



Reignite Multilateralism
via Technology

D3.1 Overview normative construction of technology governance

Call: Reshaping democracies (HORIZON-CL2-2022-DEMOCRACY-01)
Topic: HORIZON-CL2-2022-DEMOCRACY-01
Funding Scheme: HORIZON Research and Innovation Actions
Grant Agreement no: 101094228

Contractual Submission Date: 31-3-2024

Actual Submission Date: 28-3-2024

Responsible partner: 03 - UBREMEN



Grant agreement no.	101094228
Project full title	Reignite Multilateralism via Technology
Deliverable number and title	D3.1 Overview normative construction of technology governance
Type	R: Document, report (excluding the periodic and final reports)
Dissemination level	PI: Public, fully open, e.g. web
Work package number	WP3
Work package leader	UBREMEN
Author(s)	Katerina Yordanova (KUL) Dennis Redeker (UBREMEN) Paul Timmers (KUL) Mariëlle Wijermars (UM) Eoin McNamara (FIIA) Katleen Gabriels (UM) Joren Baillière (KUL)
Keywords	Norms, technology governance, social construction, multilateralism, paradigms, regulation, regulatory landscape analysis, advocacy coalition framework

Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union. Neither the European Union nor the granting authority can be held responsible for them.

Document History

Version	Date	Description
V1	15 March	First draft provided for internal review
V2	26 March	Second draft after internal review
V3	28 March	Version for submission



Background of the REMIT project

The REMIT project aims to “**Reignite Multilateralism via Technology**”. A reigniting that not only reacts to China’s rise as a systemic technology rival or Russia’s resurgence as a technology abuser or the dominance of large U.S.-based digital platforms, but that sets a clear vision for the future — one in which Europe plays a leading role.

Coordinated by Maastricht University, the REMIT project brings together leading European researchers from nine partners from Belgium, Estonia, Finland, Germany, Italy, the Netherlands, Romania and the United Kingdom. The goal is to develop recommendations, clear understanding of the status quo and innovative methodologies that support effective policies to revitalize global democratic structures.

REMIT aims to re-mobilize a transnational collective spirit that addresses global problems through technology, because

1. Technology has strong effect on economic competitiveness
2. Technology is important to national security including threats to democratic principles
3. Technology is crucial to the solutions for global challenges

By focusing on technology and the policy areas that emerge from the REMIT researchers’ expertise, the project provides the needed analysis and the theory building to support the EU. The four technology areas are also instrumental in finding solutions to all important challenges, including climate, digital transitions, the rise of inequalities, ageing and disabilities, migrations, health pandemics, and information disorder. Ultimately, REMIT intends to design policy recommendations that will give a remit to reignite multilateralism via technology.

The detailed objectives of the REMIT project are:

» **Objective 1:** To define the EU’s role in leading the renewal and defence of multilateralism starting with the global governance of technologies in four crucial policy areas (digital, health bio, security and defence, and financial technologies). The lack of comprehensive, multilateral tech regulations represents material national security threats to the EU and its allies by allowing others (especially China) to set the rules for the digital future.

» **Objective 2:** To provide evidence-based advice to reinforce European institutions in the field of technology that work and propose innovative, multilateral-governance constructs for those that do not.

» **Objective 3:** To develop policy recommendations and scenario testing workshops offered to relevant EU administrators, important regional groups, and national officials.

» **Objective 4:** To share knowledge among stakeholders and to communicate policy recommendations. REMIT will recommend policy action for the European Union that further re-conceptualizes multilateralism in the four technology areas.

The REMIT project is carried out from March 2023 until February 2027 and has a total budget of almost €3 million, of which €2.6 million is funded by the EU’s Horizon Europe research and innovation program and €370k is provided by the UK government through the UK Research and Innovation fund (UKRI). The project is being carried out by internationally recognized researchers from Maastricht University, Universitatea Babes Bolyai, Universitaet Bremen, Katholieke Universiteit Leuven, Luiss Libera Universita Internazionale Degli Studi Sociali Guido Carli, Erasmus University Rotterdam, the Finnish Institute for International Affairs and the University of Tartu. In addition, the European Cyber Conflict Research Initiative (ECCRI) joins the consortium as an associate partner, receiving funding from UKRI.



Table of Contents

Executive Summary	1
1. Introduction	2
2. Framework: The Normative Construction of Technology Governance	3
3. Initial Overview of Technology Governance Practices: Regulatory Landscape Analysis...	6
3.1 Governance, legislation and regulation from a legal perspective.....	6
3.2 Technology regulation and technology governance	8
3.3 Key features and continuous evolution of legislation and regulation	10
3.4. Mapping the tools for regulation of key technologies.....	14
4. Conclusion.....	16
5. Next steps	19
References	21
Annex	26

List of Abbreviations and Definitions

Abbreviation	Definition
ACF	Advocacy Coalition Framework
AI	Artificial Intelligence
AV	Autonomous Vehicles
EU	European Union
GDC	Global Digital Compact
ICANN	Internet Corporation for Assigned Names and Numbers
IETF	Internet Engineering Task Force
IGF	United Nations Internet Governance Forum
IoT	Internet of Things
ITU	International Telecommunication Union
NGO	Non-Governmental Organization
REMIT	Reignite Multilateralism via Technology
TFEU	Treaty on the Functioning of the European Union
UN	United Nations
WSIS	World Summit on the Information Society



Executive Summary

This deliverable provides an overview on work conducted in Work Package 3 during M1-M13 of the REMIT project. A sizable share of the data collection to occur as part of Task 3.1 takes place during the first two years of the project. In subsequent deliverables, Tasks 3.2-3.4. will be successively covered, moving from data collection and understanding of the regulatory landscape to analyzing policy sub-systems, identifying barriers and opportunities to improve multilateral governance, and developing (from this) policy recommendations for European actors and beyond. The current deliverable provides an overview of findings and update on work in progress. Specifically, the deliverable reports on WP 3's conceptual framework by **defining how we approach the “normative construction of technology governance”**, while also reporting on a **regulatory landscape analysis** conducted. The latter represents an important foundation for our ongoing research activities.

Our framework definition for the ongoing research into the normative construction of technology governance can be summarized as follows:

- We take **norms as a social construct, created intersubjectively between different social groups within political actors and between them** (Björkdahl, 2002). We understand that norms, held by the public or specific stakeholders (e.g., policymakers, companies) are an important foundation to build technology governance institutions for different fields of technology governance. Norms can relate to the specific substantive outcomes of technology governance, or to the governance principles entailed (e.g., transparency or participatory consultations).
- **Technology governance is a broad field that includes civil and defense technologies.** For defense technologies specifically, multilateralism is usually referred to a normative aim of the European Union and other actors, indicating a **willingness to cooperate among states and a departure from unilateralism**. Going beyond ad-hoc cooperation, this ideally includes setting up of institutions to develop multilateralism and make it sustainable. With respect to civilian technologies, multilateral approaches likewise represent a way of being inclusive toward many *countries* when it comes to their governance or “coordination of coordination” (Hofmann et al., 2017: 1417) through multilateralism. However, a widely held norm in fields such as Internet and artificial intelligence (AI) governance is that of **multistakeholder approaches**, which include a wide variety of stakeholders such as states, companies, technical experts, academics, civil society, and technology end users into the governance process.

Taking this framework as a starting point for the research on the normative construction of technology governance, we conduct an initial survey of the regulatory landscape i.e., the legal-normative background against which the global governance of technology plays out. **Core findings of the regulatory landscape analysis** can be summarized as follows:

- While **hard law** remains the predominant choice for regulators and legislators, its overall share is less than the combined shares of soft law, standards, and the various forms of *anticipatory regulation* in a broad sense.
- The significant share of **soft law** signifies the need for more agile forms of regulation when dealing with technologies, especially internationally. Furthermore, it allows the adoption of rules (even if non-binding) in a context of a fragmented international community where consensus is hard to be reached.
- The overall large share of **alternative forms of regulation** shows we need a different approach to regulation of dynamic and highly impactful technologies. It also indicated the need for a broader participation in the regulatory process from companies, civil society representatives and technology experts. Finally, the data suggests that while regulation is certainly high on the agenda of states and international organizations, facilitating and supporting innovation is also



taken into account, to the point that experimentation and regulation are considered to not be mutually exclusive anymore, but rather mutually beneficial.

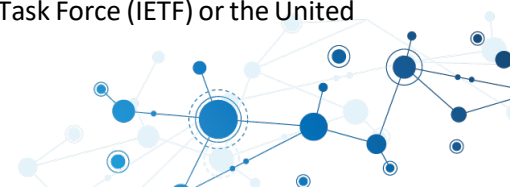
We also suggest how the **Advocacy Coalition Framework (ACF)** can be used to better understand and improve technology *regulation*. We close this deliverable by highlighting ongoing empirical research that approaches critical fields of normative developments in the field of technology governance, spanning a number of fields such as AI, the Internet, blockchain and cybersecurity, and a number of different levels of analysis, including populations in potential partner countries and stakeholders in Brussels, the Nordic and Baltic States, and those participating in global technology fora and debates. We point out how we aim to utilize the ACF as a common frame for REMIT.

1. Introduction

In this first deliverable of Work Package 3 of the project “Reignite Multilateralism via Technology” (REMIT), we outline our conceptual framework of the “normative construction of technology governance”. This deliverable provides an overview on work conducted in Work Package 3 during the first thirteen months of the project. A sizable share of the data collection to occur as part of Task 3.1 takes place during the first two years of the project. **Defining early on how we define our collaborative work enables us to work together** and allows readers, who follow REMIT’s work, to have a clearer picture of the work conducted as part of the work package. In addition to this definitional work, in this deliverable we present a first mapping exercise, a **regulatory landscape analysis**, in order to provide a strong cross-cutting groundwork in terms of socio-legal knowledge for later analyses, which focuses on specific fora, spaces, actors, technologies and norms. Lastly, we present the avenues to study further this normative construction of technology governance empirically (the remainder of data collection entailed in Task 3.1).

The work we conduct as a work package is based on the **assumption that we need to understand how global technology governance is normatively constituted (or constructed), in order to better understand how European values, specifically an open and participatory, transparent, rights-based and effective governance fare in this global concert of empirical and legal norms**. We also interrogate the values held by EU policy makers to better understand the possible strategies and advocacy coalitions in global technology governance, across a set of technologies. **Without a good understanding of the socio-legal and empirical normative environment, no action toward extending the advocacy coalitions around these values and in different technology domains can be achieved**. Furthermore, policy recommendations that suggest multilateral paths forward for the governance of the various technologies addressed by REMIT require all three - an understanding of the norms held by actors, knowledge of the modes of governance - often specific to the domain of *technology* governance, and the resulting opportunities for coalition building.

When classifying the values applied to cross-border technology governance, in many cases **a meta value of multilateralism is presupposed**. After all, unilateralism does not concern itself very much with the effort of jointly governing any policy field. Generally, multilateralism refers to the “practice of co-ordinating national policies in groups of three or more states, through ad hoc arrangements of by means of institutions” (Keohane, 1989: 731), which has a strong state-centric vision when scholars started to develop new IR theories about it (Keohane, 1989), but which has ever since been infused with notions of broader society participation (Hampson & Heinbecker, 2011). Civil society participation and engagement with global governance organizations based on inter-state interactions can raise these institutions’ accountability to the global public and their mission (Scholte, 2004). Particularly in the field of **digital technology governance, a more participatory multistakeholder model of governance has been established** (Hofmann, 2016). Organizations such as the private-entity Internet Corporation of Assigned Names and Numbers (ICANN), the informal Internet Engineering Task Force (IETF) or the United



Nations (UN) Internet Governance Forum (IGF) make up an important part of the regime complex of “global cyber activities” (Nye, 2010). The institutionalization of the multistakeholder model in global digital governance goes at least back to the 2003-2005 World Summit of the Information Society (WSIS), which saw sovereigntist ideas of more control over Internet infrastructure and neoliberal wishes to fend off strong regulation of the technologies, companies and content (Mueller, 2010; Radu, 2019). In these fora, civil society and others have engaged in an effective “politics of representation” by being at the table (Mueller, 2010). Multistakeholder governance has also been practiced across other fields such as part of the worldwide slot guidelines in aviation (Gasser et al., 2015; Schebesta & Sartor, 2015) and global climate governance (Frank, 2021), but it is nowhere as institutionalized as in the field of Internet and digital governance. Importantly, through the field of cybersecurity norms, multistakeholder approaches have recently found their way into security debates at the UN through an Open-Ended Working Group established in 2018 (Trachtmann, 2023).¹

Multilateralism and multistakeholderism both fall on a continuum with arguably different degrees of openness to non-state actors and authority of state actors, both within the scope of current EU values and strategies, depending on the specific technology domain. As we do see with the large range of technologies REMIT examines, some technology domains - such as defense technology - tend to be less affected by the opening of governance to additional actors. When studying what can “Reignite Multilateralism via Technology”, then we expressly do not stop at the inter-state vision of multilateralism but understand multistakeholderism to be an important, and normatively relevant, extension (or development from) multilateralism. In addition, compared to other analytical approaches within REMIT, **Work Package 3 tends to naturally take a global and comparative view (on matters of norms and their construction in technology governance) rather than focus on a specific national and regional political arena** (Work Package 4) or specific strategic technologies (Work Package 5). **Applying the advocacy coalition framework (ACF) in this research thus represents a challenge, which requires, at times, methodological innovation.** This is particularly true when working with no-so-well tested data types such as population level comparative surveys and advocacy coalitions, whose recorded statements span several decades and the entire planet - amid swiftly-evolving technologies. At other times, to be able to gain insights from applying the ACF, we venture into more traditional settings such as in the context of epistemic and governance communities concerned with technology governance.

In this deliverable, we introduce our theoretical model of “normative construction of technology governance”, conduct an initial survey, analyze the regulatory landscape, and discuss appropriate methods for empirical investigation of the relations presented. The deliverable’s findings provide a robust, interdisciplinary foundation for subsequent research for the Work Package and across REMIT.

2. Framework: The Normative Construction of Technology Governance

In this section, we present a framework and our shared understanding of the normative construction of technology governance. We organize this framework’s presentation by defining the co-constituent concepts.

The term **„normative“** indicates our primary interest lies in understanding the use of norms in the shaping of governance. **Norms are a social construct, created intersubjectively between different social groups within political actors and between them** (Björkdahl, 2002). We use the term norms to

¹ More recently, scholars suggested that polycentric governance ought to be considered as a new mode of governance of (digital) technologies, further complicating the demands on multilateralism (Aguerre et al., 2024; Gasser & Almeida, 2022).



capture the spectrum from **collective and formalized norms to informal understandings of how an issue ‘should be handled’** that are based on values and assumptions. The issue to be handled, in our case, is „**technology governance**“. Our aim is to examine how processes of norm formation and norm contestation shape („**construct**“) the governance of technology.² Formalized norms are for instance entailed in laws and agreements. Public declarations by governance stakeholders, including public and private actors are also relatively formalized. These documents usually make explicit the normative principles or normative legal basis. In contrast, informal understandings are commonly held views, for instance as held by the public or a functional elite such as policymakers. If formalized or not, norms and understandings about them can be at a high level, for instance respect of fundamental rights. They can also be at a more specific level, such as in the form of technical standards, such as an ISO standard for privacy-by-design. We argue that **in the context of technology governance, both social and technical norms need to be included in a broader analysis of its normative construction.**

While the emphasis of the research that will be conducted within Work Package 3 lies on **examining the beliefs held and/or expressed by various actor groups and their interactions** (approached through the perspective of the ACF), it is **essential to first take stock of the (inter)national legal frameworks within which these actors formulate** their normative positions and seek to push for normative change. The outcome of this step – the regulatory landscape analysis - is presented in this document. From a legal perspective, the notion of **normative is closely associated with the establishment, application, and interpretation of laws and regulations.** This concept revolves around a structured system of rules developed, interpreted, and enforced by governmental bodies and institutions. Legal norms carry the weight of the state's authority, ensuring compliance through formal sanctions such as fines or imprisonment. The objective of the legal normative framework is to establish societal order, safeguard rights, and address disputes, functioning within a codified system where laws are clearly articulated and their enforcement is determined through judicial processes. **This approach to normativity emphasises the formal, systematic, and uniform application of rules across a legal jurisdiction, underpinning the governance structure of society.**

Unlike legal norms, social norms are not enforced by formal sanctions but are upheld through social approval, disapproval, and informal sanctions, reflecting their flexibility and variability across different cultural contexts. The key distinction lies in the enforcement mechanisms and the source of normative authority: **legal norms rely on institutional mechanisms with a clear source of authority, whereas social norms are enforced through collective beliefs and practices without the need for formal legal backing.** This delineation between the legal and social science perspectives on normativity highlights the varied ways in which societies regulate behaviour and maintain order, each aiming to guide human behavior through distinct means and objectives. This distinction, however, becomes less pronounced with the introduction of soft law and anticipatory regulation in the technology sector, where flexible and adaptive governance is essential. These approaches merge the enforceability of legal standards with the adaptability of social expectations, addressing the dynamic challenges of disruptive innovations. **In turn, the normative beliefs held by various stakeholders shape the regulatory framework, including hard law.**

A central assumption we make for our framework is that “collective” norms, i.e. beliefs widely shared by a society, interact with other social processes, including political economy and geopolitics. Thus, we take as an important perspective the notion of „**paradigms**“ in **global technology governance that more or less align with the ideologies of large geopolitical players.** These can coalesce around normative paradigms such as the **market-led, state-led, and value-led paradigms** in the digital domain of the

² There is no single definition of what a norm is. For our relationship in terms of values and assumption to technology, see for instance Heidegger (1977).



United States, China and the EU (Bradford, 2023). The US has preferred a lighter-regulated market-orientated model, aiming to keep its industry's lead in global technological modernization. The EU has preferred a more regulatory stringent 'rights-based' model that obligates companies to adhere more to the data rights of citizens. China has favored a model where data can serve its authoritarian capitalist development trajectory, keeping the authoritarian interests of the Chinese Communist Party closely in mind (Bradford, 2023). We call these the **"three Cs": a Californian approach found in the US (emanating from Silicon valley), a constitutional European, particularly EU, approach and a Chinese or closed approach to technology governance.** These three types extend similar typologies of Internet governance models to a larger field of technology governance, e.g., the **constitutional, neoliberal and sovereigntist ideal types** described by Santaniello (2021). Our research will thoroughly test these assumptions, keeping in mind that these are ideal typical approximations.

With technology governance norms in unstable flux, it **remains uncertain which dimensions from these three models will eventually diffuse most to influence broader global norms.** This is partially a clash of 'soft powers'. The US market-orientated model might seem attractive to those beyond the West seeking to expand technological output, even though some states in the Global South appreciate EU regulations seeking to instill stronger respect for data privacy in multinational firms. This spares these governments resources for having to do so themselves. Nevertheless, as strategic competition to dominate technological innovation continues, this is also an area where Western influence is at risk of being reduced. Alongside Chinese investment in economic development in Africa, Asia and Latin America, Beijing has also maintained an effort to widely promote the technology governance norms that it prefers. **After decades of unsuccessful adaptation to Western political and economic programmes in the Global South, chiefly the neoliberal 'Washington consensus', Chinese alternatives are attractive to many authoritarian governments but may also find approval among the general public in countries around the globe.** The promise to protect regime-standing while seeming to offer a stable development model to enhance prosperity.

By „technology“ we mean the application of science, resulting in artifacts and usually constructed by humans. Although a wide range of technologies is considered by REMIT, in this deliverable we focus on our research on the regulatory landscape and norms relating to digital and financial technologies including artificial intelligence (AI), Distributed Ledger Technology (Blockchain), Internet of Things (IoT), Cloud Computing, and 5G/6G. This selection covers highly relevant technologies, illustrates a range of regulatory approaches and norms regarding technology governance, and allows to identify dependencies such as on the specifics of technology, and on political and historical contexts. Ongoing research of members of the work package will add the technologies analyzed, including research related to the governance of defense technologies and Internet governance.

We use the term „construction“ to highlight how technology governance should be understood as a **set of continuously developing processes.** In understanding these processes, we should identify who has agency (the **actors and stakeholders** seeking to shape norms related to technology governance), the referent object or objects (**technology**) and the relevant **existing and emerging normative frameworks.** The **ACF provides the toolkit to analyze the relationship between these three components:** how coalitions of actors seek to influence processes of norm formulation, institutionalization, implementation and contestation as they apply to the governance of technology. The extensive body of literature on norm contestation in International Relations, building upon the classic conceptualisation of international norm dynamics by Finnemore and Sikkink (1998), demonstrates the **power of established norms in shaping (state) behavior, while simultaneously stressing the role of so-called norm entrepreneurs who seek to contest existing norms and/or establish new ones.**



3. Initial Overview of Technology Governance Practices: Regulatory Landscape Analysis

Exploring **hard law is an essential first step in understanding the normative construction of technology governance and grasping the multidimensional nature of the notion of *normative***. Hard law provides the foundational legal framework that defines clear boundaries, rights, and obligations within which individuals, entities and institutions operate. It establishes a baseline of enforceable rules and standards that ensure order, protect rights, and resolve disputes in society. **This formal legal structure is crucial for understanding how normative concepts are applied and enforced at the institutional level, offering a clear contrast to the more fluid and interpretative norms studied within social sciences.**

Soft law, technical standards, and anticipatory regulation serve as a bridge between the rigid frameworks of hard law and the flexible, evolving norms of social science. These instruments embody a middle ground, incorporating the enforceability and structured approach of legal norms with the adaptability and consensus-driven nature of social norms. **Soft law, for instance, while not legally binding in the traditional sense, influences behaviour through guidelines and standards recognised by the international community, offering a form of governance that is responsive to the rapid changes in technology.** Similarly, technical standards and anticipatory regulation reflect collaborative efforts to preemptively address the challenges posed by innovation, emphasising ethical considerations, stakeholder engagement, and forward-looking policies. **This blend of formal and informal regulatory mechanisms illustrates the complex interplay between legal requirements and societal expectations,** highlighting why an exploration of these middle-ground approaches is vital for comprehensively understanding the multifaceted nature of normativity in technology governance and beyond.

Since norms are usually embedded in written sources of law such as legal acts, codexes, ordinances, etc., a regulatory landscape analysis is the first necessary step in comprehending the status quo of the technology governance and identifying the relevant stakeholders. Additionally, soft law instruments, tools and frameworks, as well as technical standards, might incorporate equally influential norms, without their binding power being necessarily based on the nature of the instrument they are contained in. To further examine this tendency, in the next section, **we differentiate between governance, legislation, and regulation when examining the regulatory landscape of digital technology regulation.** We do so to create a foundation for later analyses within REMIT that concern themselves with general or specific norms across the above-mentioned set of technologies.

3.1 Governance, legislation and regulation from a legal perspective

Governance, legislation, and regulation are distinct concepts in the field of law, each serving a unique role in the legal system (Kosti et al, 2019; Drahos et al, 2017), taking into account the differences which reflect the distinctive characteristics of various legal systems. (Black et al, 2005). **Governance** refers to the **overall structure, decision-making processes, and management of an organization, institution, or government.** It encompasses the establishment of rules, policies, and procedures that guide the behavior of individuals and entities within that organization (Brousseau et al, 2012). Governance sets the framework for how laws and regulations are created and enforced. It often involves the appointment of leaders, boards, or authorities responsible for making key decisions and ensuring compliance with established norms. While governance plays a crucial role in shaping legal frameworks, it is not inherently a source of legal rules or requirements itself (Morth, 2004).

Legislation, on the other hand, refers specifically to *the process of making laws or statutes by a legislative body*, such as a parliament or congress (Rubin, 1989; Guastini, 2007). Legislation is a formal and comprehensive means of creating **binding rules and obligations** that apply to society as a whole. It



involves the **drafting, debating, and passing of bills**, which then become law once they are approved by the legislative body and, in some cases, signed by the executive branch (Aldisert, 1982). Legislation can cover a wide range of issues, from criminal laws to tax codes, and it serves as the primary source of written laws in many legal systems. It is important to note that legislation in the context of a national state has some differences compared to 'legislation' in international law. First, in the latter case, we usually talk about **sources of international law**, rather than legislation. While the term 'sources of international law' does not have a concrete unilateral understanding (Degan, 1998), it is typically employed in a formal sense, indicating "methods and procedures by which international law is created" (Briggs, 1952). This is necessary due to the nature of international law, its rules emerging via law-creating (i.e. treaties) as well as law-determining (i.e. customs) processes (Schwarzenberger, 1986). However, in the case of the European Union (EU), the language of the Treaty of the Functioning of the European Union (TFEU) clearly refers to 'legal acts', which are further defined in Art. 288 TFEU, as sources of the legal rules, necessary for the EU to exercise its competences. This, combined with the legislative procedures, stipulated in Art. 289 TFEU, leads us to the conclusion that in the specific instance of EU-made rules, we can talk about **legislation, rather than sources of international law**, despite the international nature of the Union (Hofmann, 2009).

The third concept, **Regulation³**, is **understood in law as a subsequent step in the law-application process, where administrative agencies or bodies are tasked with implementing and enforcing the laws** passed by the legislature (Berger, 1967-1968). Regulations are the **detailed rules, guidelines, and procedures** created by these agencies to clarify how the broader laws should be applied in specific situations (Prosser, 2010). **They provide the necessary specificity to ensure compliance with legislation.** Regulations can cover a myriad of fields, such as environmental protection, financial services, or workplace safety. While **regulations derive their authority from legislation**, they are developed and enforced independently by administrative bodies, making them a crucial bridge between the broad principles of legislation and their practical application in society (Aranson et al, 1982-1983; Page, 2001). The **legal interpretation of the notion of regulation is considered fairly limited**, especially when taking into account its cross-disciplinary importance. Therefore, it is important to recognise that other definitions might be more impactful and better acknowledged in general. A typical example is the definition given by Selznick, according to whom regulation is "sustained and focused control exercised by a public agency over activities that are valued by the community." (Selznick, 1985) By contrast, other authors consider that definition of regulation is built on three main understandings, namely:

1. regulation as "the promulgation of an authoritative set of rules, accompanied by some mechanism [...] for monitoring and promoting compliance with these rules;"
 2. regulation as "all the efforts of state agencies to steer the economy;"
 3. regulation as "all mechanisms of social control – including unintentional and non-state processes."
- (Baldwin et al, 1998; Baldwin et al, 2012; Cf. Koop et al, 2017)

In summary, from a legal point of view, governance establishes the organizational structure and decision-making processes, legislation is the formal process of creating written laws, and regulation involves the development and enforcement of specific rules and procedures to implement those laws. Together, these concepts work in tandem to create and maintain a functioning legal system, by creating interdependency, as shown in *Figure 1*.

³ By regulation here we refer to a type of acts, adopted by governments, agencies and other independent bodies, which reflect delegated legislative powers, and which have subsidiary roles regarding the legislative acts, as well as the activities related to their adoption and enforcement. It is to be distinguished from Regulation as binding legislative acts on EU level, which are directly applicable in member states.



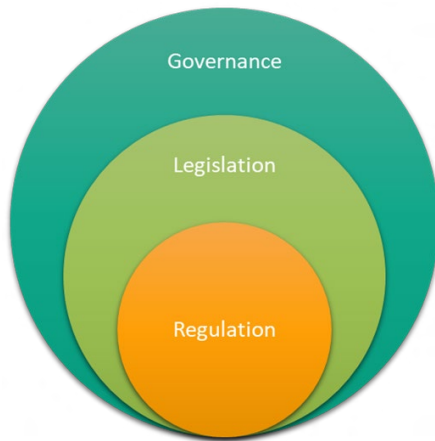


Figure 1: Distinction between governance, legislation and regulation

3.2 Technology regulation and technology governance

This distinction between legal and non-legal definitions of governance, legislation, and regulation appears to be paramount when examining the field of technology governance and the emerging technology regulation in a broad sense. While the two concepts are closely related, there are some important distinctions. **Technology regulation** refers to the process of setting rules and standards for the development, use, and operation of technology. This can be **done through laws, regulations, or other forms of government intervention** (Brownsword, 2022; Zhou et al, 2013; Moses, 2013). The primary goal of technology regulation is to protect public safety, security, and welfare (Hodson, 2021). For example, regulations may be in place to ensure that software is secure, that data is protected, and that companies do not engage in unfair or deceptive practices. **Technology governance is a broader concept** that encompasses all of the ways in which society manages and directs the development and use of technology. This **includes technology regulation, but it also extends to other forms of governance, such as industry self-regulation, international cooperation, and public education** (Sofyani et al, 2020; Bianchi et al, 2021). The goal of technology governance is often claimed to be to ensure that technology is used in a responsible and ethical manner that benefits society as a whole (Hennen et al, 2023). There are different understandings of what constitutes these “public values” around the world.

Feature	Technology regulation	Technology governance
Scope	Narrow	Broad
Focus	Setting rules and standards	Coordinating, managing and directing the development and use of technology
Primary goal	Protecting public safety, security, and welfare	Ensuring that technology is used in a responsible and ethical manner that benefits society as a whole
Leading Stakeholders	Government agencies	Governments, private companies, civil society organizations, academics, technical experts, individuals
Tools	Laws, regulations, standards, self-regulation, international cooperation, public education – <i>enforced by governments</i>	Laws, regulations, standards, self-regulation, international cooperation, public education – <i>implemented by a variety of actors, including governments, industry groups, civil society organizations, and individuals.</i>

Table 1: Features of technology governance and technology regulation



Comparing technology regulation and technology governance through features such as leading stakeholders, focus, or primary goal (*see Table 1*), allows us to better understand the interrelationships between the two modes of rule-setting and enforcement (*Figure 2*).



Figure 2: Distinction between technology governance and technology regulation

Technology regulation and technology governance influence governance, legislation, and regulation in several ways. For instance, regulatory frameworks for technology are often established through legislation, and the implementation and enforcement of these frameworks, through the respective regulation, may involve various governmental agencies, usually acting as regulators. Similarly, industry self-regulation can be guided by government-issued guidelines or principles.

Technology governance also influences the development of laws and regulations. As technology evolves, it often raises new legal and ethical questions. These questions can then inform the development of new legislation and regulations, including through the dynamic process of anticipatory regulation (Armstrong et al, 2019). However, despite the close interdependence between on one hand governance, legislation, and regulation and on other, technology governance and technology regulation, their respective scopes do not merge completely (*see Figure 3*).



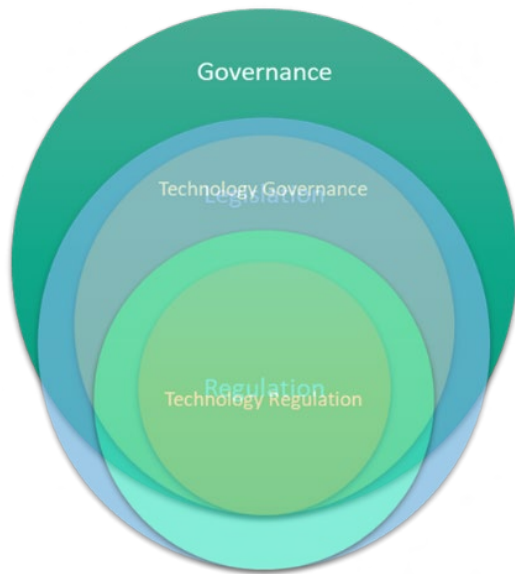


Figure 3: Intersection between technology governance and technology regulation

Therefore, when talking about technology governance and technology regulation through the tools of legislation and regulation in the legal sense, it is essential to take into consideration the characteristics and limitations of these approaches. This would allow stakeholders, including but not limited to policy makers, to adapt their methods, especially when dealing with disruptive technologies (Walsh et al, 2000).

3.3 Key features and continuous evolution of legislation and regulation

As we have already established, in democratic legal traditions, the legislation is the formal creation of laws by governments to enforce rules in society.⁴ Hence, it must be passed by a **democratically elected body with the power to create laws** (Sitaraman, 2015; Sweet, 2007). Furthermore, legislation should be designed to protect the public interest and promote social welfare and backed by legal mechanisms for enforcement (Kingsbury, 2010). Finally, in order to **ensure legal certainty**, as a fundamental element of the rule of law, legislation should be **clear and predictable** to safeguard the fair and consistent application of the law (Liebwald, 2015; Ranchordás, 2021).

Using legislation for technology regulation poses a few challenges. First, considering the economic and societal importance of the field, the political process can influence the content and implementation of legislation (Tarrant et al, 2022). Second, adopting legislation could be **inflexible, reactive, and slow** to adapt to rapidly changing technological environments (Ranchordás et al, 2019; Hansson, 2020; Ranchordás, 2021). Finally, **enforcing legislation across borders** can be challenging in a globalized economy (Arroyo et al, 2023; Brännström 2023). Legislators can adopt certain strategies, aiming to overcome these limitations, such as:

1) **Multi-stakeholder Collaboration**: Engaging with a wide range of stakeholders, including businesses, technical experts, civil society, and individuals, in the legislative process can lead to more informed and effective laws (Weber, 2011).

⁴ Legislation could also be defined in a border context as the collection of laws and statutes that are enacted by a legislative body within a governmental framework, which also covers countries which are not deemed as following the democratic legal tradition. Nevertheless, the challenges related to the slow, maladaptive nature of the legislation remain the same.



- 2) **Regular Review and Updates:** Legislators should regularly review and update laws as technology evolves to ensure their continued relevance, without compromising legal certainty.
- 3) **International Cooperation:** Cooperating with other governments to develop and enforce harmonized laws can improve the effectiveness of regulation in a globalized market.

Nevertheless, the effect of these strategies would remain limited, compared to the fast-paced development of technology. Similarly, regulation relevant to the technology domain should possess characteristics such as **clarity**, facilitating the understanding for businesses and individuals regarding the rules they are expected to comply with (Cacciaguidi-Fahy et al, 2016). Regulation should also cover a **broad range of technological activities** to address potential risks, in addition to having **clear enforcement mechanisms** to ensure compliance (Wagner et al, 2020). In principle, regulation should be flexible enough to adapt to changing technological landscapes, however, in the case of disruptive technologies this is rarely the case (Ranchordás, 2021). Nonetheless, regulation remains easier to change and more flexible vis-à-vis the tools the regulator has at its disposal with respect to enforcing the regulation in question.

Despite its benefits, regulation also has limitations such as its **complexity**, stemming from the complicated nature of technologies such as artificial intelligence, quantum computing, cybersecurity, etc. (Thomsen, 2011). Additionally, the regulatory process can be **slow**, which can lead to gaps in regulation as technology evolves in the absence of other mechanisms such as adaptive or anticipatory regulation (Ranchordás, 2021; Zwitter et al, 2020). These two challenges also lead to issues related to the **high compliance cost** for businesses and **lack of legal interoperability**, causing conflict with other areas of regulation or with legal principles (Ringe et al, 2020; Thorogood, 2020). To overcome these limitations, regulators can adopt strategies such as:

- 1) **Technology-Neutral Approach:** Regulations should be based on principles rather than specific technologies to ensure long-term applicability (Bertolini, 2022; Shadikhodjaev, 2021).
- 2) **Risk-Based Approach:** Regulations should prioritize regulating the most risky aspects of technology (Buckley et al, 2020; De Gregorio et al, 2022).
- 3) **Regulatory Sandboxes:** Regulators can create experimental environments to test new technologies and regulations in a controlled setting (Buckley et al, 2020; Ranchordás, 2021; Zwitter et al, 2020; Johnson, 2023).
- 4) **Public Engagement:** Regulators should engage with stakeholders, including businesses, civil society, and individuals, to develop and implement effective regulations (OECD, 2023; Epstein et al, 2014).

These mitigation strategies could be adopted by the regulators either **separately or in combination** with one another. However, this necessarily leads to evolution in the traditional understanding of regulation. As demonstrated above, a big contributing factor to this evolution is the rapid development of technologies. While we can certainly pinpoint some tendencies of this evolution emerging earlier (Wasserman, 2014; Ranchordás, 2014), there is a common understanding that the rise of FinTech and the Financial crisis from 2008 accelerated this evolution immensely (Zwitter et al, 2020, Ranchordás, 2021; Zetzsche 2017).⁵

The characteristics of this evolution and its direction are probably best described by Armstrong et al. (2017, 2019) who recognise that challenges presented by emerging technologies result in the development of various ‘**anticipatory regulation**’ approaches such as regulatory sandboxes, testbeds,

⁵ This temporal specification of technology regulation was the reason why we chose to include FinTech regulation in the conducted mapping exercise. This is without prejudice to any substance exploration of the topic which would not be feasible at this point.



policy labs, etc. These approaches could be classified under the framework of three modes of regulation. All of them share certain common features (**proactiveness, forward-facing, flexibility, iteration and increased inclusiveness**) which differentiate them from the more traditional and reactive forms of regulation and technology regulation in particular. The three modes are:

1) **Advisory regulation:** The **advisory approach** to regulation aims at helping new products and services **to adhere to already existing regulation**. The outcome is ultimately **altering the products/services**. The novelty lies in the **simplification of the interactions** between businesses introducing new products or services (the innovators) and the regulatory bodies. These approaches involve granting innovators **temporary flexibility within existing regulations to test their ideas**. **Regulators actively participate in the development and testing of innovations, gaining insights into potential disruptions and how they align with current regulations**. The goal is to minimize regulatory hurdles and attract new businesses without extensive rule changes. Examples of advisory approaches include *financial sandboxes like Dubai's Innovation Testing License* and open data initiatives, such as the *Open Up Challenge* and *Open Data Challenge*, which promote open innovation and may lead to future regulatory adjustments, even if it's not the primary goal (Armstrong et al, 2017; Armstrong et al, 2019).

2) **Adaptive regulation:** Adaptive approaches are used by regulators to **facilitate the development of new products or services, even if existing regulations need to be adjusted**. The goal is to **assess the value** of these innovations in a controlled environment and then modify either the innovation itself or the existing regulations to bring the product or service to market. Similar to advisory approaches, participants receive **guidance and temporary regulatory relaxations**. However, unlike advisory approaches, **if significant regulatory barriers are identified, permanent changes to existing regulations may be considered on a case-by-case basis**. This process involves **consultation and engagement with industry stakeholders**. It is important to note that adapting regulations can be challenging, especially if the existing legislation which is the primary law, is inflexible. Examples of adaptive approaches include *financial sandboxes like the FCA's Innovate project*, which aims to reduce existing regulatory barriers and consider changes to legislation while collaborating with the industry to ensure consumer protection (Armstrong et al, 2017; Armstrong et al, 2019).

3) **Anticipatory regulation:** Anticipatory regulatory approaches aim to **proactively understand the potential impacts of emerging technologies on society and the economy, even before these technologies are fully developed**. This involves dealing with uncertainty and limited evidence, with **regulators actively engaging in research to build an evidence base**. Identifying future threats, risks, and opportunities is a key part of this approach, with some regulators already performing such horizon scanning functions. Additionally, anticipatory approaches emphasize **broad inclusion and engagement of stakeholders**, such as regulators, local authorities, research institutions, and technology companies, who collaborate to gather data and insights. For example, *Singapore's Autonomous Vehicle Initiative* involved cross-industry cooperation to oversee the integration of autonomous vehicles and establish a collaborative research center for testing and improving AV technology (Armstrong et al, 2017; Armstrong et al, 2019).

Ultimately, the three approaches could be compared based on their goals, the desired primary outcome and the participants or stakeholders. Table 2 provides a schematic view of those criteria for each of the approaches. Furthermore, since regulation does not exist in a vacuum, it is not only possible but highly desirable to combine advisory, adaptive, and anticipatory regulation approaches. The mixed utilization of their various tools, especially in the area of disruptive technologies such as AI, 5G/6G, IoT, etc., contributes not only to nurturing and promotion of innovation, but also to development of strategic autonomy and fostering of digital sovereignty (Serentschy et al, 2023).



	Advisory regulation	Adaptive regulation	Anticipatory regulation
Goal	Facilitate compliance of new products/services with the existing regulation	Supporting innovation through, where necessary, adaptation of the existing regulatory framework	Recurring development of regulation and standards around the emerging field
Outcome	Change in the product/service	Change in product/service/regulation/legislation	Better understanding of the impact of technologies on society and economy/ regulatory planning and vision
Stakeholders	Regulator, innovators and businesses	Regulators/legislator, innovators, businesses, and industry stakeholders	Regulators, businesses, cross-industry, civil society, local authorities, cities, citizens, early adopters, NGOs

Table 2. Advisory, adaptive, and anticipatory regulation

With respect to how this evolution in traditional regulation is reflected in the various tools used for regulation, the answer is linked to the tendency of the merger between hard law and soft law⁶ in the technology field. An illustrative example of this is the status of the recommendations of the **International Telecommunication Union (ITU)**. According to Art 6(1) of its Constitution, member states are bound **only** by the provisions of the Constitution, the Convention, and the Administrative Regulations and only as long as those provisions engage international services or are capable of causing harmful interference to radio services of other countries.

However, ITU, as an organization, adopts instruments in different sectors. **Recommendations, resolutions, decisions, and reports** all of which are **non-binding** are based on **thorough studies of the technical aspects** that need standardization and regulation. The essential point here is that even though states do not **have any legal obligation to comply** with those instruments **they do** but not due to some sanction or mechanism of legal enforcement. The reason is that the whole international telecommunications system that is enshrined in ITU “essentially depends upon states recognizing the effects of failure [...] to behave in a responsible manner” (Lyll, 1995). Effects, which are described by Jens Hinricher as being “**lethal**” to many of the governments (Hinricher, 2004). This could be explained by the fact that such instruments contain recommendations adopted not by politicians but by the leading **experts in the telecommunications field**. Not following them leads to a lack of standardization. The **lack of standardization** means that the users of telecommunications and radio **services would not be able to use them at an international level** or at least not universally.

For instance, Recommendation ITU-T E.164 on the international public numbering plan establishes that plan-conforming numbers shall be limited to a maximum of 15 digits and how a number is formed.

⁶ In a legal sense what we understand as ‘**hard law**’ is the legally binding obligations that are precise, and that delegate authority for interpreting and implementing the law. Hard laws are enforceable through legal systems and typically take the form of formal written statutes, regulations, and legal provisions. They have clear implications for those subject to the law, who may face sanctions or legal action if they fail to comply. Examples include treaties, international agreements, and domestic legislation. In comparison by ‘**soft law**’ we describe quasi-legal instruments that do not have legally binding force. Soft law typically includes guidelines, declarations, policy statements, codes of conduct, and recommended practices. The purpose of soft law is to influence and shape behavior without the strict enforcement mechanisms of hard law. It is often used in international contexts where enforcement mechanisms are difficult to establish or enforce.



Simply put, in the **lack of compliance** by states and telecom operators with these Recommendations, it would be **virtually impossible to dial a phone number**, let alone communicate with subscribers of telecom operators in other countries. Thus, it is understandable why the very nature of the ITU's soft law is significantly different than that of a typical soft law instrument. In reality, states comply merely because of "the simple necessity to comply" (Hinricher, 2004).

3.4. Mapping the tools for regulation of key technologies

In that light, **soft law** is not only **increasingly utilized** by typical rule-making subjects such as states and international organizations in the field of technology, but due to its standardization potential and easier adoption/amendment procedures, it is **often preferred** to hard law instruments such as laws and treaties. Therefore, it is an important tool in the normative construction of technology governance. It is especially visible in areas where consensus is not easily achievable. To better understand and explore this **shift** in the technology regulation and the role of the old, evolving, and new **tools available to regulators and legislators**, as well as **their relationship to the various stakeholders** in the technology ecosystem, a comprehensive desk research was conducted, exploring a variety of jurisdictions on a global scale. *Annex 1* presents the results of this research. The analyzed documents were selected on two criteria within the existing legislation and regulation, related to the respective technologies: 1) geographical representation with a strong focus on EU due to the need for identification of common values in WP5 and 2) representation of different types of legal systems (e.g. civil law systems, common law systems, hybrid legal systems, etc.). The analysis was performed in two steps. First, by extraction of identification features such as type of regulation, current status, etc. and second by identifying the relevant stakeholders.

Mapping the tools used globally for regulation of key technologies provided us with some interesting results. The **methodology** used first focused on **identifying and categorizing** the technologies of interest. Based on feasibility considerations as well as the contemporary dynamic in the field we concentrated our analysis on **artificial intelligence (AI), distributed ledger technologies (blockchain), Internet of Things (IoT) Internet, cloud computing, and 5G/6G technologies**. This was followed by a **global and regional jurisdictional mapping**, where countries and international bodies significant to these technologies were pinpointed based on geographical, economical and legally system representativeness criteria. The regulatory **tools were then categorized** into hard law (laws, treaties), soft law, standards, and various forms of innovative regulation like anticipatory, experimental, and collaborative regulation. **Data collection** involved the gathering of legislation, treaties, standards, guidelines, and relevant case studies. Concurrently, the **type of stakeholders in each jurisdiction**, including government bodies, regulators, industry players, academic institutions, the public, and NGOs, were identified to understand their roles in regulation formulation and impact. The next phase involved a detailed analysis of the regulatory status of each tool in different jurisdictions, assessing their current state, effectiveness, and societal impact. A **technology-regulatory tools matrix** was then created, offering a visual, ledger, representation of the correlation between technologies, and the preferred regulatory tools.

In addition, the analysis presented us with some interesting findings specifically related to the separate technologies, reflecting the **phase of their development**, their **strategic importance**, as well as **their impact on society**.

1. AI Regulation: The data indicates a diverse approach to AI regulation across different jurisdictions, with a balance between hard law, soft law, and a significant focus on standards and experimental regulations. Because AI has the capability to affect almost all areas of society, the preferred legislative approach appears to favor a *lex generalis* approach by adopting an AI-focused piece of legislation, rather than opting solely for including specific AI-related provisions in relevant law in fields such as data protection, cybersecurity, healthcare, etc. *Figure 4* still shows that soft law keeps its prominent role with respect to regulation of technologies, especially when there is not a wide consensus. Geographically,



Annex I showcases clear efforts to incorporate and harness the benefits of anticipatory and experimental regulation outside Europe. Jurisdictions such as the USA, Singapore, China, and South Korea have been heavily involved in this new type of regulatory tools. In Europe, the focus seems to be on crafting mandatory, legally binding rules, while experimental and anticipatory regulations are significantly modified, practically turned into a much 'safer' and 'softer' version of their counterparts outside Europe.

2. Distributed Ledger Technology (Blockchain) Regulation: The data reveals an interesting picture of the probably most matured technology from a regulatory point of view. The nature of the technology itself was considered a deterrent with respect to adopting *lex generalis* approach, however, instead the preferred approach was the adoption of many sector-specific law with respect to the application of blockchain technology (e.g. Regulation (EU) 2023/1114 on crypto-assets, the Austrian E-Money Act, etc.). Anticipatory regulation, predominantly in the shape of regulatory sandboxes for FinTech, is widely spread across jurisdictions. Due to the origin of the very tool of the regulatory sandbox in the context of financial regulation and the first sandboxes being FinTech sandboxes, it is not surprising that states had the time to evaluate the new tool, adapt it to their specific needs and successfully utilize it domestically, even eyeing its international applications. In addition, Europe is not at a disadvantage based solely on the number of operational sandboxes where blockchain solutions are being tested. The disadvantage, however, comes due to the broader experimentation capabilities and legal waivers offered by jurisdictions outside Europe. Singapore, in particular, offers the most developed range of anticipatory regulation tools in the field of blockchain, also meaningfully engaging an increasing number of stakeholders.

3. Internet of Things (IoT) Regulation: Similarly to the Blockchain Regulation, IoT as a technology is better approached through focus on its particular applications in diverse domains, rather than adopting a single legal act, attempting to cover all the arising risks. Additionally, IoT is often combined with other technologies such cloud computing, 5G, and AI. Therefore, a technology neutral approach should be preferred by the legislators, instead focusing on the general regulation of fields such as privacy, security, etc. and the wide adoption of the appropriate technology standards. This is currently the preferred method and it's conducted either through standardization bodies and organizations (e.g. ISO, IEEE, etc.) or through soft law on either national or international level (ITU's recommendations, India's Code of Practice for Securing Consumer IoT, etc.).



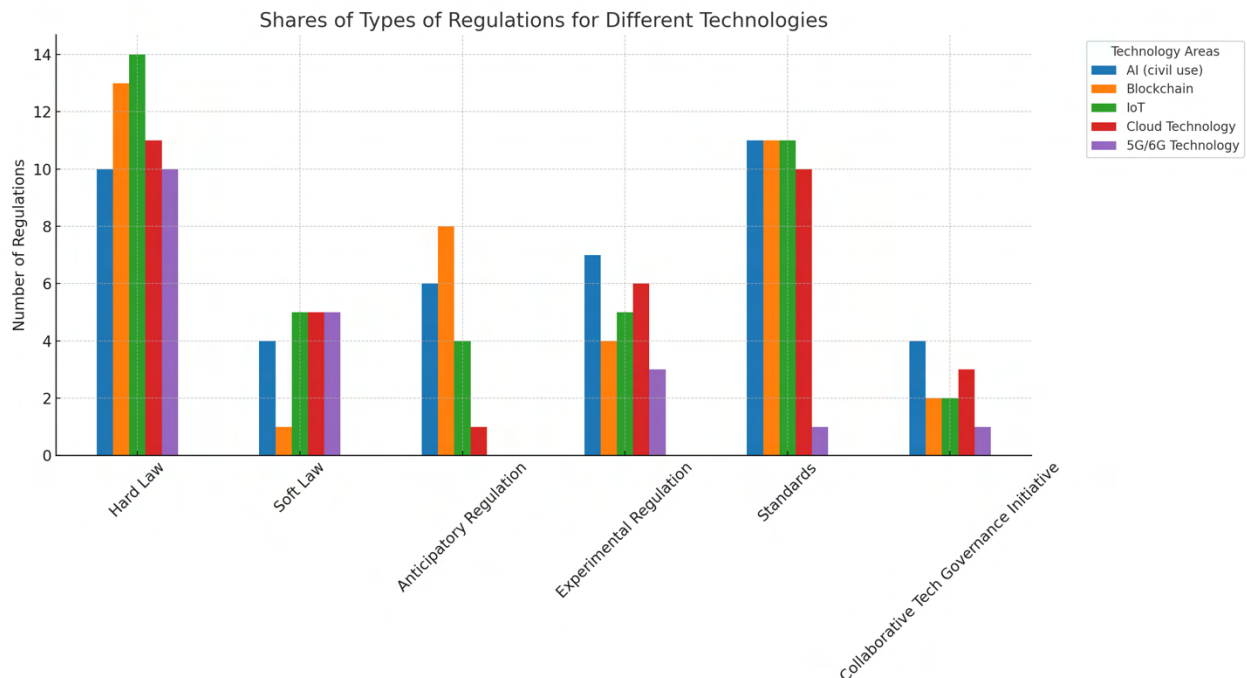


Figure 4: Types of Regulations

4. Cloud Computing Regulations: The analysis of the data revealed that the regulation of cloud computing is the area where soft law plays the most pivotal role, compared to the traditional hard law regulation. Similarly to IoT, cloud computing is usually combined with other technologies in order to be implemented within a product or service that could have a societal impact which should be regulated. Simultaneously, the technology is part of many innovative products and services which are being tested in testbeds or regulatory sandboxes, contributing to the respective regulators' better understanding of novel disruptive technologies. While this may not necessarily contribute to regulatory efforts dedicated solely to cloud computing, it does improve the quality of the regulation in the respective field the technology is being used in (e.g. automotive, manufacturing, etc.) or the protection of respective rights and freedoms (e.g. privacy).

5. 5G/6G Regulation: The collected data on regulation of 5G/6G technologies provided some interesting insights. While the specific regulation tools were rather scarce in comparison to the other four technologies, the share of the hard law was significantly larger than in the other four use-cases (see *Figure 4*). This could be explained through the geopolitical importance and implications of 5G technology, particularly with regard to digital sovereignty and strategic autonomy. Therefore, it is not surprising that the biggest chunk of the corresponding hard law in Europe, the USA and their allies is dedicated to cybersecurity and national security. Simultaneously, the share of the standards is also smaller than expected, especially compared to experimentation regulation, usually in the form of testbeds and outside Europe.

4. Conclusion

Aggregating the results from the mapping exercise, we have a more comprehensive picture of the current regulatory landscape globally. *Figure 5* illustrates a few essential trends in the regulation of disruptive technologies.

1) While hard law remains the predominant choice for regulators and legislators, its overall share is less than the combined shares of soft law, standards, and the various forms of anticipatory regulation in a broad sense.



2) The significant share of soft law signifies the need for more agile forms of regulation when dealing with technologies, especially internationally. Furthermore, it allows the adoption of rules (even if non-binding) in a context of a fragmented international community where consensus is hard to be reached.

3) The overall large share of alternative forms of regulation shows we need a different approach to regulation of dynamic and highly impactful technologies. It also indicated the need for a broader participation in the regulatory process from companies, civil society representatives and technology experts. Finally, the data suggests that while regulation is certainly high on the agenda of states and international organizations, facilitating and supporting innovation is also taken into account, to the point that experimentation and regulation are considered to not be mutually exclusive anymore, but rather mutually beneficial.

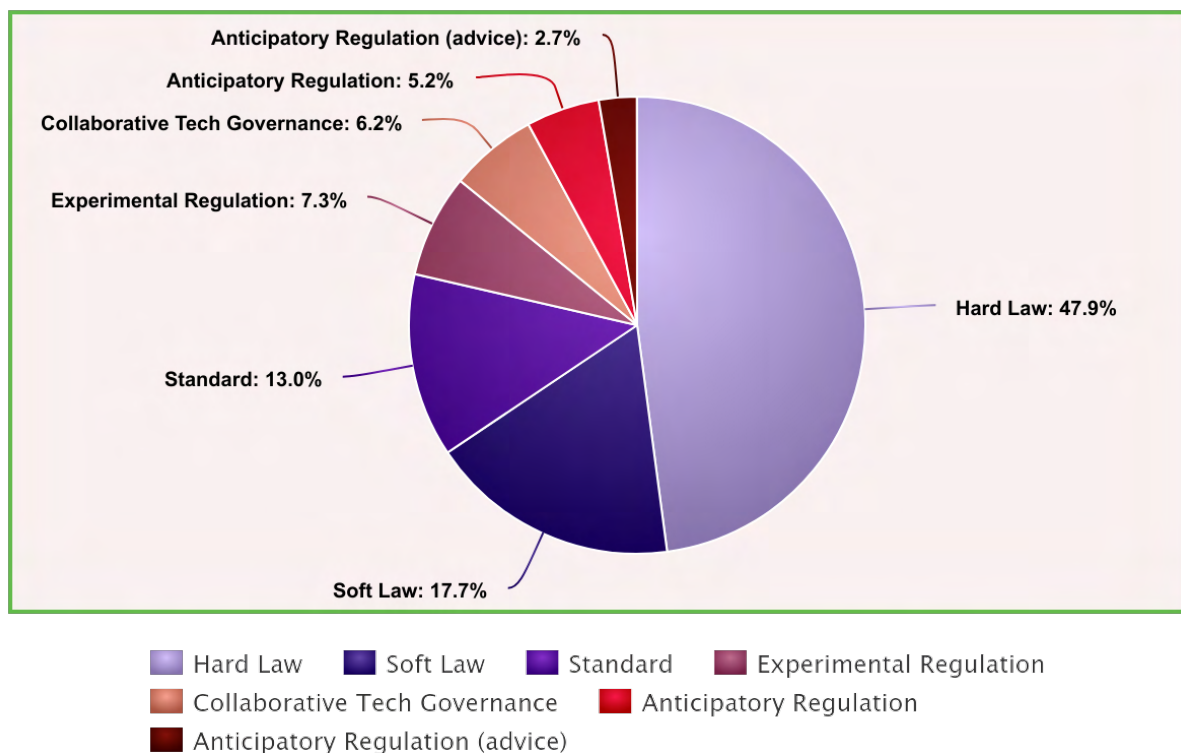


Figure 4: Regulatory landscape

Reflecting on the doctrinal analysis and the mapping of the existing tools for regulation in selected key technology areas, documented in full in *Appendix 1*, we can draw several conclusions, which are also important for the application of the ACF to technology regulation.

- 1) Defining policy subsystems could prove to be difficult due to the **increase of stakeholders** in the context of anticipatory regulation, as well as their evolving importance for the regulatory process.
- 2) ACF can prove to be a timely instrument in a period of change in the regulatory process by helping to provide a **more nuanced understanding of the dynamics of policy change** on technology issues.
- 3) ACF can be used to develop **more effective policy design strategies**. By understanding the beliefs and values of different advocacy coalitions, policymakers can tailor their policy proposals to be more acceptable to a wider range of stakeholders, in addition to the evidence-based anticipatory strategy which remains the core goal for the regulation of the future.
- 4) Due to the collaborative nature of the anticipatory regulation, ACF can **promote collaboration among stakeholders** involved in technology regulation. By understanding the different perspectives and goals of different groups, policymakers can work to find common ground and develop consensus-based solutions.



Nevertheless, these conclusions are applicable mostly with respect to the tools of technology regulation which demonstrate certain anticipatory characteristics, even in the form of advisory regulation. Despite the many positive sides of a more flexible and agile regulation, particularly in the fast-phased field of disruptive technologies, the **predominant tools for technology regulation remain the legally binding instruments** on national or international level (treaties, conventions, laws, etc.). Furthermore, the application of tools of anticipatory regulation often is accompanied by **confusion by the stakeholders and the regulators** who are faced with a choice between instruments they are not entirely familiar with, hence, the choice of the best suited tool for a concrete use-case or technology domain, **might not be properly justified and informed**.

As demonstrated by *Table 3*, which focuses on experimental regulation by analyzing the tools of regulatory sandboxes, testbeds, living labs and policy learning labs, many of the anticipatory regulation's tools have **close and sometimes overlapping scope**. What is currently lacking, however, is a **comprehensive methodology, informing and guiding both regulators and other stakeholders** on their respective choices and helping them understand their needs. In the case of the regulator, such a methodology would also incorporate horizon scanning regulatory strategy. Importantly, solving these issues with the anticipatory regulation on local or state level is a **necessary step towards its utilization in bilateral and multilateral settings**. While cross-border regulatory sandboxes have been heavily discussed, to the point of being explicitly mentioned in the EU's Proposal for the AI Act, it is far from clear how they are going to be structured, operated and valorised (Bromberg et al, 2019; Allen, 2019; Truby et al, 2022).

	Regulatory sandbox	Testbed	Living Lab	Policy Learning Lab
Purpose	A regulatory sandbox is a framework provided by regulatory authorities to facilitate the testing and development of innovative products, services, or business models within a regulated industry. It allows businesses to operate in a limited, controlled (or sometimes real-life) environment with certain regulatory exemptions , fostering innovation while managing risks.	A testbed is a controlled environment designed for testing and experimentation, typically in the context of technology, research, or development. It provides a setting where new technologies, systems, or processes can be tested under controlled conditions to assess their performance and functionality.	Living labs are broader in scope and focus on real-world experimentation , often in urban or community settings.	A policy learning lab is an environment designed for collaborative learning, experimentation, and the development of new policy solutions . It involves stakeholders working together to address complex societal challenges .
Scope	Regulatory sandboxes are specifically designed to test and implement innovations in a real-world, regulated environment , with a focus on industries subject to regulatory oversight.	Testbeds are generally focused on technology testing and experimentation , often within the domain of research and development.	Policy learning lab has a broader scope, emphasizing collaborative learning and experimentation across various policy domains and societal challenges.	Policy learning labs involve collaboration between researchers, businesses, and users to test and co-create innovative solutions in various domains , including urban planning, healthcare, and smart cities.
Regulatory aspect	Regulatory sandboxes involve regulatory oversight to ensure that consumer protection and other regulatory objectives are maintained. However, certain regulatory requirements may be temporarily relaxed to encourage innovation.	Testbeds offer a high level of control over the testing environment, allowing for systematic and controlled experiments, without necessarily involving a regulator . If one is involved, nevertheless, they are with primary observant status or with approval functions in regulated industries .	Living labs emphasise user involvement and co-creation , engaging end-users in the design, testing, and refinement of innovations. Collaboration with the community and end-users is a central aspect of living labs, while regulator's participation is not needed .	While it may involve policy experimentation, the emphasis is on learning, collaboration, and co-creation rather than providing regulatory exemptions .
Industries	Regulatory sandboxes are commonly associated with regulated industries , such as finance, fintech, and emerging technologies (AI). The focus is often on financial services, privacy, energy, etc. and sectors with strict regulatory requirements , the focus being on getting a certain solution to the market quicker but in a compliant way .	Testbeds are used in various industries for technology and product testing . Typical fields are information technology, telecommunications, and engineering. They are often employed by researchers, developers, and engineers to evaluate the feasibility and functionality of new solutions.	Living labs can span a wide range of industries , including urban planning, healthcare, education, and sustainability. The focus is on creating solutions that address societal challenges and improve the quality of life in communities.	It can be applied to various domains , including urban planning, healthcare, education, and sustainability, where diverse stakeholders collaborate to develop and test policy solutions.

Table 3: Experimental regulation – overview of approaches



5. Next steps

The regulatory landscape analysis provides Work Package 3 with a legal-analytical understanding of the diversity of technology regulation approaches around the world, focused on a set of key technologies. The analysis allows for the empirical analysis to proceed with a knowledge of different EU and national approaches, and international regulatory practices (such as norm development at the ITU), which **allows us to adequately analyze and interpret the normative construction of technology governance and the diversity of beliefs present in this domain**. Following from this, some of the key tasks for the work package are to **identify the most relevant - or most contested - norms, specify the types of (multilateral) governance regimes focusing on specific technology policy subsystems, and to identify the advocacy coalitions and their beliefs about the technologies and their governance**. Particularly important in answering these questions is to address the **various types of actors involved in processes of the normative construction of technology governance**, e.g., civilian – military, public-private, to analyze **how governance is constructed**, e.g. through power or legitimacy (Haggart & Keller, 2021; Rodrik, 2012), and reflect on how technology governance fits within broader debates about intergovernmentalism versus transnational governance in global governance, historic contingencies, path-dependencies and ‘paradigms’. Last, but not least, as a work package we address to what extent these norms and processes differ across technologies covered by REMIT. This final section presents the methodological approaches currently underway order to empirically examine the framework outlined in this deliverable, which will build on the regulatory landscape analysis in the previous section.

In order to study the **multi-layered model of normative construction of technology governance**, we examine the normative foundations of global technology governance from a number of levels simultaneously, in close cooperation and with exchange of intermediate results. On the **micro-level**, we conduct and analyze interviews with individual policy-makers, who serve in various functions within EU institutions, and with members of different stakeholder groups, who engage in technology governance from around the world, who represent companies, international organizations, civil society organizations, academia and technical specialists, and national public institutions. We also conduct a **meso-level** analysis based on the normative written outputs from a variety of actors engaged in specific fields of global technology governance - Internet infrastructure and AI. On the **macro level**, we survey citizens from countries around the world about their normative positions and preferences toward global technology governance. Using data from these diverse sources, we aim to better **understand how global technology governance and governors are perceived today and which normative positions EU policy-makers, global representatives of different stakeholder groups, and citizens express**. Each of these already ongoing research activities is recalled and specified below, starting from micro-level and leading up to the macro-level empirical analyses.

Micro-level: Via an **interview-based vignette study**, directed in empirical ethics and conducted by a moral philosopher, policymakers are confronted with moral scenarios on digital technology and digital technology governance. We seek to invite twenty EU policymakers for an individual in-depth interview, structured around vignettes. Vignettes are concise descriptions of a person or a detailed, concrete (social or moral) situation that contain specific references to the most significant aspects within a decision-making or judgment-making process. Each vignette (ten in total) will contain a statement and/or scenario on digital technology (including AI) and/or its governance. Each policymaker is subsequently asked to reflect and to argue for their standpoints. A vignette, for instance, can focus on responsibility or contain a statement such as “too much governance regulation will kill innovation”. The body of data will be analysed using qualitative content analysis techniques and will reveal policymaker beliefs about how technology *should* be governed globally, though here from a distinctively EU perspective. We integrate these individual moral reflections (cf. lay morality) in an ethical reflection that



also includes normative guidelines for digital technology policymaking. Thus, this micro-level research will clearly contribute to achieving the **objective to “Understand the beliefs and values of EU policymakers concerning the questions of who and how technology should best be governed” (REMIT grant agreement).**

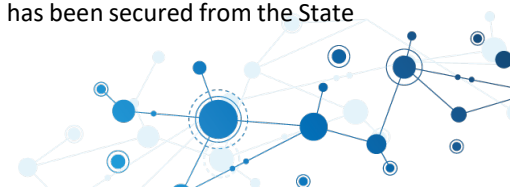
Additionally, by conducting *focus groups and interviews with stakeholders at global and regional technology governance fora*, we aim to broaden the scope to cover regional and global technology issues of the day in order to better understand the possibilities for an inclusive technology governance across levels. There are two case studies we focus on, for which we are in the research process:

- An analysis of **blockchain technologies and debates over security in digital governance platforms at the domestic, supranational and global levels from a Baltic and Nordic perspective**. Despite the EU’s Nordic and Baltic regions comprising mostly small states, both regions are highly modernized in terms of technological capability and in use of technological platforms for domestic governance. Three decades after the restoration of independence in the Baltic states – Estonia, Latvia and Lithuania – in 1991, the gap in socio-economic development between Baltic and neighboring Nordic states continues to close, while political and economic cooperation multilaterally between various states and within the EU continues to grow. With this wider convergence in the background, this research examines whether Nordic-Baltic cooperation can be a driver for technology governance within the EU and for the EU’s outlooks on global norms in technology governance. Through empirical data collection and a theoretical model utilizing the Advocacy Coalition Framework (ACF), this research will examine convergence and divergence in Baltic and Nordic normative positions through a most similar systems comparison.
- An analysis of the ongoing process of **drafting the United Nations Digital Global Compact (GDC)**, which is due to be passed by the General Assembly in September 2024 on occasion of the Summit of the Future. The ongoing consultations with stakeholders and negotiations among member states allow us to better understand the normative backstory of inclusive governance of the Internet, AI and other technologies covered by the GDC. A core theme for REMIT – **the challenge of sovereigntism and unilateralism to multilateralism and multistakeholderism – is investigated in this case study**. Interviewees are members of various stakeholder groups, who provide insights into the advocacy coalitions and actors’ core and policy beliefs within the negotiation process and the possible ramifications for open and inclusive governance arrangements post-GDC (and also after the upcoming WSIS+20 review). This case study is conducted following a single-case study design, with the aim to understand the ongoing negotiations and normative positions from a global perspective.

Both case studies are conducted using **focus groups and semi-structured interviews with members of governance/epistemic communities combining industry, policymaking and academic experts in the respective technology fields**. The initial approach to hold focus group meetings exclusively at (the side of) policy conferences has proven to be a challenge, with virtual follow-up focus groups as a possible go-around. Interviewees tend to be unwilling to spend too much time during a conference serving as a research subject, and coordination of focus group sessions proves difficult logistically. Nonetheless, the policy conferences serve for a great recruitment opportunity for follow-up interviews and focus group sessions.

Meso-level: We examine normative standards held about digital technology governance by a variety of stakeholders through a **qualitative and quantitative analysis of declaratory documents, so-called Digital Bills of Rights**. The analysis covers 321 digital bills of rights from 1992 to 2023, qualitatively analyzed through hand-coding for various rights and principles.⁷ The underlying dataset includes

⁷ As indicated in the project proposal, this database is based on a set of previous efforts by the scholarly Digital Constitutionalism Network. Outside funding, including prior to the start of REMIT, has been secured from the State



documents that make **normative claims about how the Internet, AI and – in general – the digital environment ought to be, with respect to rights that people have (e.g., privacy) and governing principles (e.g., participatory)**. The dataset that includes documents such as AI principles documents published by industry groups, Internet rights declaration by networks of civil society groups and non-binding recommendations by international inter-state organizations such as the UN, the Council of Europe or the ITU. This type of documents is often referred to as an output of a digital constitutionalist ideology or movement in digital governance (Celeste, 2019; Redeker et al., 2018). Looking from this constitutional perspective, which focuses on how rights and principles can be entrenched in national, regional and global digital governance, we examine how other advocacy coalitions – and paradigms, specifically sovereigntist and neoliberal models, have developed as evidenced by these documents. Employing elements from the Advocacy Coalition Framework (ACF), we analyze deep core and policy core beliefs of actors in the transnational Internet governance field. This adaptation helps to understand the advocacy coalitions behind digital bills of rights and their alignment with normative positions aligned with the three paradigms. **Quantitatively, through semantic and affiliation network analysis**, we assess how actors align around rights claims and policy options, showing a shift from a focus on freedom of expression to a more complex landscape with diverse concerns, actors, and an emphasis on procedural guarantees in both private and public sectors. Thus, this meso-level research will clearly contribute to achieving the **objective to “understand civil society, corporate, international organization and multistakeholder beliefs and values concerning various paradigms of governing technology in Europe and globally”** (REMIT grant agreement).

Macro-level: We employ a **large-scale public opinion survey** in order to better understand the normative stances of populations toward technology governance in countries that are possible partners for the EU. While representing one element of the **background conditions for meaningful cooperation and coalitions toward an open and participatory governance of technologies** (much like domestic regulatory frameworks as explored earlier in this deliverable), public opinion can obviously also be affected by the behavior of states in the international system. Few comprehensive public opinion surveys have been conducted thus far about the relationship between technology and multilateral and multistakeholder governance. Hence, being essentially exploratory in nature, we will conduct a thorough quantitative analysis to *inter alia* **create knowledge about the degree to which the different paradigms in technology governance are accepted among populations, and about the degree to which states, digital corporations and international multilateral institutions command the public’s trust in these countries**. With rising prices to conduct a high-quality quota sample for the online survey, a pilot study has already been conducted with 1,168 respondents in the Republic of Georgia to test possible survey questions and options for analysis.⁸ The analysis of the data is ongoing at the time of writing of the deliverable, while we expect a decision for survey questions and final scoping by September 2024. Thus, this macro-level research is connected to achieving the **objective to “understand the beliefs and values of citizens in 40 [to be determined] countries to understand public attitudes concerning the questions of who and how technology should best be governed”** (REMIT grant agreement).

References

Aguerre, C., Campbell-Verduyn, M., & Scholte, J. A. (2024). Introduction: Polycentric perspectives on digital data governance. In C. Aguerre, M. Campbell-Verduyn, J. A. Scholte (eds.) *Global Digital Data Governance: Polycentric Perspectives*. New York: Routledge.

of Bremen and from the Academy of Arts and Humanities in Hamburg. The database has been recoded, updated and significantly extended.

⁸ This pilot study has been co-financed by the Academy of Arts and Humanities in Hamburg.



- Aldisert, R. J. (1982). Rambling through continental legal systems. *University of Pittsburgh Law Review*, 43(4), 935-994.
- Allen, H. J. (2019). Sandbox boundaries. *Vand. J. Ent. & Tech. L.*, 22, 299.
- Aranson, P. H., Gellhorn, E., & Robinson, G. O. (1982-1983). Theory of legislative delegation. *Cornell Law Review*, 68(1), 1-67.
- Armstrong, H., & Rae, J. (2017). A working model for anticipatory regulation. Working Paper. NESTA.
- Armstrong, H., Gorst, C., & Rae, J. (2019). Renewing regulation: Anticipatory Regulation in an age of disruption. NESTA.
- Arroyo, V., Hess, K., Grünbaum, N., Ribeiro, G., & G'sell, F. (2023). What specific measures could the US, the EU and China take in order to foster and facilitate cross-border data flows? SciencesPo Chair Digital, Governance and Sovereignty. Comparative Approach to Big Tech Regulation.
- Baldwin, R., Cave, M., & Lodge, M. (2012). Understanding regulation: Theory, strategy, and practice (2nd ed.). Oxford: Oxford University Press.
- Baldwin, R., Scott, C., & Hood, C. (1998). Introduction. In R Baldwin, C Scott, C Hood (Eds.), A reader on regulation (pp. 1–55). Oxford: Oxford University Press.
- Berger, R. (1967-1968). Do regulations really bind regulators? *Northwestern University Law Review*, 62(2), 137-180.
- Bertolini, A. (2022). Artificial Intelligence does not exist! Defying the technology-neutrality narrative in the regulation of civil liability for advanced technologies. *EUROPA E DIRITTO PRIVATO*, (2), 369-420.
- Björkdahl, A. (2002). Norms in international relations: Some conceptual and methodological reflections. *Cambridge Review of International Affairs*, 15(1), 9-23.
- Black, J., Lodge, M., & Thatcher, M. (2005). Regulatory innovation. A comparative perspective. Cheltenham: Edward Elgar.
- Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford: Oxford University Press.
- Brännström, L. (2023). Global inequality and the EU international law position on cross-border data flows. *Nordic Journal of International Law*, 92(1), 119–137.
- Bromberg, L., Godwin, A., & Ramsay, I. (2018). Cross-border cooperation in financial regulation: Crossing the Fintech bridge. *Capital Markets Law Journal*, 13(1), 59-84.
- Brousseau, E., Marzouki, M., & Méadel, C. (Eds.). (2012). Governance, regulation, and powers on the internet. Cambridge: Cambridge University Press.
- Brownsword, R. (2022). Rethinking law, regulation and technology. Edward Elgar Publishing.
- Buckley, R., Arner, D., Veidt, R., & Zetsche, D. (2020). Building FinTech ecosystems: Regulatory sandboxes, innovation hubs, and beyond. *Wash. UJL & Pol'y*, 61, 55.
- Cacciaguidi-Fahy, S., & Wagner, A. (2016). Introduction: The chiaroscuro of legal language. In S. Cacciaguidi-Fahy & A. Wagner (Eds.), *Obscurity and clarity in the law: Prospects and challenges*. London: Routledge.
- Celeste, E. (2019). Digital constitutionalism: a new systematic theorisation. *International Review of Law, Computers & Technology*, 33(1), 76-99.
- De Gregorio, G., & Dunn, P. (2022). The European risk-based approaches: Connecting constitutional dots in the digital age. *Common Market Law Review*, 59(2).
- Degan, V. (1998). Sources of international law. Kluwer Law International.
- Drahoš, P. (Ed.). (2017). Regulatory theory: Foundations and applications. Canberra: ANU Press.
- Epstein, D., Newhart, M., & Vernon, R. (2014). Not by technology alone: The “analog” aspects of online public engagement in policymaking. *Government Information Quarterly*, 31(2), 337-344.
- Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, 52(4), 887-917.
- Frank, J. (2021). Toward more effective "multi-stakeholderism". *Georgetown Journal of International Affairs*, 22(2), 239-245.
- Gasser, U., & Almeida, V. (2022). Futures of digital governance. *Communications of the ACM*, 65(3), 30-32.



- Gasser, U., Budish, R., & West, S. (2015). Multistakeholder as governance groups: Observations from case studies. *Berkman Center Research Publication*, 2015(1).
- Guastini, R. (2007). On the theory of legal sources: A continental point of view. *Ratio Juris*, 20, 302-309.
- Haggart, B., & Keller, C. I. (2021). Democratic legitimacy in global platform governance. *Telecommunications Policy*, 45(6), 102152.
- Hampson, F. O., & Heinbecker, P. (2011). The "new" multilateralism of the twenty-first century. *Global Governance*, 17(3), 299-310.
- Hansson, L. (2020). Regulatory governance in emerging technologies: The case of autonomous vehicles in Sweden and Norway. *Research in Transportation Economics*, 83, 100967.
- Heidegger, M. (1977). *The Question concerning technology, and other essays* (12.2.1976 ed.). New York: Harper Torchbooks.
- Hennen, L., & van Est, R. (2023). Globalisation as reflexive modernisation—Implications for S&T governance. In L. Hennen et al. (Ed.), *Technology assessment in a globalized world: Facing the challenges of transnational technology governance* (1st ed.). Cham: Springer International Publishing.
- Hinricher, J. (2004). The law-making of the International Telecommunication Union (ITU) - Providing a new source of international law? *Zeitschrift für ausländisches öffentliches Recht und Völkerrecht*, 64(2).
- Hodson, D. (2021). The politics of FinTech: Technology, regulation, and disruption in UK and German retail banking. *Public Administration (London)*, 99(4), 859–872.
- Hofmann, H. (2009). Legislation, delegation and implementation under the Treaty of Lisbon: Typology meets reality. *European Law Journal*, 15, 482-505.
- Hofmann, J. (2016). Multi-stakeholderism in internet governance: Putting a fiction into practice. *Journal of Cyber Policy*, 1(1), 29-49.
- Hofmann, J., Katzenbach, C., & Gollatz, K. (2017). Between coordination and regulation: Finding the governance in Internet governance. *New Media & Society*, 19(9), 1406-1423.
- Johnson, W. G. (2023). Caught in quicksand? Compliance and legitimacy challenges in using regulatory sandboxes to manage emerging technologies. *Regulation & Governance*, 17(3), 709-725.
- Keohane, R. O. (1989). Multilateralism: An agenda for research. *International Journal*, 45(4), 731-764.
- Kingsbury, B., & Schill, S. W. (2010). Public law concepts to balance investors' rights with state regulatory actions in the public interest—the concept of proportionality. In S. W. Schill (Ed.), *International investment law and comparative public law*. Oxford University Press Inc.
- Koop, C., & Lodge, M. (2017). What is regulation? An interdisciplinary concept analysis. *Regulation & Governance*, 11, 95–108.
- Kosti, Nir, Levi-Faur, David, & Mor, Guy (2019). Legislation and regulation: Three analytical distinctions. *The Theory and Practice of Legislation*, 7(3), 169-178, DOI: 10.1080/20508840.2019.1736369
- Liebwald, D. (2015). On transparent law, good legislation and accessibility to legal information: Towards an integrated legal information system. *Artificial Intelligence and Law*, 23, 301–314.
- Lyall, F. (1995). Posts and telecommunications. In O. Schachter & Ch. Joyner (Eds.), *United Nations legal order* (Vol. 2). Cambridge: Cambridge University Press.
- Morth, U. (2004). *Soft Law in Governance and Regulation*. Cheltenham: Edward Elgar.
- Moses, L. B. (2013). How to think about law, regulation and technology: Problems with 'technology' as a regulatory target. *Law, Innovation and Technology*, 5(1), 1-20.
- Mueller, M. L. (2010). *Networks and states: The global politics of internet governance*. Cambridge: MIT Press.
- Nye, J. S. (2014). The regime complex for managing global cyber activities. *CIGI Paper No. 206*. https://www.cigionline.org/sites/default/files/gcig_paper_no1.pdf
- OECD. (2023). *Government at a glance 2023*. OECD Publishing, Paris. http://dx.doi.org/10.1787/gov_glance-2017-en
- Page, E. (2001). *Governing by Numbers: Delegated Legislation and Everyday Policy-Making* (1st ed.). Oxford: Hart Publishing.



- Prosser, T. (2010). *The regulatory enterprise: Government, regulation, and legitimacy*. Oxford: Oxford University Press.
- Radu, R. (2019). *Negotiating internet governance*. Oxford: Oxford University Press.
- Ranchordás, S. (2014). Innovation-friendly regulation: The sunset of regulation, the sunrise of innovation. *Jurimetrics*, 55, 201.
- Ranchordás, S. (2021). Experimental regulations and regulatory sandboxes: Law without order? University of Groningen Faculty of Law Research Paper, (10).
- Ranchordás, S., & van't Schip, M. (2019). Future-proofing legislation for the digital age. Time, Law, and Change. Hart. University of Groningen Faculty of Law Research Paper, (36).
- Redeker, D., Gill, L., & Gasser, U. (2018). Towards digital constitutionalism? Mapping attempts to craft an Internet Bill of Rights. *International Communication Gazette*, 80(4), 302-319.
- REMIT. (2023). Advocacy coalition framework - REMIT handbook.
- Ringe, W. G., & Christopher, R. U. O. F. (2020). Regulating Fintech in the EU: The case for a guided sandbox. *European Journal of Risk Regulation*, 11(3), 604-629.
- Rodrik, D. (2012). *The globalization paradox: Why global markets, states, and democracy can't coexist*. Oxford: Oxford University Press.
- Santaniello, M. (2021). From governance denial to state regulation: A controversy-based typology of internet governance models. In B. Haggart, N. Tusikov, & J. A. Scholte (Eds.), *Power and Authority in Internet Governance: Return of the State?* London: Routledge.
- Scalabrin Bianchi, I., Dinis Sousa, R., & Pereira, R. (2021). Information technology governance for higher education institutions: A multi-country study. *Informatics*, 8(2), 26.
- Scharpf, F. W. (1997). Economic integration, democracy and the welfare state. *Journal of European Public Policy*, 4(1), 18-36.
- Schebesta, H., & Sartor, G. (2015). NoC Internet Governance Case Studies Series: Aviation—The worldwide slot guidelines. In *Multistakeholder as Governance Groups: Observations from Case Studies*. Berkman Center for Internet & Society.
- Scholte, J. A. (2004). Civil society and democratically accountable global governance. *Government and Opposition*, 39(2), 211-233.
- Selznick, P. (1985). Focusing organizational research on regulation. In R. Noll (Ed.), *Regulatory policy and the social sciences* (pp. 363–367). Berkeley: University of California Press.
- Serentschy, G., Timmers, P., & Matinmikko-Blue, M. (2023). Toward anticipatory regulation and beyond. In *The changing world of mobile communications: 5G, 6G and the future of digital services* (pp. 221-251). Cham: Springer International Publishing.
- Shadikhodjaev, S. (2021). Technological neutrality and regulation of digital trade: How far can we go? *European Journal of International Law*, 32(4), 1221-1247.
- Sitaraman, G. (2015). The origins of the legislation. *Notre Dame Law Review*, 91(1), 79-132.
- Sofyani, H., Riyadh, H. A., & Fahlevi, H. (2020). Improving service quality, accountability and transparency of local government: The intervening role of information technology governance. *Cogent Business & Management*, 7(1).
- Sweet, A. S. (2007). The politics of constitutional review in France and Europe. *International Journal of Constitutional Law*, 5(1), 69–92.
- Tarrant, A., & Cowen, T. (2022). Big tech lobbying in the EU. *The Political Quarterly*, 93, 218-226.
- Thorogood, A. (2020). Policy-aware data lakes: A flexible approach to achieve legal interoperability for global research collaborations. *Journal of Law and the Biosciences*, 7(1).
- Trachtman, J. (2023). Developing multistakeholder structures for cybersecurity norms: Learning from experience. In I. Johnstone, A. Sukumar, J. Trachtman (Eds.) *Building an International Cybersecurity Regime* (pp. 85-110). Cheltenham: Edward Elgar Publishing.
- Truby, J., Dahdal, A., & Ibrahim, I. A. (2022). Sandboxes in the desert: Is a cross-border 'gulf box' feasible? *Law, Innovation and Technology*, 14(2), 447-473.
- Wagner, B., Rozgonyi, K., Sekwenz, M.T., Cobbe, J., & Singh, J. (2020). Regulating transparency? Facebook, twitter and the German network enforcement act. In *Proceedings of the 2020 conference on fairness, accountability, and transparency* (pp. 261-271).



- Walsh, S., & Linton, J. (2000). Infrastructure for emerging markets based on discontinuous innovations. *Eng. Manag. J.*, 12(2), 23–31.
- Wasserman, M. F. (2014). Deference asymmetries: Distortions in the evolution of regulatory law. *Tex. L. Rev.*, 93, 625.
- Weber, R. H. (2011). Shift of legislative powers and multi-stakeholder governance. *International Journal of Public Law and Policy*, 1(1), 4-22.
- Zetzsche, D. A., Buckley, R. P., Barberis, J.N., & Arner, D. W. (2017). Regulating a revolution: From regulatory sandboxes to smart regulation. *Fordham Journal of Corporate & Financial Law*, 23, 31.
- Zhou, W., & Piramuthu, S. (2013). Technology regulation policy for business ethics: An example of RFID in supply chain management. *Journal of Business Ethics*, 116(2), 327–340.
- Zwitter, A., & Hazenberg, J. (2020). Decentralized network governance: Blockchain technology and the future of regulation. *Frontiers in Blockchain*, 3, 12.



Annex

Artificial Intelligence (civil use)

Explanatory notes:

- The colour coding in column 'Status' indicates:
 - Yellow: under negotiations/ yet to enter into force or become applicable
 - Green: applicable/ published
 - Red: process paused/ceased
- The categories in column 'Stakeholders' follow the specific language of the instrument/organisation/ initiative. The additional indications represent:
 - (a) – active stakeholder – having means for direct impact on the content of the regulatory instrument
 - (p) – passive stakeholder – the regulatory instrument is directly targeting the stakeholder, without them having means for direct impact on the content of the regulatory instrument.
- The mapped regulatory tools reflect solely specific AI-regulation, without prejudice to other types of regulation and legislation, connected to AI technologies but not entirely related to them such as data regulation, cybersecurity regulation, sectorial regulation in industries such as healthcare, manufacturing, etc.

Jurisdiction	Type of regulation	Name	Status	Stakeholders (directly involved)	Source
European Union	Hard Law	AI Act Proposal		EU institutions (a), EU Member States (a), AI developers and providers (p), consumers and users (p).	Press release on the provisional agreement reached between the Council and the Parliament
European Union	Hard Law	AI Liability Directive Proposal		EU institutions (a), EU Member States (a), AI developers and providers (p), consumers and users (p).	AI Liability Directive proposal published by the European Commission
European Union	Anticipatory regulation	Regulatory sandbox for AI (transnational)		EU institutions(a), EU Member States (a), AI developers and providers (a), Industry and Business (a)	Shaping Europe's Digital Future: First Regulatory Sandbox on Artificial Intelligence European Parliamentary Research Service (EPRS) Briefing
Council of Europe	Hard Law	Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (draft)		Council of Europe ecosystem (a), AI developers and producers (p), CSOs (p), academia (p), national governments (a), international organisations (a), ethics advisory bodies (p), industry associations and trade bodies (p), users and consumers (p)	Draft Framework Convention on Artificial Intelligence, Human Rights, Democracy and the Rule of Law (2nd reading by CAI)
United Nations	Soft Law	The UN Secretary-General's AI		UN (a), CSOs (p), academia (p), national governments (a), industry (p), international	Interim Report: Governing AI for Humanity



		Advisory Body Interim Report		organisations (a), ethics advisory bodies (p), industry associations and trade bodies (p), users and consumers (p)	
UNESCO	Soft Law	Recommendations on the Ethics of Artificial Intelligence		UNESCO (a), UN (a), national governments (a), CSOs (p), research and academia (p), industry (p), international organisations (a), ethics advisory bodies (p),	Recommendations on the Ethics of Artificial Intelligence
UNDP	Anticipatory regulation	SDG AI Lab		International organisations (a), UN agencies (a), national governments (a), civil society organisations (a), academia (p), private sector (a)	SDG AI Lab
World Economic Forum	Collaborative Tech Governance Initiative	AI Governance Alliance		WEF (a), national governments (a), businesses (a), researchers and academia (a), CSOs (a), international organisations (a), ethics advisory bodies (a), users and consumers (p), journalists (p).	AI Governance Alliance
Organisation for Economic Co-operation and Development	Soft Law	Recommendation of the Council on Artificial Intelligence		OECD (a), national governments (a), businesses (p), researchers (p), CSOs (p), public interest organisations (p), individual users (p)	Recommendation of the Council on Artificial Intelligence
International Organization for Standardization	Standards	ISO/IEC 22989:2022 Artificial intelligence concepts and terminology		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC 22989:2022
International Organization for Standardization	Standards	ISO/IEC 23053:2022 Artificial intelligence Framework for artificial intelligence systems using machine learning		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC 23053:2022
International Organization for Standardization	Standards	ISO/IEC 42001:2023 Artificial intelligence Management system		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC 42001:2023
International Organization for Standardization	Standards	ISO/IEC 23894:2023 Artificial intelligence Guidance on risk management		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC 23894:2023
International Organization for Standardization	Standards	ISO/IEC DIS 5259-1 Artificial intelligence Data quality for analytics and machine learning		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC DIS 5259-1
International Organization for Standardization	Standards	ISO/IEC TR 24368:2022 Artificial intelligence		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC TR 24368:2022



		Overview of ethical and societal concerns			
International Organization for Standardization	Standards	ISO/IEC TR 24027:2021 Artificial intelligence Bias in AI systems and AI aided decision making		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC TR 24027:2021
International Organization for Standardization	Standards	ISO/IEC WD 27091 Artificial intelligence Privacy protection		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC WD 27091
International Organization for Standardization	Standards	ISO/IEC 38507:2022 Artificial intelligence Governance implications of the use of artificial intelligence by organizations		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC 38507:2022
International Organization for Standardization	Standards	ISO/IEC AWI 42105 Artificial intelligence Guidance for human oversight of AI systems		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p).	ISO/IEC AWI 42105
International Telecommunication Union	Collaborative Tech Governance Initiative	ITU Focus Groups		ITU (a), national governments (a), industry (p), academia (p), CSOs (p)	Focus Group on Artificial Intelligence for Health Focus Group on Artificial Intelligence (AI) and Internet of Things (IoT) for Digital Agriculture (FG-AI4A)
International Telecommunication Union	Collaborative Tech Governance Initiative	AI4Good		ITU (a), national governments (a), businesses (a), researchers (a), CSOs (a), international organisations (a)	AI for Good Global Summit
International Telecommunication Union	Soft Law	ITU-T Y.3115 (02/2022) AI enabled cross-domain network architectural requirements and framework for future networks including IMT-2020		ITU (a), national governments (a), businesses (a), researchers (a), CSOs (a)	ITU-T Y.3115 (02/2022)
International Telecommunication Union	Soft Law	ITU-T M.3383 (04/2023) Requirements for log analysis in telecom management with artificial intelligence		ITU (a), national governments (a), businesses (a), researchers (a), CSOs (a)	ITU-T M.3383 (04/2023)
International Telecommunication Union	Soft Law	ITU-T F Suppl. 4 (04/2021)		ITU (a), national governments (a), businesses (a), researchers (a), CSOs (a)	ITU-T F Suppl. 4 (04/2021)



		Overview of convergence of artificial intelligence and blockchain			
G7	Soft Law	The Hiroshima AI Process Comprehensive Policy Framework		National governments (a), businesses (p), individuals (p)	G7 Leaders' Statement on the Hiroshima AI Process
Public – Private Initiative	Experimental regulation	Open Loop		Governments (a), civil society organisations (a), academia (a), tech companies (a), users and communities (p)	Open Loop
Public – Private Initiative	Collaborative Tech Governance Initiative	The Global Partnership on Artificial Intelligence (GPAI)		International organisations (a), national governments (a), civil society organisations (a), the private sector (a)	GPAI
Bilateral Initiative	Collaborative Tech Governance Initiative	EU-US Trade and Technology Council (TTC)		Bipartisan Governmental stakeholders (a)	TTC
Brazil	Hard Law	Projeto de Lei nº 2338/2023		State (a), business (p), citizens (p), CSOs (p)	AI Bill
Brazil	Anticipatory Regulation	Regulatory sandbox for AI and data protection		Regulator (a), business (p), citizens (p), CSOs (p)	Regulatory sandbox for AI and data protection
Canada	Hard Law	The Artificial Intelligence and Data Act		State (a), business (p), citizens (p), CSOs (p)	The Artificial Intelligence and Data Act
Canada	Hard Law	Directive on Automated Decision-Making		State (s), institutions subject to the Policy on Service and Digital (p)	Directive on Automated Decision-Making
China	Hard Law	Internet Information Service Algorithmic Recommendation Management Provisions		State (a), citizens (p), business (p)	Internet Information Service Algorithmic Recommendation Management Provisions
China	Hard Law	Interim Measures for the Management of Generative Artificial Intelligence Services		State (a), citizens (p), business (p)	Interim Measures for the Management of Generative Artificial Intelligence Services
China	Hard Law	Internet Information Service Deep Synthesis Management Provisions		State (a), citizens (p), business (p)	Internet Information Service Deep Synthesis Management Provisions
China	Experimental regulation	AI pilot zones		State (a), industry (p), business (p)	The Shanghai FTZ The Beijing National New-Generation AI Innovation & Development Pilot Zone
France	Anticipatory regulation with	Sandbox for AI		State (a), privacy regulator (a), industry (a)	Sandbox for AI



	advisory approach				
Japan	Soft Law	Governance Guidelines for Implementation of AI Principles		State (a), citizens (p), business (p)	Governance Guidelines for Implementation of AI Principles
Norway	Anticipatory regulation	Regulatory sandbox for AI		State (a), privacy regulator (a), business (a), civil society organisation (p)	Regulatory sandbox for AI
Singapore	Soft Law	Proposed Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems		Government (a), business (a), academia (p), civil society (p)	Proposed Advisory Guidelines on use of Personal Data in AI Recommendation and Decision Systems
Singapore	Experimental Regulation	AI Verify Foundation		Regulator (a), government (a), business (a), civil society (p)	AI Verify Foundation
Singapore	Anticipatory Regulation	Veritas Initiative		Regulator (a), government (a), business (a)	Veritas Initiative
Singapore	Soft Law	Model AI Governance Framework		Regulators (a), government (a), industry (a), research organisations (p), consumer groups (p), CSOs (p)	Model AI Governance Framework (2nd edition)
Singapore	Experimental Regulation	Generative AI (Gen AI) Evaluation Sandbox		Regulators (a), AI Verify Foundation (a), government (a), industry (p), third-party testers (a), model developers (a), app developers (a)	Generative AI (Gen AI) Evaluation Sandbox
South Korea	Hard Law	Act on Promotion of AI Industry and Framework for Establishing Trustworthy AI		State (a), citizens (p), business (p)	AI Act Proposal
Spain	Anticipatory regulation with advisory approach	AI Regulatory Sandbox		State (a), business (a)	AI Regulatory Sandbox
Switzerland	Experimental Regulation	Innovation Sandbox for AI		State (a), academia (a), industry (a), municipality (a)	Innovation Sandbox for AI
United Arab Emirates	Soft Law	AI System Ethics Self-Assessment Tool		State (a), citizens (p), business (p)	AI System Ethics Self-Assessment Tool
United Arab Emirates	Soft Law	AI Ethics Principles and Guidelines		State (a), citizens (p), business (p)	AI Ethics Principles and Guidelines
United Kingdom	Collaborative Tech Governance Initiative	Algorithmic Transparency Recording Standard Hub		Government (a), industry (a), academia (a), civil society (a)	Algorithmic Transparency Recording Standard Hub
United States of America	Hard Law	Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence		President (a), governmental agencies (a), industry (p), academia (p), civil society (p)	Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence
United States of America	Hard Law	AI Training Act		Government (a), Office of Management and Budget (a), citizens (p)	AI Training Act
United States of America	Hard Law	National AI Initiative Act		Government (a), industry (p), academia (p), civil society (p)	National AI Initiative Act



United States of America	Hard Law	AI in Government Act		Government (a), industry (p), academia (p), civil society (p)	AI in Government Act
United States of America	Hard Law	Algorithmic Accountability Act Proposal		Government (a), industry (p), consumers (a), academia (a), technology experts (a), standards bodies (a), advocates for civil rights (a)	Algorithmic Accountability Act Proposal
United States of America	Hard Law	Transparent Automated Governance Act Proposal		Government (a), industry (p), academia (p), civil society (p)	Transparent Automated Governance Act Proposal
United States of America	Soft Law	Blueprint for an AI Bill of Rights		Government (a), industry (p), academia (p), civil society (p)	Blueprint for an AI Bill of Rights
United States of America	Soft Law	Guidance for Regulation of Artificial Intelligence Applications		Government (a), industry (p), academia (p), civil society (p), research institutions (p), consumer groups (p), workers' groups (p), religious groups (p)	Guidance for Regulation of Artificial Intelligence Applications
United States of America	Collaborative Tech Governance Initiative	Voluntary Commitments from Leading AI Companies to Manage the Risks Posed by AI		Leading AI companies (a), government (a), civil society (p), academia (p)	Voluntary Commitments from Leading AI Companies to Manage the Risks Posed by AI
United States of America	Experimental Regulation	The Argonne Leadership Computing Facility (ALCF) AI Testbed		Governmental agencies and agency-led initiatives (a), industry partners (p), academic institutions (p)	ALCF AI Testbed
United States of America	Experimental Regulation	The Assured Autonomy portal		Governmental agencies (a), industry partners (p), academic partners (p), non-governmental institutions	The Assured Autonomy portal
United States of America	Experimental Regulation	The National Cybersecurity Center of Excellence (NCCoE) Dioptra Testbed		Governmental agencies (a), industry partners (p), academic institutions (p), standardisation bodies (p), research and development organisations (p), user communities (p)	Dioptra Testbed
United States of America	Collaborative Tech Governance Initiative	AI Now		AI researchers and developers (a), Government agencies (a), Civil society organizations (a), the general public (p)	AI Now

Distributed Ledger Technology (Blockchain)

Explanatory notes:

- The colour coding in column 'Status' indicates:
 - Yellow: under negotiations/ yet to enter into force or become applicable
 - Green: applicable/ published
 - Red: process paused/ceased
- The categories in column 'Stakeholders' follow the specific language of the instrument/organisation/ initiative. The additional indications represent:



- (a) – active stakeholder – having means for direct impact on the content of the regulatory instrument
 - (p) – passive stakeholder – the regulatory instrument is directly targeting the stakeholder, without them having means for direct impact on the content of the regulatory instrument.
- The mapped regulatory tools reflect the relevant legislation/regulation (with particular focus on anticipatory and experimental regulation) in selected jurisdictions, based on the level of utilisation of blockchain technologies specific fields which include: digital ID, electronic money/crypto currency, digital and open banking,

Jurisdiction	Type of regulation	Name	Status	Stakeholders (directly involved)	Source
Bank for International Settlements	Experimental Regulation	BIS Innovation Hub		BIS (a), central banks (a), international organisations (a)	BIS Innovation Hub
EU	Hard Law	Regulation (EU) 2023/1114 of the European Parliament and of the Council of 31 May 2023 on markets in crypto-assets		EU (a), national member states/governments/regulators (a), citizens (p), businesses (p)	Regulation (EU) 2023/1114
EU	Hard Law	Directive 2009/110/EC of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions		EU (a), national member states/governments/regulators (a), citizens (p), businesses (p)	Directive 2009/110/EC
EU	Hard Law	Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market		EU (a), national member states/governments/regulators (a), citizens (p), businesses (p)	PSD2 Directive
EU	Hard Law	Proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro		EU (a), national member states/governments/regulators (a), citizens (p), businesses (p)	Digital Euro Regulation Proposal
EU	Anticipatory regulation	Pan-European blockchain regulatory sandbox		EU (a), regulators (a), supervising authorities (a), private sector (a), public sector (p)	European blockchain sandbox
Global Financial Innovation Network	Anticipatory regulation	Cross Border Testing		National regulators (a), businesses (a), industry (a)	Cross Border Testing
IEEE	Standard	IEEE 2140.4-2023 for Distributed/Decentralized Exchange Framework using Distributed Ledger Technology (DLT)		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2140.4-2023
IEEE	Standard	IEEE 2140.5-2020 for a Custodian Framework of Cryptocurrency		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	2140.5-2020



IEEE	Standard	IEEE 2140.1-2020 for General Requirements for Cryptocurrency Exchanges		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2140.1-2020
IEEE	Standard	IEEE 2143.1-2020 for General Process of Cryptocurrency Payment		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2143.1-2020
IEEE	Standard	IEEE 2144.1-2020 for Framework of Blockchain-based Internet of Things (IoT) Data Management		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2144.1-2020
IEEE	Standard	IEEE 2418.7-2021 for the Use of Blockchain in Supply Chain Finance		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2418.7-2021
IEEE	Standard	IEEE 3801-2022 for Blockchain-based Electronic Contracts		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 3801-2022
IEEE	Standard	IEEE P3226 for Trusted Data Circulation based on Blockchain and Distributed Ledger Technologies (DLT)		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE P3226
IEEE	Standard	IEEE P3222 for the Reference Architecture of Blockchain as a Service		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE P3222
IEEE	Standard	IEEE P3218/D3.0 for Using Blockchain for Carbon Trading Applications		IEEE (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE P3218/D3.0
International Monetary Fund	Soft Law	IMF's Central Bank Digital Currency (CBDC) Virtual Handbook		IMF (a), national governments (p), experts (p)	CBDC Virtual Handbook
ISO	Standard	ISO/TR 23244:2020 Blockchain and distributed ledger technologies Privacy and personally identifiable information protection considerations		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/TR 23244:2020
ISO	Standard	ISO/TS 23635:2022 Blockchain and distributed ledger technologies Guidelines for governance		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/TS 23635:2022
ISO	Standard	ISO/TR 6277 Blockchain and distributed ledger technologies Data flow models for blockchain and DLT use cases		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/TR 6277
ISO	Standard	ISO/AWI TS 18126		ISO (a), national governments (p), businesses (p), researchers (p),	ISO/AWI TS 18126



		Smart contract taxonomy and classification		CSOs (p), consumers (p), investors (p), educational institutions (p)	
UN	Collaborative Tech Governance Initiative	Task Force on Digital Financing of the Sustainable Development Goals		UN (a), governments (a), businesses (p), CSOs(p), academia (p)	Task Force on Digital Financing of SDGs
The Inter-American Development Bank, the Office of the Inspector General of Colombia and the World Economic Forum	Collaborative Tech Governance Initiative	Unlocking Government Transparency with Blockchain Technology (the Transparency Project)		International organisations (a), national governments (a), businesses (p), citizens (p)	Transparency Project
Australia, Singapore, South Africa, and Malaysia	Anticipatory regulation	International settlements using multi-CBDCs (Project Dunbar)		National governments/regulators	Project Dunbar
Australia	Anticipatory regulation	Enhanced regulatory sandbox		Government/regulator (a), business (a)	Enhanced regulatory sandbox
Australia	Anticipatory regulation	CBDC Pilot for Digital Finance Innovation		Government/regulator	CBDC Pilot for Digital Finance Innovation
Austria	Hard Law	Security Police Act (35a)		Government/ law enforcement (a), citizens (p)	Security Police Act
Austria	Anticipatory regulation with advisory approach	FMA Sandbox		Government/regulator (a), businesses (a), innovators (a)	FMA Sandbox
Austria	Hard Law	E-Money Act 2010		Government/regulator (a), citizens (p), business (p)	E-Money Act
Belgium	Hard Law	Loi portant des dispositions diverses concernant le Registre national et les registres de population (eID Act)		Government/ law enforcement (a), citizens (p)	eID Act
Brazil	Hard Law	Lei Nº 13.444, de 11 de Maio de 2017 (eID Act)		Government/ law enforcement (a), citizens (p)	eID Act
Brazil	Hard Law	Law Nº 12,865, of October 9, 2013 (e-money Act)		Government/regulator (a), citizens (p), business (p)	e-money Act
Brazil	Anticipatory regulation	BCB's Regulatory Sandbox		Government/regulator (a), business (a), public companies (a)	BCB's Regulatory Sandbox
Brazil	Experimental regulation	Open Finance		Government/regulator (a), service providers (a), consumers (a), businesses (a)	Open Finance
Canada	Hard Law	Electronic Payments Regulations SOR/98-129		Government/regulator (a), citizens (p), business (p)	Electronic Payments Regulations
Canada	Experimental regulation	CSA Financial Innovation Hub		Government/regulator (a), industry (a), business (a)	CSA Financial Innovation Hub
Canada	Anticipatory regulation	CSA Regulatory Sandbox		Government/regulator (a), industry (a), business (a)	CSA Financial Innovation Hub
China	Experimental regulation	e-CNY Testbed		Government/regulator (a), consumers (p), businesses (p)	e-CNY Testbed
China	Hard Law	Regulation of the People's Republic of China		Government/ law enforcement (a), citizens (p)	eID Law



		Concerning Resident Identity Cards			
China	Hard Law	The Act Governing Electronic Payment Institutions		Government/regulator (a), industry (p), businesses (p)	Electronic Payment Institutions
Denmark	Anticipatory regulation with advisory approach	The Danish FSA's sandbox initiative (FT lab)		Government/regulator (a), businesses (a)	FT lab
Estonia	Hard Law	Payment Institutions and E-money Institutions Act		Government/regulator (a), businesses (p), citizens (p)	Payment Institutions and E-money Institutions Act
Estonia	Hard Law	Identity Documents Act		Government/law enforcement (a), citizens (p)	Identity Documents Act
France	Hard Law	Loi n° 2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique		Government/regulators (a), businesses (p), citizens (p)	Loi n° 2000-230
France	Hard Law	Loi n° 2019-486 du 22 mai 2019 relative à la croissance et la transformation des entreprises		Government/regulators (a), businesses (p), citizens (p)	Loi PACTE
France	Hard Law	Décret n°55-1397 du 22 octobre 1955 instituant la carte nationale d'identité		Government/law enforcement (a), citizens (p)	Décret n°55-1397
Germany	Hard Law	Act on identity cards and electronic identification		Government/law enforcement (a), citizens (p)	eID Law
Germany	Anticipatory regulation with advisory approach	FinTech Innovation Hub		Government/regulators (a), businesses (a), citizens (p)	FinTech Innovation Hub
Greece	Anticipatory regulation with advisory approach	BOG Regulatory Sandbox		Government/regulators (a), businesses (a), citizens (p)	BOG Regulatory Sandbox
Hungary	Anticipatory regulation	MNB regulatory sandbox		Government/regulator (a), businesses (a)	MNB regulatory sandbox
Hungary	Anticipatory regulation with advisory approach	MNB iNNOHUB		Government/regulator (a), businesses (a), industry (a)	MNB iNNOHUB
India	Anticipatory regulation	Inter-operable Regulatory Sandbox (IoRS)		Government/regulator (a), businesses (a)	IoRS
India	Hard Law	The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act		Government/law enforcement (a), citizens (p)	The Aadhaar Act
Italy	Anticipatory regulation with advisory approach	Regulatory Sandbox for FinTech		Government/regulator (a), businesses (a), industry (a)	Regulatory Sandbox
Japan	Anticipatory regulation	Regulatory Sandbox Framework		Government/regulator (a), businesses (a)	Regulatory Sandbox Framework
Japan	Hard Law	Payment Services Act		Government/regulators (a), businesses (p), citizens (p)	Payment Services Act



Kenya	Hard Law	E-money Regulation		Government/regulator (a), businesses (p), citizens (p)	E-money Regulation
Kenya	Anticipatory regulation	CMA Regulatory Sandbox		Government/regulator (a), businesses (a), public bodies (a)	CMA Regulatory Sandbox
Lithuania	Anticipatory regulation with advisory approach	Regulatory sandbox		Government/regulator (a), businesses (a), public bodies (a)	Regulatory sandbox
Malta	Anticipatory regulation with advisory approach	FinTech Regulatory sandbox		Government/regulator (a), businesses (a), public bodies (a)	FinTech Regulatory sandbox
Saudi Arabia	Hard Law	Payment Service Provider Regulation		Government/regulators (a), businesses (p), citizens (p)	Payment Service Provider Regulation
Saudi Arabia	Anticipatory regulation with advisory approach	SAMA Regulatory Sandbox		Government/regulators (a), businesses (a), citizens (p)	SAMA Regulatory Sandbox
Singapore	Soft Law	Open API Playbook		Government/regulators (a), businesses (p)	Open API Playbook
Singapore	Hard Law	Payment Service Act		Government/ law enforcement/ regulators (a), citizens (p), businesses (p)	Payment Service Act
Singapore	Anticipatory regulation	Regulatory Sandbox		Government/regulator (a), businesses (a), public bodies (a), citizens (p)	Regulatory Sandbox
Singapore	Experimental regulation	Digital Banks		Government/regulator (a), industry (a), businesses (p), public bodies (a), citizens (p)	Digital Banks
South Africa	Anticipatory regulation	Regulatory Sandbox		Government/regulator (a), businesses (a), public bodies (a)	Regulatory Sandbox
South Korea	Anticipatory regulation	Sandbox Korea		Government/regulator (a), businesses (a), public bodies (a)	Sandbox Korea
South Korea	Hard Law	Electronic Financial Transactions Act		Government/regulator (a), businesses (a), public bodies (a)	Electronic Financial Transactions Act
South Korea	Anticipatory Regulation	Special regulation-free zone in Busan City on blockchain		Government/regulator (a), businesses (a), public bodies (a), citizens and residents (p)	Busan regulation-free zone
Spain	Hard Law	Law 7/2020, of 13 November, for the digital transformation of the financial system		Government/regulator (a), businesses (p), public bodies (p)	Ley 7/2020
Spain	Anticipatory regulation with advisory approach	SGTFI Regulatory sandbox		Government/regulator (a), businesses (a), public bodies (a)	SGTFI Regulatory sandbox
Switzerland	Hard Law	Financial Market Infrastructure Act		Government/regulators (a), businesses (p), industry (p), public sector (p), citizens (p)	Financial Market Infrastructure Act
Switzerland	Anticipatory regulation	FINMA regulatory sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a), individuals (a)	FINMA regulatory sandbox
Switzerland	Hard Law	Proposal for eID Act		Government/ law enforcement/ regulators (a), citizens (p), businesses (p)	Proposal for eID Act
The Netherlands	Anticipatory regulation with advisory approach	DNB, AFM and ACM's Innovation Hub		Government/regulators (a), businesses (a), industry (a), public sector (a)	Innovation Hub



UAE	Hard Law	Decretal Federal Law No. (14) of 2018 Regarding the Central Bank & Organization of Financial Institutions and Activities		Government/ law enforcement/ regulators (a), citizens (p), businesses (p)	Decretal Federal Law No. (14) of 2018 (e-money)
UAE	Soft Law	Guidelines for Financial Institutions Adopting Enabling Technologies		Government/ law enforcement/ regulators (a), industry (p), businesses (p)	Guidelines for Financial Institutions
UAE	Experimental regulation	Open Finance Lab		Government/ law enforcement/ regulators (a), industry (a), businesses (a), citizens (p)	Open Finance Lab
United Kingdom	Anticipatory regulation	FCA Regulatory Sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a)	FCA Regulatory Sandbox
United Kingdom	Anticipatory regulation	FCA Digital Sandbox		Government/regulators (a), businesses (a), technology providers (a), investors (a)	FCA Regulatory Sandbox
United States of America	Hard Law	Bank Security Act		Government/ law enforcement/ regulators (a), citizens (p), businesses (p)	Bank Security Act
United States of America	Anticipatory regulation	Arizona's Regulatory Sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a)	Arizona's Regulatory Sandbox
United States of America	Anticipatory regulation	Florida's Financial Technology Sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a)	Arizona's Regulatory Sandbox
United States of America	Anticipatory regulation	Digital Currency Innovation Lab		Government/regulators (a), businesses (a), industry (a), public sector (a)	Digital Currency Innovation Lab
United States of America	Anticipatory regulation	Financial and Insurance Regulatory Sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a)	Financial and Insurance Regulatory Sandbox
United States of America	Anticipatory regulation	Utah Office of Regulatory Relief		Government/regulators (a), businesses (a), industry (a), public sector (a)	Utah Office of Regulatory Relief
United States of America	Anticipatory regulation	FinTech Sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a)	FinTech Sandbox
United States of America	Anticipatory regulation	Financial Technology Sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a)	Financial Technology Sandbox
United States of America	Hard Law	Proposal for Responsible Financial Innovation Act		Government/regulators (a), businesses (p), citizens (p)	Proposal for Responsible Financial Innovation Act

Internet of Things (IoT)

Explanatory notes:

- The colour coding in column 'Status' indicates:
 - Yellow: under negotiations/ yet to enter into force or become applicable
 - Green: applicable/ published
 - Red: process paused/ceased
- The categories in column 'Stakeholders' follow the specific language of the instrument/organisation/ initiative. The additional indications represent:



- (a) – active stakeholder – having means for direct impact on the content of the regulatory instrument
- (p) – passive stakeholder – the regulatory instrument is directly targeting the stakeholder, without them having means for direct impact on the content of the regulatory instrument.

• The nature and broad application of the IoT technology makes it undesirable to regulate the technology as such. Thus, the regulatory tools focus on its application in various domains from cybersecurity to privacy and smart manufacturing. Due to feasibility considerations, the mapping is going to provide a selective pattern of various regulatory tools in different domain in selected jurisdictions without claiming exhaustiveness. The aim is to demonstrate the preferred tools, as well as to look for correlations and best practices across jurisdictions. It is also recognised that 5G/6G, cloud and IoT technologies, in particular have an overlapping and combine applications, therefore they might be simultaneously governed by one tool or in combination with the more distinctive legal regulations of AI and blockchain.

Jurisdiction	Type of regulation	Name	Status	Stakeholders (directly involved)	Source
EU	Hard Law	Directive 2014/53/EU of the European Parliament and of the Council of 16 April 2014 on the harmonisation of the laws of the Member States relating to the making available on the market of radio equipment		EU (a), national member states/governments/regulators (a), citizens (p), businesses (p) industry (p)	The Radio Directive
EU	Hard Law	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data		EU (a), national member states/governments/regulators (a), data subject (p), businesses (p) industry (p), controllers (p), processor (p)	GDPR
EU	Hard Law	Proposal for a Regulation of the European Parliament and of the Council on horizontal cybersecurity requirements for products with digital elements		EU (a), national governments (a), manufacturers (p), distributors and importers (p), economic operators (p), consumers (p), standardisation bodies (a), consumer protection organisations (p), academia (p)	Cyber Resilience Act
EU	Hard Law	Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification		EU (a), national governments (a), ENISA (a), OES (p), providers (p), citizens (p), certification bodies (a), businesses (p), academia (p)	Cybersecurity Act
EU	Hard Law	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union		EU (a), national governments (a), ENISA (a), OES (p), IPS (p), citizens (p), certification bodies (a), SDOs (a), academia (p), citizens (p), businesses (p)	NIS2 Directive
EU	Hard Law	Proposal for a Regulation of the European Parliament and the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem		EU (a), national governments (a), Chip manufacturers (p), Fabless chip companies (p), Equipment and materials suppliers (p), Research institutions and universities (p), industry (p), Trade Unions and Worker Representatives (p), investors (p)	The EU Chips Act



ENISA	Soft Law	Good Practices for Security of IoT - Secure Software Development Lifecycle		ENISA (a), industry (p), regulatory bodies (p), academia (p), standardisation bodies (p) IoT device users (p), investors and insurers (p)	Good Practices for Security of IoT
IEEE	Standards	IEEE 2413-2019 Standard for an Architectural Framework for the Internet of Things (IoT)		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2413-2019
IEEE	Standards	IEEE 3219-2023 Approved Draft Standard for Blockchain-based Zero-Trust Framework for Internet of Things (IoT)		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 3219-2023
ISO	Standards	ISO/IEC 30162:2022 Internet of Things (IoT) Compatibility requirements and model for devices within industrial IoT systems		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 30162:2022
ISO	Standards	ISO/IEC 27402:2023 Cybersecurity IoT security and privacy Device baseline requirements		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 27402:2023
ISO	Standards	ISO/IEC 30141:2018 Internet of Things (IoT) Reference Architecture		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 30141:2018
ISO	Standards	ISO/IEC 27400:2022 Cybersecurity IoT security and privacy Guidelines		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 27400:2022
ISO	Standards	ISO/IEC TR 30164:2020 Internet of things (IoT) Edge computing		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC TR 30164:2020
ISO	Standards	ISO/IEC TR 30166:2020 Internet of things (IoT) Industrial IoT		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC TR 30166:2020
ISO	Standards	ISO/IEC 30147:2021 Information technology Internet of things Methodology for trustworthiness of IoT system/service		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 30147:2021
ITU	Soft Law	ITU-T Q.4071 (12/2023) The testing of 3D ultra high density Internet of things networks		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Q.4071 (12/2023)
ITU	Soft Law	ITU-T Y.4491 (11/2023) Framework of blockchain-based self-organization networking in Internet of things environments		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.4491 (11/2023)
ITU	Soft Law	ITU-T Y.4494 (11/2023) Reference architecture of collaborative decentralized machine learning for intelligent Internet of things services		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.4494 (11/2023)
ITU	Soft Law	ITU-T Y.4604 (09/2023) Metadata for camera sensing information of autonomous mobile Internet of things devices		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.4604 (09/2023)



ITU	Soft Law	ITU-T Y.4223 (09/2023) Common requirements and capabilities of smart cities and communities from IoT and ICT perspectives		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.4223 (09/2023)
UNECE	Collaborative Tech Governance Initiative	Working Group contributing to hard law instruments		UNECE(a), international organisations (a), national governments (a), industry (p), consumer organisations (p), consumers (p)	Working group
UNECE	Soft Law	White Paper on IoT Standards for Trade Facilitation		UNECE(a), international organisations (a), national governments (a), industry (p)	IoT White Paper
UNIDO	Experimental regulation	Innovation Lab		UNIDO (a), international organisations (a), national governments (a), businesses (a), academia (a), citizens (a)	Innovation Lab
Bilateral Initiative	Collaborative Tech Governance Initiative	South Korea and Singapore's Memorandum of Understanding regarding the mutual recognition of Internet of Things (IoT) security certification systems.		South Korea (a), Singapore (a), industry (p)	MOU
Australia	Soft Law	Code of Practice: Securing the Internet of Things for Consumers (Code of Practice)		Government (a), consumers (p), manufacturers (p), retailers (p), cybersecurity researchers (p), academia (p), industry organisations (p)	Code of Practice
Belgium	Experimental Regulation	Cyber Green House		Government (a), businesses (a)	Cyber Green House
Brazil	Hard Law	Requisitos de segurança cibernética para equipamentos para telecomunicações		Government (a), IoT manufacturers (p), IoT suppliers (p), consumers (p)	Act nº 77, 5th of January 2021
Canada	Hard Law	Personal Information Protection and Electronic Documents Act (PIPEDA)		Government (a), IoT manufacturers (p), consumers (p)	PIPEDA
China	Hard Law	Guidelines for the Construction of IoT Basic Security Standard Systems		Government (a), IoT manufacturers (p)	IoT BSSS
Finland	Soft Law	Finish Cybersecurity Label		Government (a), IoT manufacturers (a)	Finish Cybersecurity Label
Germany	Soft Law	IT Security Label		Government (a), IoT manufacturers (a), individuals (p)	BSI IT-Security Label
India	Soft Law	Code of Practice for Securing Consumer Internet of Things (IoT)		Government (a) IoT device manufacturers (a), IoT service providers / system integrators (a), mobile application developers (a), retailers (a)	Code of Practice
Japan	Soft Law	IoT Security Safety Framework		Government (a), IoT manufacturers (a)	IoT Security Safety Framework
Saudia Arabia	Hard Law	Internet of Things Regulatory Framework		Government (a), IoT manufacturers (p), IoT service providers (p)	Internet of Things Regulatory Framework
Singapore	Soft Law	Cyber Security Agency of Singapore's Cybersecurity Labelling Scheme		Government (a), IoT manufacturers (a), consumers (p)	Cybersecurity Labelling Scheme
Singapore	Anticipatory Regulation	Smart University Living Lab		Government (a), industry (a), student (p), academia (a), educational institutions (a)	Living Lab



South Korea	Soft Law	Guidelines on automatic processing, IoT, and Privacy by Design		Government (a), data subjects (p), industry (a)	Guidelines
South Korea	Anticipatory Regulation	Special regulation-free zone in Sejong City on autonomous driving		Government/regulator (a), businesses (a), public bodies (a), citizens and residents (p)	Sejong regulation-free zone
South Korea	Hard Law	Personal Information Protection Act (PIPA)		Government/regulator (a), controllers (p), data subjects (p), public organisations (p)	PIPA
South Korea	Hard Law	Personal Information and Information Security Management System (ISMS-P).		Government/regulator (a), industries organisation (a), individuals (p), businesses (p)	ISMS-P
UAE	Anticipatory Regulation	IoT Framework (IoT Policy + IoT Procedures)		Government (a), telecommunication service providers (a), IoT service providers (a), users (p)	IoT Framework
United Kingdom	Soft Law	Code of Practice for Consumer IoT Security		Government (a), NCSC(a), consumers (p), manufacturers (p), IoT service providers (p), retailers (p), cybersecurity researchers (p), academia (p), industry organisations (p)	Code of Practice for Consumer IoT Security
United Kingdom	Hard Law	The Product Security and Telecommunications Infrastructure Bill		Government (a), IoT manufacturers (p), distributors (p), consumers (p)	PSTI (Secure by Design)
United Kingdom	Anticipatory regulation	FCA Regulatory Sandbox		Government/regulators (a), businesses (a), industry (a), public sector (a)	FCA Regulatory Sandbox
United States of America	Experimental regulation	PNNL's Power Networking, Equipment, and Technology (powerNET) testbed		Government (a), academia (a), business (a), industry (a), users (p)	powerNET
United States of America	Experimental regulation	Smart Manufacturing Systems (SMS) Test Bed		Government (a), academia (a), business (a), industry (a)	SMS Testbed
United States of America	Hard Law	IoT Cybersecurity Improvement Act		Government (a), industry (p), academia (p), consumer groups (p)	IoT Cybersecurity Improvement Act
United States of America	Hard Law	Health Insurance Portability and Accountability Act		Government (a), industry (p), academia (p), patient organisations (p), patients (p)	Health Insurance Portability and Accountability Act
United States of America	Hard Law	Children and Teens' Online Privacy Protection Act		Government (a), children/parents (p), online service operators (p), industry (p), data brokers and advertisers (p)	Children and Teens' Online Privacy Protection Act
United States of America	Hard Law	California Senate Bill 327 California Internet of Things (IoT) Security Law		Government (a), consumers (p), manufacturers (p), retailers (p), security researchers (p), industry associations (p)	California Internet of Things (IoT) Security Law
United States of America	Hard Law	California Senate Bill SB-327 California Consumer Privacy Act		Government (a), residents (p), businesses (p), data brokers (p), industry (p), industry academia (p)	California Consumer Privacy Act

Cloud Technology

Explanatory notes:

- The colour coding in column 'Status' indicates:



- Yellow: under negotiations/ yet to enter into force or become applicable
- Green: applicable/ published
- Red: process paused/ceased
- The categories in column 'Stakeholders' follow the specific language of the instrument/organisation/ initiative. The additional indications represent:
 - (a) – active stakeholder – having means for direct impact on the content of the regulatory instrument
 - (p) – passive stakeholder – the regulatory instrument is directly targeting the stakeholder, without them having means for direct impact on the content of the regulatory instrument.
- The nature and broad application of the cloud technology makes it undesirable to regulate the technology as such. Thus, the regulatory tools focus on its application in various domains from cybersecurity to privacy and healthcare. Due to feasibility considerations, the mapping is going to provide a selective pattern of various regulatory tools in different domain in selected jurisdictions without claiming exhaustiveness. The aim is to demonstrate the preferred tools, as well as to look for correlations and best practices across jurisdictions. It is also recognised that 5G/6G, cloud and IoT technologies, in particular have an overlapping and combine applications, therefore they might be simultaneously governed by one tool or in combination with the more distinctive legal regulations of AI and blockchain.

Jurisdiction	Type of regulation	Name	Status	Stakeholders (directly involved)	Source
EU	Hard Law	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data		EU (a), national member states/governments/regulators (a), citizens (p), businesses (p) industry (p)	GDPR
EU	Hard Law	Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector		EU (a), national member states/governments/regulators (a), gatekeeper platforms (p), business users (p) end users (p), civil society (p)	Digital Markets Act
EU	Hard Law	Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services		EU (a), national member states/governments/regulators (a), online intermediaries (p), users (p) industry (p), civil society (p), content creators (p), fact-checkers (p)	Digital Services Act
EU	Hard Law	Proposal for a Regulation of the European Parliament and the Council on harmonised rules on fair access to and use of data		EU (a), national member states/governments/regulators (a), data providers (p), data intermediaries (p) data users (p), data holders (p), cloud providers (p), standardisation organisations (p)	Data Act
EU	Hard Law	Regulation (EU) 2022/2554 of the European Parliament and		EU (a), national member states/governments/regulators (a), financial entities (p), CTSPs (p), IT	DORA



		of the Council of 14 December 2022 on digital operational resilience for the financial sector		vendors (p), consumers and investors (p), auditors (p)	
EU	Hard Law	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union		EU (a), national governments (a), ENISA (a), OES (p), IPS (p), citizens (p), certification bodies (a), SDOs (a), academia (p), citizens (p), businesses (p)	NIS2 Directive
ESMA	Soft Law	Guidelines on outsourcing to cloud service providers		EU/ESMA (a), national governments/regulators (a), financial institutions (a), CSPs (a)	ESMA Guidelines
European Banking Authority	Soft Law	Guidelines on outsourcing arrangements		EU/EBA (a), national governments/regulators (a), financial and banking institutions (p), industry (p)	Guidelines on outsourcing arrangements
IEEE	Standards	IEEE 2301-2020 Guide for Cloud Portability and Interoperability Profiles (CPIP)		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2301-2020
IEEE	Standards	IEEE 2302-2021 Standard for Intercloud Interoperability and Federation (SIIF)		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 2302-2021
ISO	Standards	ISO/IEC 19086-4:2019 Cloud computing Service level agreement (SLA) framework Part 4: Components of security and of protection of PII		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 19086-4:2019
ISO	Standards	ISO/IEC 27000:2018 Information technology Security techniques Information security management systems Overview and vocabulary		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 27000:2018
ISO	Standards	ISO/IEC 19831:2015 Cloud Infrastructure Management Interface (CIMI) Model and RESTful HTTP-based Protocol An Interface for Managing Cloud Infrastructure		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 19831:2015
ISO	Standards	ISO/IEC 5140:2024 Information technology Cloud computing Concepts for multi-cloud and the use of multiple cloud services		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 5140:2024
ISO	Standards	ISO/IEC 19941:2017 Information technology Cloud computing Interoperability and portability		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 19941:2017
ISO	Standards	ISO/IEC 23751:2022 Information technology Cloud computing and distributed platforms		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO/IEC 23751:2022



		Data sharing agreement (DSA) framework			
ITU	Soft Law	ITU-T H.431.1 (01/2024) Functional architecture for cloud virtual reality systems		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T H.431.1 (01/2024)
ITU	Soft Law	ITU-T Y.3540 (10/2023) Edge computing – Overview and high-level requirements		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.3540 (10/2023)
ITU	Soft Law	ITU-T Y.3550 (12/2023) Cloud computing – Requirements for artificial intelligence based cloud service development and operation management		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.3550 (12/2023)
ITU	Soft Law	ITU-T Q.5007 (12/2023) Signalling architecture for microservices based intelligent edge computing		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Q.5007 (12/2023)
ITU	Soft Law	ITU-T Y.3091 (12/2023) Digital twin network – Capability levels and evaluation methods		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.3091 (12/2023)
Public-Private Initiative	Experimental regulation	Common European Data spaces		EU (a), national states (a), industry (a), academia (a), data providers (a), CSPs (a), data intermediaries (a)	Common European Data spaces
SCOPE Europe endorsed by EDPB (Art 40 GDPR)	Soft Law	EU Cloud Code of Conduct		EU regulator (a), industry (a), civil society organisations (a), privacy advocates (p)	EU Cloud Code of Conduct
Public-private partnership	Collaborative Tech Governance Initiative	European Alliance for Industrial Data, Edge and Cloud		EU (a), member states (a), industry (a)	European Alliance for Industrial Data, Edge and Cloud
Public-private partnership	Experimental Regulation	Smart Highway		Antwerp (a), imec (a), industry (a), individuals (p), research organisations (p)	Smart Highway
Australia	Hard Law	Australian Prudential Regulation Authority ("APRA") Prudential Standards and Guidance		Government (a), industry (p), businesses (p), investors (p)	APRA Prudential Standard CPS 231 on Outsourcing
Brazil	Hard Law	Brazilian National Monetary Council Resolution No. 4,893, effective as of 26 February 2021		Government (a), industry (p), businesses (p), auditors (p), financial institutions (p)	Resolution No. 4,893
Canada	Soft Law	B-10 Outsourcing of Business Activities, Functions and Processes		Government/regulator (a), investors (p), consumers (p), auditors (p), trade associations (p), auditors (p), third-party service providers	OSFI B-10 Guidelines
Germany	Soft Law	Orientierungshilfe zu Auslagerungen an Cloud-Anbieter		Government/regulator (a), financial institutions (p), consumers (p), CSPs (p)	Guidance Note on Cloud Services
South Africa	Soft Law	South Africa National Data and Cloud Policy and Guidelines		Government (a), industry (p), businesses (p), individuals (p)	Cloud Policy Guidelines
Taiwan	Anticipatory Regulation	Regulatory sandbox for self-driving vehicles		Government/regulator (a), businesses (a), industry (a), individuals (p)	Regulatory sandbox for



					self-driving vehicles
United Kingdom	Hard Law	Data Protection Act 2018		Governments/regulators (a), data subject (p), businesses (p) industry (p), controllers (p), processor (p)	Data Protection Act 2018
United States of America	Experimental regulation	CLOUDLAB		Government (a), academia (a), business (a), industry (a)	CLOUDLAB
United States of America	Hard Law	Gramm-Leach-Bliley Act		Government/regulators (a), financial institutions (p), consumers (p), technology companies (p)	The Gramm-Leach-Bliley Act
United States of America	Experimental regulation	Cloud Enhanced Open Software Defined Mobile Wireless Testbed for City-Scale Deployment (COSMOS)		Government (a), municipalities (a), academia (a), business (a), industry (a)	COSMOS
United States of America	Experimental regulation	POWDER Testbed		Government (a), academia (a), business (a), industry (a), standard bodies (a), open-source organisations (a)	POWDER Testbed
United States of America	Standards	Federal Risk and Authorization Management Program (FedRAMP)		Government (a), governmental agencies (a), CSP (p)	FedRAMP
United States of America	Hard Law	US CLOUD Act (H.R.4943)		Government/ law enforcement (a), business (p), data subjects (p) foreign governments (p), technology companies (p)	CLOUD Act

5G/6G Technology

Explanatory notes:

- The colour coding in column 'Status' indicates:
 - Yellow: under negotiations/ yet to enter into force or become applicable
 - Green: applicable/ published
 - Red: process paused/ceased
- The categories in column 'Stakeholders' follow the specific language of the instrument/organisation/ initiative. The additional indications represent:
 - (a) – active stakeholder – having means for direct impact on the content of the regulatory instrument
 - (p) – passive stakeholder – the regulatory instrument is directly targeting the stakeholder, without them having means for direct impact on the content of the regulatory instrument.

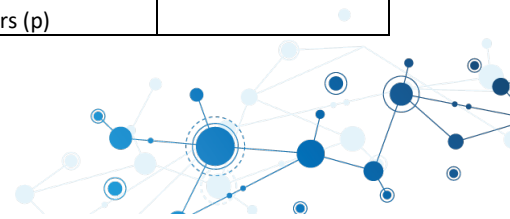
This division is done without prejudice to the specific stakeholders' division, existing in the 5G/6G ecosystem (customer/consumer, Telecom sector, DCSP, Connected devices industry, cybersecurity assessment, cybersecurity information exchange, SDOs and research and innovation organisations)

- The nature and broad application of the 5G/6G technology makes it undesirable to regulate the technology as such. Thus, the regulatory tools focus on its application in various domains from cybersecurity to privacy and healthcare. Due to feasibility considerations, the mapping is going to provide a selective pattern of various regulatory tools in different domain in selected jurisdictions without claiming exhaustiveness. The aim is to demonstrate the preferred tools, as well as to look for correlations and best practices across jurisdictions. It is also recognised that 5G/6G, cloud and IoT technologies, in particular have an overlapping and combine applications, therefore they might be



simultaneously governed by one tool or in combination with the more distinctive legal regulations of AI and blockchain.

Jurisdiction	Type of regulation	Name	Status	Stakeholders (directly involved)	Source
EU	Hard Law	Directive (EU) 2018/1972 of the European Parliament and of the Council of 11 December 2018 establishing the European Electronic Communications Code		EU (a), national member states/governments/regulators (a), individuals (p), businesses (p)	Electronic Communications Code
EU	Hard Law	Regulation (EU) 2015/2120 of the European Parliament and of the Council of 25 November 2015 laying down measures concerning open internet access		EU (a), national member states/governments/regulators (a), end-users (p), ISPs (p), CAPs (p), OTT (p)	Open Internet Access Regulation
EU	Hard Law	Directive 2014/61/EU of the European Parliament and of the Council of 15 May 2014 on measures to reduce the cost of deploying high-speed electronic communications networks		EU (a), national member states/governments/regulators (a), ECOs (p), citizens (p), businesses (p), technology providers and manufacturers (p)	BCR Directive
EU	Hard Law	Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union		EU (a), national governments (a), ENISA (a), OES (p), IPS (p), citizens (p), certification bodies (a), SDOs (a), academia (p), citizens (p), businesses (p)	NIS2 Directive
EU	Hard Law	Proposal for a Regulation of the European Parliament and the Council on measures to reduce the cost of deploying gigabit electronic communications networks		EU (a), national governments (a), ECOs (p), Investors and Financial Institutions (p), Civil Society Organizations and Consumer Groups (p), Technology Providers and Equipment Manufacturers (p)	The Gigabit Infrastructure Act Proposal
EU	Hard Law	Proposal for a Regulation of the European Parliament and the Council establishing a framework of measures for strengthening Europe's semiconductor ecosystem		EU (a), national governments (a), Chip manufacturers (p), Fabless chip companies (p), Equipment and materials suppliers (p), Research institutions and universities (p), industry (p), Trade Unions and Worker Representatives (p), investors (p)	The EU Chips Act
EU	Soft Law	Commission Recommendation of 26.03.2019 Cybersecurity of 5G Networks		EU (a), EU Member States (a), Telecommunication operators (p), equipment vendors (p), citizens and business (p)	Commission Recommendation
EU	Soft Law	Cybersecurity of 5G networks EU Toolbox of risk mitigating measures		EU (a), EU Member States (a), Mobile network operators (p), telecom equipment manufacturers (p), end users (p)	5G Toolbox



IEEE	Standards	IEEE 1930.1-2022 Recommended Practice for Software-Defined Networking (SDN) Based Middleware for Control and Management of Wireless Networks		ISO (a), national governments (p), international organisations (a), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	IEEE 1930.1-2022
IEE	Experimental regulation	IEEE 5G/6G Innovation Testbed		IEEE (a), (a), telecommunications operators (a), equipment vendors (a), application developers (a), academia (p)	IEEE 5G/6G Innovation Testbed
ISO	Standards	ISO 37184:2023 Sustainable mobility and transportation Framework for transportation services by providing meshes for 5G communication		ISO (a), national governments (p), businesses (p), researchers (p), CSOs (p), consumers (p), investors (p), educational institutions (p)	ISO 37184:2023
ITU	Soft Law	ITU-T L.1391 (01/2024) Specification of 5G network sharing and co-construction adapting to climate change mitigation		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T L.1391 (01/2024)
ITU	Soft Law	ITU-T F.780.5 (01/2024) Requirements, reference framework and use cases for telemonitoring systems in rapid deployment hospitals		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T F.780.5 (01/2024)
ITU	Soft Law	ITU-T Q.5007 (12/2023) Signalling architecture for microservices based intelligent edge computing		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Q.5007 (12/2023)
ITU	Soft Law	ITU-T F.740.6 (09/2023) Reference framework and requirements for Internet protocol multimedia subsystem early media and extension service system		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T F.740.6 (09/2023)
ITU	Soft Law	ITU-T X.1817 (09/2023) Security requirements for 5G messaging service		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T X.1817 (09/2023)
ITU	Soft Law	ITU-T Y.3128 (12/2023) Requirements for network function communication between public networks and public network integrated non-public networks in IMT-2020		ITU (a), national states (a), industry (p), businesses (p), academia (p)	ITU-T Y.3128 (12/2023)
ARIB, ATIS, CCSA, ETSI, TSDSI, TTA & TTC	Standards	The 3rd Generation Partnership Project (3GPP)		Standardisation bodies (a), market representation partners (a), observers (p)	3GPP
Public-Private Partnership	Collaborative Tech Governance Initiative	Smart Networks and Services Joint Undertaking (SNS JU)		EU (a), 6GIA (a), industry (a), national regulators (p), standardisation bodies (p), investors (p)	SNS JU
Australia	Hard Law	Governmental 5G security guidance to carriers		Government/ regulator (a), carriers (p), industry (p)	5G Security Guidelines



Austria	Hard Law	Telecommunication Act 2021		Government/regulator (a), telecommunication operators (p), content providers and applications developers (p), consumer and users' organisations (p), investors (p)	Telecommunication Act 2021
Austria	Hard Law	TKK Draft Decision on broadband expansion		Government/regulator (a), telecommunication operators (p), industry (p), consumers (p)	Draft Decision on broadband expansion
Austria	Hard Law	Telekom- Network Security Ordinance 2020 (TK-NSiV 2020)		Government/regulator (a) operators of electronic communications networks(p), providers of electronic communications services (p) industry (p), consumers (p)	TK-NSiV 2020
Belgium	Hard Law	Loi portant transposition du code des communications électroniques européen et modification de diverses dispositions en matière de communications électroniques		Government/regulator (a), businesses (p), individuals (p)	Act C – 2021/43554
Belgium	Hard Law	Arrêté royal concernant l'accès radioélectrique dans la bande de fréquences 1427-1517 MHz		Government/regulator (a), mobile operators (p), individuals (p)	Royal Decree 1400 MHz
Belgium	Hard Law	Arrêté royal concernant l'accès radioélectrique dans la bande de fréquences 3400-3800 MHz		Government/regulator (a), mobile operators (p), individuals (p)	Royal Decree 3600 MHz
Belgium	Hard Law	Arrêté royal concernant l'accès radioélectrique dans la bande de fréquences 700 MHz		Government/regulator (a), mobile operators (p), individuals (p)	Royal Decree 700 MHz
Belgium	Hard Law	Arrêté royal concernant l'accès radioélectrique dans les bandes de fréquences 900 MHz, 1800 MHz et 2 GHz		Government/regulator (a), mobile operators (p), individuals (p)	Royal Decree 2G3G
Brazil	Experimental Regulation	Open Lab 5G WEG-V2COM project		Government/ regulator (a), WEG (a), TPSs (a), manufacturers (a), technology providers (a)	Open Lab 5G WEG-V2COM project
Canada	Hard Law	Critical Cyber Systems Protection Act (Bill C-26)		Government/ regulator (a), designated operators (p), cybersecurity providers (p), NCSC (p), consumer and privacy advocacy groups (p)	Bill C-26
China	Experimental Regulation	5G+ Industrial Internet Public Service Platform		Government/regulator/municipal authorities (a), industry (a), academia (p), industry professionals (p)	5G+ Industrial Internet Public Service Platform
Czech Republic	Hard Law	The Recommendation for assessing the trustworthiness of technology suppliers of 5G networks		Government/ regulator (a), designated operators (p), cybersecurity providers (p), NCSC (p)	The Recommendation
France	Hard Law	Loi n° 2019-810 du 1er août 2019 visant à		Government/ regulator (a), designated operators (p),	The 5G Law



		préserver les intérêts de la défense et de la sécurité nationale de la France dans le cadre de l'exploitation des réseaux radioélectriques mobiles		cybersecurity providers (p), NCSC (p)	
Germany	Hard Law	Catalogue of security requirements for the operation of telecommunications and data processing systems and for processing personal data		Government/ regulator (a) operators of telecommunications networks and data processing systems (p), public telecommunications networks (p), providers of services with a high level of risk (p)	Catalogue of security requirements
India	Experimental regulation	Indigenous 5G Test Bed		Government/ regulator (a), recognised start-ups and MSME (a) Industry (a) Academia (a) Service Providers (a) R&D (a) Equipment Manufacturers (a)	Indigenous 5G Test Bed
Italy	Hard Law	Resolution No. 231/18/CONS		Government/ regulator (a), mobile network operators (p), equipment manufacturers (p)	Resolution No. 231/18/CONS
Italy	Hard Law	Decreto Legge 1 marzo 2022, n. 21 Misure urgenti per contrastare gli effetti economici e umanitari della crisi ucraina		Government/ regulator (a), designated operators (p), cybersecurity providers (p), NCSC (p)	Law-Decree No. 21/2022
Japan	Hard Law	Radio Act		Government/ regulator (a), telecommunication operators (p), broadcasting stations (p), radio equipment manufacturers and developers (p)	Radio Act
Japan	Soft Law	Ministry of Internal Affairs and Communications IoT 5G comprehensive security measures		Government/ regulator (a), manufacturers (p), telecommunication carriers (p), service providers (p), testing and certification bodies	The Measures
South Korea	Hard Law	Telecommunications Business Act		Government/ regulator (a), telecommunication business operators (p), users (p), manufacturers (p), investors (p)	Telecommunication Business Act
Spain	Hard Law	Ley 11/2022, de 28 de junio, General de Telecomunicaciones.		Government/ regulator (a), telecommunication operators (p), users (p), infrastructure providers (p), manufacturers (p)	The General Telecommunication Law
Spain	Hard Law	Real Decreto-ley 7/2022, de 29 de marzo, sobre requisitos para garantizar la seguridad de las redes y servicios de comunicaciones electrónicas de quinta generación.		Government/ regulator (a), telecommunication operators (p), users (p), infrastructure providers (p), cybersecurity solution providers (p)	Royal Decree-Law 7/2022 to guarantee secure 5G electronic communications networks and services
Taiwan	Anticipatory regulation				
The Netherlands	Hard Law	Telecommunications Act		Government/regulator (a), mobile operators (p), individuals (p)	Telecommunications Act



The Netherlands	Hard Law	Regeling aanvraag- en veilingprocedure vergunningen 700, 1400 en 2100 MHz		Government/regulator (a), mobile operators (p), individuals (p)	Regulations on the application and auction procedure for 700, 1400 and 2100 MHz licences
The Netherlands	Hard Law	Guidelines for sharing of mobile networks		Government/regulator (a), mobile operators (p), individuals (p)	Guidelines for sharing of mobile networks
United Kingdom	Hard Law	Monitoring and enforcement programme: General Condition 9 (requirement to offer contracts with minimum terms)		Government/regulator (a), communication providers (p), consumers (p), businesses (p), industry (p)	General Condition 9
United Kingdom	Experimental Regulation	The 5G Testbeds and Trials Programme (5GTT)		Government/regulator (a), project consortia (a), mobile network operators (a), technology providers (a), end users (p), academia (a)	5GTT
United States of America	Experimental regulation	Aerial Experimentation and Research Platform for Advanced Wireless (ERPAW)		Government (a), municipalities (a), academia (a), business (a), industry (a)	ERPAW
United States of America	Experimental regulation	POWDER Testbed		Government (a), academia (a), business (a), industry (a), standard bodies (a), open-source organisations (a)	POWDER Testbed

