal of International Law and Business*, 44(1), 1-68. https://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1896&context=njilb
- Waldman, A. E. (2020). Cognitive biases, dark patterns, and the 'privacy paradox'. *Current Opinion in Psychology*, 31, 105-109. https://doi.org/10.1016/j.copsyc.2019.08.025
- Wasserman, H. (2018). *Media, Geopolitics, and Power: A View from the Global South*. University of Illinois Press.
- Wasserman, H. (2020b). The state of South African media: A space to contest democracy. Publizistik, 65(3), 451-465. https://doi.org/10.1007/s11616-020-00594-4
- Wilding, D. (2021). Regulating news and disinformation on digital platforms: Self-regulation or prevarication? *Journal of Telecommunications and the Digital Economy*, 9(2), 11-46. https://doi.org/10.18080/jtde.v9n2.415
- Winseck, D., & Pooley, J. D. (2017). A reply to Faulhaber, Singer, and Urschel's Curious tale of economics and common carriage (net neutrality) at the FCC. *International Journal of Communication*, 11(0), 32. https://ijoc.org/index.php/ijoc/article/view/7543
- Wintour, P. (2024). US leading global alliance to counter foreign government disinformation. *The Guardian*, 26 February. www.theguardian.com/technology/2024/feb/26/us-leading-global-alliance-to-counter-foreign-government-disinformation
- Wu, T. (2018). The Curse of Bigness: Antitrust in the New Gilded Age. Columbia Global Reports.
- Wu, T. (2003). Network neutrality, broadband discrimination. *Journal of Telecommunications and High Technology Law*, 2, 141-179. https://doi.org/10.2139/ssrn.388863
- Yoo, C. S. (2024). Network slicing and net neutrality. *Telecommunications Policy*, 48(2), 1-10. https://doi.org/10.1016/j.telpol.2023.102619
- Zhu, J. (2022). AI ethics with Chinese characteristics? Concerns and preferred solutions in Chinese academia. *AI & Society*, 39(3), 1261-1274. https://doi.org/10.1007/s00146-022-01578-w