Digital Society (2024) 3:59
https://doi.org/10.1007/s44206-024-00146-7

ORIGINAL PAPER

Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models

Samuele Fratini[1,2,3] · **Emmie Hine**[4,5,7] · **Claudio Novelli**[4,7] · **Huw Roberts**[6] · **Luciano Floridi**[4,7]

Received: 8 May 2024 / Accepted: 24 October 2024

Abstract
Digital sovereignty is a popular yet still emerging concept. It is claimed by and related to various global actors, whose narratives are often competing and mutually inconsistent. This article offers a mapping of the types of national digital sovereignty that are emerging, while testing their effectiveness in response to radical changes and challenges. To do this, we systematically analyse a corpus of 271 peer-reviewed articles to identify descriptive features (*how* digital sovereignty is pursued) and value features (*why* digital sovereignty is pursued), which we use to produce four models: the *rights-based model, market-oriented model, centralisation model*, and *state-based model*. We evaluate their effectiveness within a framework of *robust governance* that accounts for the models' ability to absorb the disruptions caused by technological advancements, geopolitical changes, and evolving societal norms. We find that none of the models fully combine comprehensive regulation of digital technologies with a sufficient degree of responsiveness to fast-paced technological innovation and social and economic shifts. This paper's analysis offers valuable lessons to policymakers who wish to implement an effective and robust form of digital sovereignty.

Keywords Digital sovereignty · Data sovereignty · International relations · Robust governance · Turbulence

1 Introduction

Digital sovereignty and its variants have become a topic of increasing interest to policymakers across jurisdictions, particularly over the past ten years (Roberts et al., 2021). Early pioneers of the concept, like China, emphasised the importance of states' sovereign control over content "in" cyberspace (Creemers, 2020), while oth-

Extended author information available on the last page of the article

Published online: 14 November 2024

ers, like the European Union[1] (EU), have used industrial policy and digital regulation in the name of protecting fundamental rights (Farrand & Carrapico, 2022). Episodes like the Snowden revelations or the COVID-19 pandemic were "catalytic events" that provoked the diffused implementation of measures related to digital sovereignty by a variety of other countries (Thumfart, 2021). Since the diffusion of digital sovereignty processes has concerned different kinds of societies, diverse versions of the phenomenon have emerged.

Existing literature has delineated and categorised digital sovereignty to create different typologies (Roberts, 2024). Some scholars have distinguished between digital sovereignty and related terms like cyber sovereignty, information sovereignty, and data sovereignty (Hummel et al., 2021). Others have focused on the *type* of actors who make claims over digital sovereignty, including governments, private sector actors, and citizen groups (Couture & Toupin, 2019; Tretter, 2023). A third approach is distinguishing between different state models of digital sovereignty, such as the differences in approaches taken by China, the European Union, and the United States (Chander & Sun, 2021; Roberts et al., 2023).

These approaches help clarify conceptual differences between digital sovereignty and related terms, and support understanding of how digital sovereignty is being enacted, and competed for, by different actors. In this paper, we take an alternative approach focused on assessing the effectiveness of various models of digital sovereignty. Distinguishing between digital sovereignty and related terms, like cyber sovereignty, is helpful for analytical precision, but unhelpful for a normative analysis focused on what a good model for digital sovereignty should look like. Similarly, understanding the different actors asserting control over digital technologies is useful for considering what a successful model for state digital sovereignty may be, but it does not provide models that can be compared and assessed. Since this article's aim is to produce a descriptive and critical account of how existing forms of digital sovereignty are articulated to inform both scholars and policymakers, and because the literature describes what policies governments are implementing, scientific articles on how states are currently enacting digital sovereignty are the most promising sources for this paper. However, it should be acknowledged that collected materials provide an effective portrait of the academic debate on and existing landscape of digital sovereignty policies, but that incongruencies between scholarly analyses and implemented policy do exist. What we produce is a set of abstract models derived from the academic analysis of a state-level phenomenon; it is not an analysis of primary sources. Furthermore, we argue that simply focusing on comparing how a handful of actors are presently enacting digital sovereignty would mean falling into an is-ought trap. We overcome this last limitation by systematically including every existing country mentioned in the literature.

[1] We recognize the difficulties with applying the concept of digital sovereignty to the EU, which does not constitute a sovereign state. For this reason, we accept the consideration advanced in Bellanova et al. (2022) that "sovereignty is an unfulfilled political goal, insofar it is never truly absolute nor undisputed. […] But it is a claim that comes with consequences since actors shape a given social order according to their normative worldviews". The EU is thus included as an agent of digital sovereignty because the concept has a primary role in guiding both policymaking and infrastructural practices of the Union.

Against this background, our analysis transitions towards the mapping and normative evaluation of existing digital sovereignty models. While the descriptive section provides an updated review of the forms of digital sovereignty presented in the literature, the normative section is structured on the paradigm of *robust* governance as the evaluative perspective (Ansell et al., 2023, 2024; Ansell & Trondal, 2018) which embodies a diachronic dimension of (good) governance. This approach highlights the critical ability of governance models to effectively respond and adjust to the challenges and changes (i.e., the turbulences) unique to the digital realm.

2 Methodology

Given the above, a new typology of digital sovereignty models needs to be developed to achieve the aims of this paper. Our approach maps idealised types of digital sovereignty (Scott & Marshall, 2015). That is to say, we are interested in mapping "types" of digital sovereignty states are enacting, without focusing on the approach being taken by any single state. There are several reasons to adopt such a state-based high-level approach: firstly, this level of abstraction is appropriate as it ensures models are grounded in real practices, without limiting what "good" can look like to the practices of a single state. Secondly, existing literature on digital sovereignty has predominantly adopted nation-states as the main units of analysis, because they are regarded as the subjects exerting a kind of "traditional" sovereignty based on legitimacy (Roberts, 2024). Prominent works categorise forms of digital sovereignty based on state entities (e.g. Bradford, 2023). For this reason, we expected to find a vibrant academic debate based on state agency.

A state-centric approach also has limitations. In particular, sovereignty as the supreme authority of the state has always been more of a normative claim (though with its performative effects), rather than a fact. Adopting the state as the sole unit of analysis risks overlooking the role played by other relevant actors in enhancing or limiting state control, such as individuals (Fratini & Musiani, 2024), indigenous communities (Walter et al., 2020), civil society groups (Haché, 2014), and technology designers (Musiani, 2022) Nevertheless—even considering these limitations—socio-political systems are characterized by power relations and a prevailing party, which is usually the dominant political and cultural group governing the state.

To develop these models, we undertake a literature review focused on how states enact digital sovereignty. For every UN-recognised country, we used the Google Scholar advanced search function to search for <COUNTRY> with the exact phrase "cyber sovereignty" OR "data sovereignty" OR "digital sovereignty" OR "Internet sovereignty" OR "network sovereignty" with the date range of 2014–2024 (inclusive). 2014 was selected as the starting point because it is the year after the Snowden Revelations, which sparked a general demand for a "digital sphere that allows for exclusive national control over communications, data, and regulation" (Pohle & Thiel, 2020). Our inclusion criteria were:

- Written in English;
- Peer-reviewed journal contribution;

- Describes digital sovereignty practices directly associated with the actions of state entities.

Manual title and abstract screening filtered out items that did not meet the inclusion criteria, duplicates, and items with missing full text. Screening proceeded until theoretical saturation, understood in the pragmatic sense of Low (2019), was reached. Simply put, we stopped data collection, where our understanding of a country's digital sovereignty was not becoming more nuanced based on the topics of new articles (Hennink et al., 2017). The number of results by country and the number of results remaining after screening is shown in the Annex.

Following the literature gathering, we coded papers and reports to identify key features of the different states' approaches to digital sovereignty. Then, we grouped these into ideal types based on similar features. Following this article's descriptive and normative goals, we used a two-pronged approach combining descriptive coding of passages with values coding (Saldaña, 2014). Descriptive coding labelled passages with a feature of digital sovereignty, while values coding labelled passages with a value or a goal being promoted by the actor, such as privacy or national security. This process produced 19 descriptive features and 8 value features, which were used to inductively build ideal types based on similar features and to capture, in full, single digital sovereignty instances found in the literature. We looked for shared features, paying particular attention to unique ones that showed distinctive approaches to digital sovereignty, and clustered countries into models based on these features. To produce the models, value codes were used as the building blocks, for the normative and political goals towards which undertaken efforts are oriented. Values codes were combined with the aim to capture all the countries for which data collection has provided an adequately detailed profile while keeping the number of models few enough to be informative. Thus, we prioritized full coverage over mutual exclusivity. As is to be expected from the construction of ideal types, several countries displayed hybrid characteristics, which we note in our model analysis. Descriptive codes delineate how certain objectives related to state control are achieved and contribute to our later analysis. From this process, we identified four distinct approaches to digital sovereignty, shown in Table 1.

It should be noted that this study was limited to English-language results and academic literature, which thus excluded primary documents published only in some countries' official languages and restricts results to countries that the literature has focused on. We acknowledge that to assess the full context of culturally specific manifestations of digital sovereignty would require document collection in multiple languages (Thumfart, 2021). We outline some possible future lines of research opened by the limitations of the present study. It is also limited to only websites and documents indexed in Google Scholar. Furthermore, while we uncovered documents related to 191 countries, the lack of relevant documents on some countries means that specific countries' digital sovereignty approaches may have been under- or mischaracterised. For this reason, we integrated some relevant academic literature, policy materials, and journal pieces into our empirical corpus to offer a more complete presentation of the models (Table 2).

Table 1 Construction of models from codes

Value codes	Rights-based	State-based	Centralisation	Market-oriented
National security		X	X	X
Digital self-sufficiency		X	X	
State expansionism				X
Fundamental rights	X			
Market-rights balance	X			X
State sovereignty over corporations	X		X	
Territorialization of cyberspace		X	X	
Nationalised governance		X		
Descriptive codes	**Rights-based**	**State-based**	**Centralisation**	**Market-oriented**
Constraining corporate power	X		X	
Supporting domestic corporations		X	X	X
Stimulating digital innovation	X	X	X	X
Regulating digital innovation	X	X	X	
Enhancing national digital competencies	X	X	X	X
Re-negotiating existing standards and norms		X	X	
Supporting existing standards and norms	X			X
Exerting control over public and private data	X	X	X	X
Reinforcing and securing infrastructures	X	X	X	X
Regulating digital contents	X	X	X	
Influencing or damaging foreign countries		X	X	X
Digitization of the public administration and corporate processes	X	X	X	X
Centralising digital regulation			X	
Enforcing individual digital rights	X			
Enhancing military power		X	X	X
Enhancing defence against cybercrime	X	X	X	X
Influencing domestic public opinion		X	X	
Enhancing national interoperability and data circulation	X	X	X	
Banning corporations, technologies, and contents		X	X	

"X" indicates inclusion

Upon collecting this literature and delineating the main digital sovereignty models for descriptive analysis, our next step was to assess these models against a normative governance ideal, specifically robust governance, i.e., a governance model capable of addressing turbulence should withstand various conditions and adapt over time, maintaining stability amidst change (Ansell et al., 2023, 2024; Howlett et al., 2018; Pot et al., 2023; Scognamiglio et al., 2023). This governance framework was chosen due to its focus on addressing changes, demands, and support in unpredictable circumstances. Data collection and analysis suggested that ensuring a fair balance

Table 2 Collected documents by country

Country	Number of initial results	Results post-screening
Afghanistan	30	9
Albania	19	7
Algeria	3	1
Andorra	1	0
Angola	11	2
Antigua and Barbuda	0	0
Argentina	24	9
Armenia	10	2
Australia	28	12
Austria	6	1
Azerbaijan	3	1
Bahamas	0	0
Bahrain	0	0
Bangladesh	2	0
Barbados	0	0
Belarus	9	3
Belgium	1	1
Belize	0	0
Benin	4	2
Bhutan	0	0
Bolivia	7	5
Bosnia and Herzegovina	0	0
Botswana	0	0
Brazil	14	4
Brunei	0	0
Bulgaria	0	0
Burkina Faso	1	0
Burundi	1	1
Cabo Verde	0	0
Cambodia	0	0
Cameroon	1	0
Canada	3	0
Central African Republic	1	0
Chad	1	0
Chile	3	1
China	46	23
Colombia	3	0
Comoros	0	0
Congo	1	0
Costa Rica	1	0
Côte D'Ivoire	0	0
Croatia	3	1
Cuba	1	0
Cyprus	1	0
Czechia	1	0
Democratic People's Republic of Korea	2	1
Democratic Republic of the Congo	1	0

Table 2 (continued)

Country	Number of initial results	Results post-screening
Denmark	2	1
Djibouti	0	0
Dominica	0	0
Dominican Republic	0	0
Ecuador	2	1
Egypt	0	0
El Salvador	1	0
Equatorial Guinea	0	0
Eritrea	1	1
Estonia	4	3
Eswatini	0	0
Ethiopia	6	3
Fiji	0	0
Finland	2	0
France	20	13
Gabon	0	0
Gambia	0	0
Georgia	0	0
Germany	9	3
Ghana	0	0
Greece	2	0
Grenada	0	0
Guatemala	1	0
Guinea	1	0
Guinea Bissau	0	0
Guyana	1	0
Haiti	0	0
Honduras	1	0
Hungary	2	0
Iceland	2	1
India	5	4
Indonesia	11	8
Iran	8	5
Iraq	1	0
Ireland	4	0
Israel	2	3
Italy	9	2
Jamaica	0	0
Japan	5	4
Jordan	0	0
Kazakhstan	0	0
Kenya	5	1
Kiribati	3	1
Kuwait	8	6
Kyrgyzstan	1	0
Lao(s)	8	6
Latvia	2	0

Table 2 (continued)

Country	Number of initial results	Results post-screening
Lebanon	8	4
Lesotho	3	0
Libya	6	5
Liechtenstein	0	0
Lithuania	3	0
Luxembourg	2	0
Madagascar	1	0
Malawi	4	2
Malaysia	6	1
Maldives	12	8
Mali	13	8
Malta	2	0
Marshall Islands	1	0
Mauritania	1	1
Mauritius	0	0
Mexico	1	0
Micronesia	1	0
Monaco	1	0
Mongolia	5	3
Montenegro	0	0
Mozambique	0	0
Myanmar	4	1
Namibia	4	0
Nauru	6	4
Nepal	4	4
Netherlands	8	3
New Zealand	9	3
Nicaragua	0	0
Niger	3	0
Nigeria	8	3
North Macedonia	5	4
Norway	4	0
Oman	0	0
Pakistan	9	5
Palau	6	3
Panama	5	3
Papua New Guinea	4	0
Paraguay	9	3
Peru	5	2
Philippines	9	2
Poland	9	4
Portugal	5	1
Qatar	7	0
Republic of Korea	6	3
Republic of Moldova	3	0
Romania	4	0
Russian Federation	47	3

Table 2 (continued)

Country	Number of initial results	Results post-screening
Rwanda	7	0
Saint Kitts and Nevis	1	1
Saint Lucia	1	1
Saint Vincent and the Grenadines	0	0
Samoa	0	0
San Marino	0	0
Sao Tome and Principe	0	0
Saudi Arabia	7	1
Senegal	6	0
Serbia	11	5
Seychelles	5	2
Sierra Leone	0	0
Singapore	12	2
Slovakia	10	0
Slovenia	9	0
Solomon Islands	0	0
Somalia	4	0
South Africa	7	0
South Sudan	0	0
Spain	15	2
Sri Lanka	0	0
Sudan	8	1
Suriname	2	0
Sweden	18	1
Switzerland	1	0
Syrian Arab Republic	0	0
Tajikistan	2	0
Thailand	2	1
Timor Leste	0	0
Togo	1	0
Tonga	0	0
Trinidad and Tobago	0	0
Tunisia	5	3
Turkey/Türkiye	11	5
Turkmenistan	10	5
Tuvalu	0	0
Uganda	6	1
Ukraine	20	3
United Arab Emirates	4	1
United Kingdom	27	0
United Republic of Tanzania	6	0
United States of America	32	0
Uruguay	9	0
Uzbekistan	5	0
Vanuatu	1	0
Venezuela	5	0
Yemen	6	1

Table 2 (continued)

Country	Number of initial results	Results post-screening
Zambia	3	0
Zimbabwe	7	0
Total	911	271

between short-term adaptability and long-term stability of state control over digital infrastructure is a pressing concern. In particular, our collected material often presents the tension between fast-paced technological development (usually vested with corporate disruptive ethos) and slow-paced state regulation as a major impediment to the achievement of said balance. Academic literature seems thus to call for digital governance solutions that are sustainable in the long run. Our analysis concludes by examining how closely the four models outlined in Sect. 3—or elements thereof—align with the principles of robust governance.

3 Digital Sovereignty Models

Based on combinations of values and descriptive codes, we constructed four models of digital sovereignty. These models are defined by their descriptive characteristics and the values and goals they pursue. In the following section, we outline the values and the goals shaping each model, and for each, we show existing measures to attain them—as captured by our descriptive codes—in italics. It must be made clear that since we deal with ideal types, the same country may enact measures that fall into different models. For instance, the EU's provisions tend to fit the rights-based model, but it is increasingly resorting to security as the main reason to limit the reach of Chinese companies such as Huawei within the internal market. Figure 1 shows the model categorisation for countries with sufficient data to classify.

3.1 Rights-Based Model

The rights-based model is characterised by the framing of digital regulation as a means of strengthening fundamental and democratic rights, the attempt to find a good balance between rights and market benefits, and a resolute regulatory approach to private companies. The ultimate objective of this model is the reinforcement and introduction of rights for citizens in the digital space. Although the model provides for several measures aimed at asserting state sovereignty over digital corporations, state control is understood as a means to an end, i.e., the possibility for citizens to act freely in the digital sphere. This is frequently labelled as autonomy, empowerment, and user sovereignty.

3.1.1 Fundamental Rights

Some provisions emblematic of this model are often linked with users' control over their data, thus emphasising data sovereignty and *asserting control over data* as significant components of this model. The EU GDPR is perhaps the most well-known.

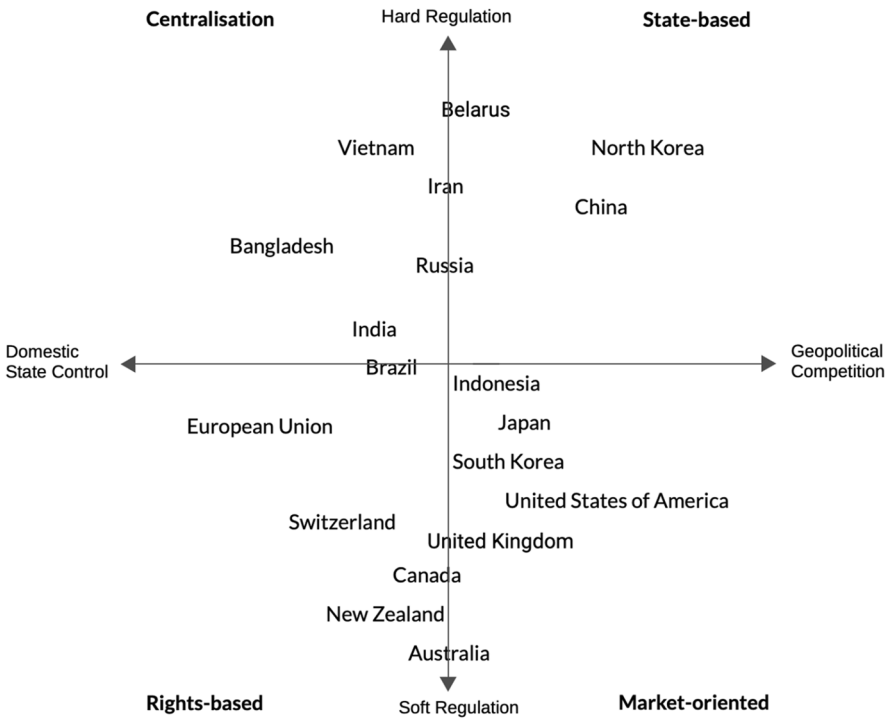

Fig. 1 Countries by model membership. The vertical axis captures the degree of assertiveness of state regulation, the horizontal axis distinguishes states whose objective is to design and enforce internal regulation from those that regulate digital technologies intending to advance their geopolitical interests

While this regulation aims to match market benefits with users' rights, its main objective is to give citizens the right to control the data they generate online (Herian, 2020). Protecting fundamental rights is also the cornerstone on which the risk assessment in the AI Act is developed (Novelli et al., 2023). Another significant example of *enforcing individual digital rights* is the referendum held on 18 June 2023 in the Geneva Canton, where people agreed on including the right to digital integrity in the Cantonal Constitution. While the new right includes some milestones regarding user data protection (the right to be forgotten, the right to life offline, and protection against abusive processing of personal data) and is in line with the Swiss privacy-centric narrative (Fratini, 2024), it is framed as a step forward for "the development of digital sovereignty in Switzerland".[2] Finally, similar measures can be oriented towards marginalised communities, such as those provisions labelled "indigenous data sovereignty" that are especially identified in Australia, Canada, New Zealand, and the US (Walter et al., 2020). These measures try to strengthen the control of marginalised indigenous communities over the data they generate by *enhancing national digital competencies* and *reinforcing and securing infrastructures*.

[2] See https://c4dt.epfl.ch/geneva-digital-sovereignty/.

3.1.2 Market-Rights Balance

This model tries to pair individual data protection with *enhanced interoperability and data circulation* to maximise market benefits while keeping individual rights untouched. However, in the case of the European Union, this proved effective for the internal market, where the GDPR prescribes the free circulation of data among EU Member States. In the case of international data transfer, circulation is significantly impeded by the stringent privacy adequacy mechanism of the EU (Chander & Schwartz, 2023). In this and other cases, the quest for privacy and digital integrity results in data localisation measures that are likely to have significant risks for EU companies themselves (Christakis, 2023).

3.1.3 State Sovereignty Over Corporations

Data sovereignty measures are not the only efforts deployed to ensure user sovereignty in the digital space. A significant portion of the effort relates to *constraining platform power* and gaining independence from large digital corporations, which are usually foreign companies. Industrial policy and infrastructure building are other ways to reinforce and make private actors redundant. An important example is the GAIA-X project in the EU, whose declared objective is to create a federated secure data infrastructure for Europe to compete with the most powerful US and Chinese players in the cloud market (Monsees & Lambach, 2022). A similar initiative is the development of a Swiss cloud to store public administration data and advance Swiss sovereignty. However, both projects ended up involving US and Chinese players or their European subsidiaries, signalling the difficulty of pursuing the digital autonomy of citizens and states without a competitive private digital sector. Finally, countries fitting this model are likely to fine big corporations and put forward or at least debate strong market and *content regulations* to preserve competition and prevent hate speech, like France, Germany, the UK, and Brazil (Flew et al., 2019). Measures such as Australia's News Media Bargaining Code and Canada's Online News Act represent two attempts to regulate the dissemination of news content online (Hine, 2022; Katz, 2023). Platform liability can also be enforced with more robust measures, such as Brazil's ban on Telegram because the company refused to cooperate with an investigation into neo-Nazi groups (Leloup, 2023).

3.2 Market-Oriented Model

The market-oriented model values economic *laissez-faire*, market benefits, and competition-based innovation at the expense of state regulation. This suggests that countries adhering to this model eschew any regulation. Nevertheless, our empirical corpus indicates that a model purely driven by the market no longer exists, if it ever did. The United States is usually mentioned as the neoliberal country *par excellence*, responsible for the generation of today's untameable large corporations, and yet it would be unthinkable to imagine it without the heavy involvement of Federal agencies (Mazzucato, 2014). According to Chander (Chander, 2013, p. 639) Silicon Valley firms created a neoliberal discourse while American "judges and legislators at

the turn of the Millennium altered the law to subsidise the development of Internet companies", just as nineteenth-century judges did to support industrial development. This means that even the most neoliberal country has never left tech firms entirely unregulated. Instead, it proactively supported their growth through enormous public funds allocation for research and development. Indeed, in line with growing political tensions with China, the US has increasingly turned to industrial policy as a mechanism for maintaining its advantage in emerging technologies (Roberts et al., 2023).

3.2.1 Market-Rights Balance

In countries falling into this model, right protection is often limited by the preservation of free trade principles and economic laissez-faire, resulting in a looser regulatory approach. This is the case of digital content regulation, data protection frameworks, and antitrust laws. The main reason to avoid regulation here is the fear of hampering innovation and constraining economic growth. Thus, self-regulation has been traditionally emphasised. According to this literature, the market rationale's primacy and the preference for self-regulation were then crystallised into law through Section 230 of the 1996 Communications Decency Act, which lifted online intermediaries from any liability connected with third-party hosted content. Many pieces of literature identify the Californian high-risk venture capital industry of the 1990s as the genesis of both the US's loose regulatory approach and the traditional platform business model (Srnicek, 2017). While this can be related to the role of the US in the early stage of the Internet, digital non-regulation or self-regulation models have characterised many other countries such as Japan, France, Australia, Chile, and the United Kingdom (Bradford, 2023). Today, it has been advanced the idea that the age of self-regulation has left room for more assertive regulatory approaches (Floridi, 2021). This is the case of the United Kingdom, which experienced an upsurge of regulatory activism by institutions and civil societies after decades of loose regulation (Kretschmer et al., 2021).

3.2.2 National Security

In each of said cases, digital *laissez-faire* lost ground to the national security principle, where state action is particularly strong. After 2018, the growing resorting to national security is regarded as the primary rationale underlying digital governance decisions, often due to the emerging Chinese contestation of the US digital power. In this sense, national security has been invoked as the main reason for *banning corporations, technologies, and contents*, e.g., the federal ban on TikTok and WeChat supported by former President Donald Trump in 2020 (Rembert, 2022) and by President Biden after that (Douzet & Taillat, 2022). Security and sovereignty have also been invoked by EU Commissioner Thierry Breton as the reason behind the need to exclude Huawei from the development of 5G networks (Breton, 2023). National security is also mobilised to prevent foreign acquisitions and exclude foreign operators (Bradford, 2023), as in the case of Italy (Fonte & Cao, 2021), or threaten the implementation of encryption, as the debate in the UK has shown (Guest, 2023). The Indian government has also invoked national security as it decided to ban TikTok

(Kumar & Thussu, 2023). Countries such as Australia, Canada, France, New Zealand, Norway, and the UK resorted to national security to substantiate their ban on TikTok on national governmental devices (Navlakha, 2024).

3.2.3 State Expansionism

Lastly, while other models brand digital sovereignty as an attempt to re-negotiate the established digital order, countries of the market-oriented model largely *support existing standards and norms*. With this purpose in mind, market-oriented model countries aim to export their digital governance values in international forums or, in the case of the US, through prominent digital companies and infrastructures or by coercing foreign countries' governance decisions. This set of practices has been defined as digital expansionism (Roberts et al., 2023). This also entails protectionist actions. A recent example is represented by the latest restrictions put by the Biden Administration—whose approach to China has become increasingly confrontational (Roberts et al., 2023)—on exports of Nvidia's high-performance compute GPUs to China and "some countries in the Middle East".[3] *Damaging foreign countries* is usually paired with *supporting domestic corporations* by helping them penetrate foreign markets and access data. Expansionist measures are also supported by *stimulating digital innovation* in alliance with other countries to contain adversaries, just like the US did with Israel, South Korea, Australia, Canada, France, and Germany in the early stages of the Internet (Radu, 2019).

3.3 Centralisation Model

The centralisation model is characterised by the reshaping of digital governance based on centralised regulation. By centralised regulation we mean the exclusion of non-state actors from the process of decision-making. For countries fitting this model, centralisation is an ongoing process and can be realised with different degrees. In fact, these countries have often gone through looser regulatory approaches typical of Western countries but started changing their paradigms at the beginning of the 2010s. This differentiated transition toward a centralised governance system is what distinguishes this model from the state-based one. Instead of outsourcing governance and leveraging infrastructural features of the digital space to implement digital content regulations and economic and legal provisions, common measures of this model involve the creation of new powerful regulatory bodies.

3.3.1 Digital Self-Sufficiency and State Sovereignty Over Corporations

To ensure the highest degree of regulatory effectiveness, this model foresees measures of exclusion and replacement of foreign digital operators with domestic players that are usually easier to control by governmental agencies. Countries following this approach may aim for possibilities ranging from digital self-sufficiency to genuine autarky desires. The most prominent example of this model is Russia, where, until

[3] These restrictions have been reported by Nvidia in an official statement (NVIDIA Corporation, 2023).

the beginning of the 2010s, the Internet was still imagined as a tool of liberation and democratisation (Musiani, 2022). A watershed moment was represented by the state introduction of a unified register of banned websites containing child pornography and drugs. Over time, in the following two years, the ban was expanded to include political content marked as "extremist" or "terrorist" (Thumfart, 2021). The Russian government has also banned many popular platforms like Twitter, Facebook, and Instagram over claims of "extremism". This crackdown is part of a broader historical trend, exacerbated by Russia's invasion of Ukraine. Since the beginning of the 2010s, Russia has discouraged the usage of foreign—especially US—digital platforms and promoting the adoption of their Russian-speaking alternatives, e.g., VK, Mail.ru, and Yandex, which makes enforcing the government's expression restrictions easier. For example, a recent report found that Russia has the most restricted access to VKontakte social media content compared to other post-Soviet countries where the platform operates (Knockel et al., 2023).[4] After 2009, Iran too started banning the major Western platforms, filtering content, and using Internet shutdowns to *influence domestic public opinion* (Motamedi, 2024). Bangladesh implemented a smart filtering system and used Internet shutdowns to control instability over religious tensions (Rahman, 2023). Other countries, such as Vietnam, enforce temporary content censorship and complete bans to prevent the population from criticising the government (Ewe, 2023).

3.3.2 National Security

Countries fitting this model tend to frame state control over domestic data flows as a matter of national security and to use it as a rationale to re-centralise digital governance. Data localisation measures and legal disclosure requirements for private operators are the most common provisions to ensure state control over domestic data flows. In Russia, the 2016 Yarovaya Law forces Internet operators to record and store data covering text messages, phone conversations, and images within the Russian jurisdiction for six months to "fight terrorism" (Sivetc, 2021). Furthermore, state control of data flows is often linked with the enhancement of state surveillance. In this sense, India represents an instructive example. While the country made privacy a fundamental right some years ago, it still lacks a comprehensive regulation for data protection, and it heavily relies on Indian companies to implement strong surveillance measures. In this sense, "Indian companies have been innovating on facial- and fingerprint recognition, predictive intel, decryptors, and now, COVID-19 tech for homeland security" (Mahapatra, 2021). According to Prasad (2022), the penetration of digital surveillance in India marked a shift from political to biopolitical control. Finally, since 2009, Belarus has forced local and international websites to register with the Information Ministry for national security reasons and to *centralise digital regulation*.

[4] The aforementioned report shows that the Russian blocking is about "94.942 videos, 1.569 community accounts, and 787 personal accounts in the country". These are mainly related to independent news organisations, Ukrainian and Belarusian issues, protests, and LGBTQIA+ communities.

3.3.3 Territorialisation of Cyberspace

To equip centralising efforts with an ideological basis, this model is also characterised by the acceptance of and support for a multilateral understanding of digital regulation. Multilateralism is here understood as the alternative to multistakeholderism (Raymond & DeNardis, 2015). It implies that the state is the legitimate sovereign ordering centre of cyberspace and that the private sector and civil society are subordinated to its deliberations. Multilateralism is deeply tied with the concept of territorialism, as it roots its assumptions on the reproduction of territorial sovereignty in cyberspace. This territorialist multilateralism is strongly supported by China and Russia within and beyond the United Nations, with the objective of *negotiating existing standards and norms* (Raymond & Sherman, 2023).

3.4 State-Based Model

The state-based model is characterised by the blurry distinction between public and private sectors, the conceptualisation of digital media as a means of nation-building and socio-economic growth, the quasi-total self-reliance on domestic digital operators and resources, massive investments in emerging technologies, and the desire to export governance norms and digital standards. Contrary to any other model, the close relationship between digital corporations and state authorities makes it difficult to talk about the attempt to reinstate *state sovereignty over corporations*. Although many countries falling into the centralisation model seem inspired by the state-based one, our empirical corpus suggests that China and North Korea (although there is a significant lack of literature for the latter[5]) are the only countries where the absence of a clear private-public boundary provoked a state-centred structuration of cyberspace from the very beginning.

3.4.1 Nationalised Governance

The Chinese Communist Party (CCP) is central in implementing digital development, using technology for economic growth and political control. The dominant narrative among Chinese scholars describes the Internet as an anarchic and disorderly place that reproduces the power of global hegemons, with the US at the forefront (Arsène, 2016).

3.4.2 Digital Self-Sufficiency

Because of this structure and the dimension of its internal market, China constitutes a unique case that can hardly be compared to other countries. China has the highest number of digital users (Statista, 2023), which allowed authorities to *exclude (foreign) corporations and technologies,* let domestic digital operators grow internally, and then send them to the international arena once they became competitive. The purpose of this strategy was to *support domestic corporations* by preserving them

[5] Valuable indications for the North Korean case can be found in Lim (2022).

from international competition while allowing them to develop through the massive availability of data in a siloed internal market. These digital champions are expected to pursue the indigenation strategy, i.e., to increase the proportion of Chinese technology used within the Chinese cyberspace (Creemers, 2020), boost China's economic growth (Plantin & De Seta, 2019) and spread worldwide influence (Keane & Wu, 2018). Furthermore, China has developed and implemented smart and systematic filtering systems to *regulate digital content* and *influence domestic public opinion* through obligations for Internet Service Providers (Feng et al., 2023) and propaganda dissemination through underpaid labour (Yang et al., 2021)

3.4.3 National Security

The growth of digital companies fits into a broader strategy to reduce the reliance on foreign providers and infrastructures, particularly by *supporting and regulating digital innovation* and internalising the digital value chain (Grossman et al., 2020). China has been massively investing in AI, quantum technologies, the Internet of Things, and semiconductors, among other technologies. Regarding quantum technologies, Chinese authorities are estimated to have invested $15 billion to secure national development in the field. Today, the country holds 30% of the quantum patents in the world and AI is increasingly framed as a matter of national security and key to Chinese global dominance (Zeng, 2021). For this reason, Chinese investments in AI are expected to hit $38.1 billion by 2027, which is 9% of the global investments in the field (Chi, 2023). On the one hand, these investments have also been made necessary by external pressures, such as US restrictions on semiconductors (Malkin, 2018). On the other hand, in state-led discourse, technological developments and state-deployed financing "are portrayed as the likely saviours of China's economy" (Rao, 2023).

3.4.4 Territorialisation of Cyberspace

Investments in emerging technologies, digital innovation, and the production of regulatory measures are based on a territorial and multilateral vision of cyberspace. Especially after the Snowden Revelations, American technology is considered the material extension of the US power over China (Creemers, 2020). In this sense, the boundary between the geographical origins of a company and the nation where it is based is of little relevance, resulting in a form of economic nationalism (Helleiner, 2021). Developing Chinese technology is thus regarded as an essential step toward digital sovereignty. Finally, the intricate filtering system of China—usually called the Great Firewall—is often considered a "splinternet" because it reproduces geographic boundaries in cyberspace by regulating websites and content access (Ensafi et al., 2015).

4 Seeking Robust Governance for Digital Sovereignty

Interest around digital sovereignty has been surging both among scholars and among policymakers, and the latter increasingly refer to academic literature to design and implement digital policies. While, the first part of the article offers a summarized portrait of the state of the art, this section develops a robust governance model to test the high-level models like the one we produced. The reason to do this is that digital sovereignty frameworks, despite their varied emphases, are grounded in a governance infrastructure. This infrastructure encompasses a government's capabilities in establishing laws, enforcing them, and delivering services, independent of the specific governing political system (Fukuyama, 2013). A key metric for assessing the effectiveness of public governance is its ability to adapt to changing and often dysfunctional dynamics, which is a critical challenge. Such dynamics, sometimes termed 'turbulence' in public administration and governance literature (Ansell et al., 2024; Ansell & Trondal, 2018; Rosenau, 2018), describe scenarios where events, demands, and support change in unpredictable ways (Ansell & Trondal, 2018, p. 43). Turbulence may involve (a) shifting parameters—stable factors like budgets, political support, or technology become unstable, hindering new strategic planning; (b) intercurrences—unexpected interactions between previously separate subsystems; and (c) temporal complexity—the need to switch between routine and rapid response modes. Examples of turbulence include globalization, the escalation of (cyber)terrorism, breakthroughs in disruptive technologies, and shifts in policy or institutional frameworks (Ansell & Trondal, 2018, pp. 45–46).

A governance model capable of addressing turbulence should withstand various conditions and adapt over time, maintaining stability amidst change. This is called in literature *robust governance* (Ansell et al., 2015, 2023, 2024; Howlett et al., 2018). Unlike resilience, which implies a system's ability to return to a stable state after turbulence, robust governance is about advancing to preserve essential functions in potentially improved ways (Ansell et al., 2015). Ansell and Trondal differentiate resilience from robustness by noting that robust governance incorporates flexibility and complexity absorption into organizational structures, thus not just adapting to new environments but also integrating diverse approaches (Ansell & Trondal, 2018). Hence, a political system is considered robust when it can consistently allocate values authoritatively, even amid disruptive demands and events, without generating further destabilizing challenges.

Robust governance emerges as an alternative to traditional governance models, including public bureaucracy and network governance (Ansell et al., 2023). On the one hand, the bureaucratic model emphasizes stable, predictable administrative decisions, relying on professional, rule-bound civil servants to separate private interests from public authority, thus ensuring stability and sovereign political leadership. It operates on well-defined organizational structures, written and detailed rules, and a focus on delivering public value through long-term, programmatic investments. Also, these programs are characterized by hierarchical control, designed to buffer against external turbulence through either built-in redundancies or incremental adaptations to change. Conversely, network governance offers a polycentric, collaborative alternative, emphasizing economies of scope over scale. It involves public and private

actors across levels and sectors uniting around shared issues, fostering trust-based collaboration within semi-autonomous institutional frameworks (Ansell et al., 2023).

Robust governance combines elements from bureaucratic and network models to overcome their limitations to better handle turbulences. It inherits the structured approach to innovation from bureaucratic governance. Still, it diverges from its centralized control and inflexibility, favouring trust-based management and empowering local teams for spontaneous innovation and response to changes. From network governance, it borrows the coordination among diverse stakeholders and the capability for flexible, cross-program collaborations, but innovatively integrates these into permanent structures. This creates collaborative platforms within public bureaucracies, facilitating a seamless integration of solutions and addressing the temporary and fragmented nature of network governance (Ansell et al., 2023, p. 9). Moreover, in terms of temporal orientation, robust governance combines the long-term stability focus of bureaucracies with the short-term adaptability of networks. It acknowledges the necessity of strategic agility, especially in turbulent times, by integrating short-term adaptive responses with a vision for long-term societal goals. This blend ensures responsiveness to immediate challenges without losing sight of broader, long-term objectives (Ansell et al., 2023, p. 10).

In the context of digital sovereignty, such a governance strategy should incorporate mechanisms for absorbing the disruptions caused by technological advancements, geopolitical changes, and evolving societal norms. Innovations like quantum computing and artificial intelligence present challenges to the established frameworks of digital security, data management, and economic competitiveness, necessitating comprehensive updates to regulatory structures and national institutions (Gordon, 2024). Additionally, the complexities of data sovereignty, exacerbated by multinational corporations operating under varying data protection laws, introduce turbulence through conflicts between global data protection standards and complicate governance efforts, especially when these entities seek to influence digital policy in opaque manners.

Robust governance for digital sovereignty may involve specific strategies, such as:

- **Prototyping, regulatory sandboxes, and safety harbours:** Adopting a strategy that merges firm regulatory standards with a flexible, adaptive approach, including safety harbours, enables quick integration of technological innovations within a complex regulatory framework. Regulatory sandboxes offer a controlled environment for testing new technologies under oversight, facilitating fast feedback and regulatory adjustments (Allen, 2019). Safety harbours encourage innovation and measured risk-taking by providing a clear framework that allows for some deviation from standard compliance, dependent on adherence to set guidelines. In digital sovereignty governance, both regulatory sandboxes and safety harbours are crucial to balancing security and privacy needs with the imperative for digital innovation (Bromberg et al., 2017; Hacker, 2020; Truby et al., 2022; Washington et al., 2022). For example, establishing safety harbours for companies developing cybersecurity technologies allows governments to protect firms by sharing data on cyber threats, promoting open collaboration, and enhancing national cybersecurity resilience.

- **Digital infrastructure, accessibility, and scalability:** The ability to swiftly scale resource mobilization and organizational reactions to match evolving and emerging challenges is crucial for building robust governance (Ansell et al., 2023, p. 13). Investing in scalable and adaptable digital infrastructure is essential to handle sudden demand surges. This strategy might include leveraging cloud-based solutions, decentralized data management systems, and integrating cutting-edge technologies like blockchain to ensure secure and robust public service delivery. Additionally, a national cybersecurity protocol that can quickly scale up in response to diverse cyber threat levels is vital. For example, in a significant cyberattack, a scalable response would activate additional cybersecurity measures and resources, such as emergency response teams and enhanced surveillance, which are pre-organized but mobilized as necessary.
- **Risk-based regulatory approaches:** Tailoring legal regulations to the level of risk associated with digital services or technologies—increasingly common for AI systems and other digital innovations regulations (Chamberlain, 2023; Gonçalves, 2020; Novelli et al., 2023, 2024)—offers significant benefits for the robust governance of digital sovereignty. These include qualifying uncertainties through probabilistic predictions about potential hazards when definitive knowledge is scarce (Rothstein et al., 2013). Furthermore, risk-based approaches enable governments to identify and prioritize digital threats that could impact national security, economic stability, and public welfare, allowing for the efficient allocation of resources to protect and govern the most critical aspects of digital sovereignty effectively (Moerel & Timmers, 2021).
- **Modularisation of digital services:** Modularisation involves designing and implementing digital infrastructure and systems in a way that allows for components to be independently modified, replaced, or scaled. Creating a digital services platform—e.g., for mobility (Schreieck et al., 2016)—where modules can be independently updated or replaced without disrupting the entire system. This approach provides flexibility in adopting new technologies or protocols for data protection, privacy, and cyber-defence without overhauling the whole digital infrastructure.
- **Redundancies in digital infrastructure:** Establishing redundancies within digital governance frameworks ensures that the failure or challenge encountered by one pathway does not compromise the integrity and objectives of policies. In digital sovereignty, this could mean adopting a multi-cloud strategy for governmental data storage to ensure data redundancy across various cloud service providers in different jurisdictions (Gundu et al., 2020). This not only guards against data loss or accessibility issues due to technical failures or legal disputes but also reduces risks related to data sovereignty by minimizing dependency on any single country's legal systems or regulatory changes and developing a national digital infrastructure that relies on a mix of terrestrial fibre networks, satellite communications, and emerging technologies such as high-altitude platform stations (Arum et al., 2020).

The four digital sovereignty models assessed in Sect. 3 diverge in their realization of robust governance principles and strategies. The *rights-based* model stands out for

implementing risk-based regulations like the AI Act and demonstrating adaptability with measures like the GDPR. These efforts aim to balance individual rights against market dynamics and adjust to tech advancements by reassessing risks. However, its reliance on comprehensive regulation, requiring extended debate and accountability, may limit its responsiveness to rapid technological shifts and market changes, potentially stalling the adoption of new tech advancements.

The *market-oriented* model, with its *laissez-faire* approach, fuels innovation and market dynamism, leading to technological and economic growth. Adapting over time, it has adopted stricter regulations for national security, showing flexibility in the face of digital disruptions. However, its initial resistance to government intervention complicates the creation of a comprehensive regulatory framework that protects user rights and privacy, impacting digital sovereignty. Moreover, its approach has difficulty addressing complexities from the unchecked growth of large tech firms, resulting in significant antitrust, data privacy, and digital equity issues.

The *centralisation* model focuses on national security and the centralisation of digital governance, ensuring stability and control over digital infrastructure against external threats. However, its strict control compromises adaptability and the incorporation of technological advancements and global trends, potentially limiting innovation. Additionally, its lack of inclusivity, with state-dominated governance and limited participation from civil society, businesses, and international partners, may result in governance outcomes that inadequately address broader community needs.

Finally, the *state-based* model shares problems similar to those of centralisation. Despite significant investments in new technologies fostering innovation, its state-centric approach may hinder responsiveness to fast-paced technological shifts and changing social norms, especially in a global context where digital ecosystems are increasingly interconnected. Additionally, the blurred distinction between the government and digital firms can limit possibilities for participatory governance, hindering digital policy input from civil society and individuals.

5 Conclusion

Digital sovereignty is a popular yet still emerging concept. Despite the availability of many scientific contributions, existing analytical efforts are often heterogeneous and sometimes inconsistent. This makes it difficult to agree on a shared understanding of digital sovereignty. Our analysis provides an empirically grounded mapping of the existing forms of digital sovereignty by defining four models and a normative assessment based on a robust governance framework.

Our analysis shows that none of the existing models offers a desirable balance between comprehensive digital regulation and responsiveness to technological innovation and social changes. Nevertheless, each model offers useful lessons to policymakers who wish to implement an effective and robust form of digital sovereignty. The rights-based model displays a helpful blueprint for implementing a comprehensive regulatory regime balancing fundamental rights and market freedom. However, this could slow decision-making processes, resulting in a lack of responsiveness to disruptive socio-technical changes. The market-oriented model is a good example of market-driven

innovation with two undesirable outcomes: the rise of the national security rationale in decision-making, and the lack of regulation in some sensitive areas, e.g., data protection and content moderation. The centralisation model represents an attempt to implement a gradually centralised control over digital infrastructure that dangerously results in the exclusion of non-state governmental actors. The restriction of social representation could eventually reduce the flexibility of governing bodies to cope with socio-political changes. Finally, the state-based model certifies the possibility of state bodies to lead innovation through significant investments and offers an effective example of an innovation model to countries not characterized by open market economies. However, the continuous effort to exclusively keep decision-making in the hands of the state can lead to internal tensions and make the investing governmental bodies less sensitive to social changes and potentially disruptive innovations.

This article suggests that a robust digital governance strategy should combine flexible regulatory mechanisms, state investments in innovation, and a relatively free market regime. Combining these components ensures an effective regulation of digital technology without hampering innovation and competition and preserves a desirable balance between short-term adaptability and long-term stability. In the rights-based model, for example, overarching regulation (with long-term goals) risks limiting a country's responsiveness to technological shifts and market changes (short-term challenges). Targeted and strategic state investments and regulatory sandboxes should help fuel innovation and adaptability. It is also worth noting that the effectiveness of a given form of digital sovereignty is always contextual. The proposed model of robust governance outlines key provisions to ensure state control over digital infrastructures, but exactly what they look like in practice will vary based on national context. Furthermore, each model is sensitive to geopolitical tensions and economic pressures, often leading to less inclusive governance and the imposition of national security rationales and confrontational approaches in the global arena. This is represented in the historical trajectory of the market-based model, where national security has lately become the main force behind digital policy at the cost of increased geopolitical tensions. To prevent this, future efforts should focus on the development of a pluralist model of governance, the introduction of a framework of international cooperation among great powers, and the inclusion of less technologically developed countries.

Funding Open access funding provided by Università della Svizzera italiana. The authors did not receive any financial support for the production of this article.

Data availability An Excel file reporting all the peer-reviewed articles collected as data for this study can be freely requested at the following email: samumeme37@gmail.com.

Declarations

Competing interests The authors report there are no competing interests to declare.

References

Allen, H. J. (2019). Regulatory sandboxes. *George Washington Law Review*, *87*(3), 579–645.

Ansell, C., Boin, A., & Farjoun, M. (2015). Dynamic conservatism: How institutions change to remain the same. In *Institutions and ideals: Philip Selznick's Legacy for organizational studies* (Vol. 44, pp. 89–119, Research in the Sociology of Organizations). Emerald Group Publishing Limited. https://doi.org/10.1108/S0733-558X20150000044005

Ansell, C., Sørensen, E., & Torfing, J. (2023). Public administration and politics meet turbulence: The search for robust governance responses. *Public Administration*, *101*(1), 3–22. https://doi.org/10.1111/padm.12874

Ansell, C., Sørensen, E., Torfing, J., & Trondal, J. (2024). Robust governance in turbulent times, *Elements in Public Policy*. https://www.cambridge.org/core/elements/robust-governance-in-turbulent-times/AB44DBE9AA636390EC114E8A428BF188

Ansell, C., & Trondal, J. (2018). Governing turbulence: An organizational- institutional agenda. *Perspectives on Public Management and Governance*, *1*(1), 43–57. https://doi.org/10.1093/ppmgov/gvx013

Arsène, S. (2016). Global internet governance in chinese academic literature: Rebalancing a Hegemonic World order? *China Perspectives*, *2*, 25–35. https://doi.org/10.4000/chinaperspectives.6973

Arum, S. C., Grace, D., & Mitchell, P. D. (2020, May). A review of wireless communication using high-altitude platforms for extended coverage and capacity. *Computer Communications*, *157*, 232–256. https://doi.org/10.1016/j.comcom.2020.04.020

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/Sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Bromberg, L., Godwin, A., & Ramsay, I. (2017). Fintech sandboxes: Achieving a balance between regulation and innovation. SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=3090844

Chamberlain, J. (2023). The risk-based approach of the European Union's proposed artificial intelligence regulation: Some comments from a Tort Law perspective. *European Journal of Risk Regulation*, *14*(1), 1–13. https://doi.org/10.1017/err.2022.38

Chander, A. (2013). How law made silicon valley. *Emory Law Journal*, *63*(3), 639–694.

Chander, A., & Schwartz, P. (2023). Privacy and/or trade. *University of Chicago Law Review*, *90*, 49–136.

Chander, A., & Sun, H. (2021). Sovereignty 2.0. *Vanderbilt Law Review*, *55*.

Chi, S. (2023). China's investment in AI expected to reach $38.1b in 2027. *China Daily*. Retrieved August 23, 2023, from https://global.chinadaily.com.cn/a/202308/23/WS64e5b34fa31035260b81dc9f.html

Christakis, T. (2023). European digital sovereignty, data protection, and the push toward data localization. In *Data sovereignty: From the digital silk road to the return of the state*. Oxford University Press.

Couture, S., & Toupin, S. (2019). What does the notion of "Sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Creemers, R. (2020). China's conception of cyber sovereignty: Rhetoric and realization. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3532421

Douzet, F., & Taillat, S. (2022). Prepping for long-term competition? U.S. leadership in cyberspace from Trump to Biden. In M. Stricof & I. Vagnoux (Eds..), *U.S. leadership in a world of uncertainties* (pp. 213–234). Springer International Publishing. https://doi.org/10.1007/978-3-031-10260-8_12

Ensafi, R., Winter, P., Mueen, A., & Crandall, J. R. (2015). Analyzing the Great Firewall of China over space and time. *Proceedings on Privacy Enhancing Technologies*, *2015*(1), 61–76. https://doi.org/10.1515/popets-2015-0005

Ewe, K. (2023). Vietnam amps up authoritarian online censorship in the name of child safety. TIME. Retrieved October 12, 2023, from https://time.com/6322914/vietnam-tiktok-social-media-censorship-child-safety/

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Feng, J., Yu, Y., & Xu, T. (2023). Content regulation laws for chinese ISPs: Legal responsibilities in free speech and filtering of harmful content. *Law & Economy*, *2*(11), 53–59.

Floridi, L. (2021). The end of an era: From self-regulation to hard law for the digital industry. *Philosophy & Technology*, *34*(4), 619–22. https://doi.org/10.1007/s13347-021-00493-0

Flew, T., Martin, F., & Suzor, N. (2019). Internet regulation as media policy: Rethinking the question of digital communication platform governance. *Journal of Digital Media & Policy*, *10*(1), 33–50. https://doi.org/10.1386/jdmp.10.1.33_1

Fratini, S. (2024). Performing privacy culture. The platform Threema and the contestation of surveillance made in Switzerland. *Studi culturali*, *1*, 3–26. https://doi.org/10.1405/113065

Fratini, S., & Musiani, F. (2024). Data localization as contested and narrated security in the age of digital sovereignty: The case of Switzerland. *Information, Communication & Society*, *June*, 1–19. https://doi.org/10.1080/1369118X.2024.2362302

Fonte, G., & Cao, E. (2021). Italy's Draghi vetoes third chinese takeover this year. *Reuters*, Retrieved November 23, 2021, from, sec. Deals. https://www.reuters.com/markets/deals/italys-draghi-vetoes-third-chinese-takeover-this-year-2021-11-23/

Fukuyama, F. (2013). What Is governance? *Governance*, *26*(3), 347–368. https://doi.org/10.1111/gove.12035

Gonçalves, M. E. (2020). The risk-based approach under the new EU data protection regulation: A critical perspective. *Journal of Risk Research*, *23*(2), 139–152. https://doi.org/10.1080/13669877.2018.1517381

Gordon, G. (2024). Digital sovereignty, digital infrastructures, and quantum horizons. *AI and Society*, *39*(1), 125–137. https://doi.org/10.1007/s00146-023-01729-7

Grossman, D., Curriden, C., Ma, L., Polley, L., Williams, J. D., & Cortez, C. (2020). *Chinese views of big data analytics*. RAND Corporation. https://doi.org/10.7249/RRA176-1

Guest, P. (2023). Britain admits defeat in controversial fight to break encryption. *Wired*, Retrieved September 6, 2023, from https://www.wired.com/story/britain-admits-defeat-online-safety-bill-encryption/

Gundu, S. R., Panem, C. A., & Thimmapuram, A. (2020). Hybrid IT and multi cloud an emerging trend and improved performance in cloud computing. *SN Computer Science*, *1*(5), 256. https://doi.org/10.1007/s42979-020-00277-x

Haché, A. (2014). La Souveraineté Technologique. *Mouvements*, *79*(3), 38–48. https://doi.org/10.3917/mouv.079.0038

Hacker, P. (2020). AI regulation in Europe. SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.3556532

Helleiner, E. (2021). The diversity of economic nationalism. *New Political Economy*, *26*(2), 229–238. https://doi.org/10.1080/13563467.2020.1841137

Hennink, M. M., Kaiser, B. N., & Marconi, V. C. (2017). Code saturation versus meaning saturation: How many interviews are enough? *Qualitative Health Research*, *27*(4), 591–608. https://doi.org/10.1177/1049732316665344

Herian, R. (2020). Blockchain, GDPR, and fantasies of data sovereignty. *Law, Innovation and Technology*, *12*(1), 156–174. https://doi.org/10.1080/17579961.2020.1727094

Hine, E. (2022). The impact of Australia's news media bargaining code on journalism, democracy, and the battle to regulate big tech. In J. Mökander & M. Ziosi (Eds.), *The 2021 yearbook of the digital ethics lab* (pp. 63–74). Springer International Publishing. https://doi.org/10.1007/978-3-031-09846-8_5

Howlett, M., Capano, G., & Ramesh, M. (2018). Designing for robustness: Surprise, agility and improvisation in policy design. *Policy and Society*, *37*(4), 405–421. https://doi.org/10.1080/14494035.2018.1504488

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data and Society*, *8*(1). https://doi.org/10.1177/2053951720982012

Katz, A. (2024). Sedating Democracy's Watchdogs: Critical reflections on Canada's proposed online news act. *Columbia Journal of Law & the Arts*, *46*(3). Available at SSRN: https://ssrn.com/abstract=4458514

Keane, M., & Wu, H. (2018). Lofty ambitions, new territories, and turf battles: China's platforms "Go Out"'. *Media Industries Journal*, *5*(1). https://doi.org/10.3998/mij.15031809.0005.104

Knockel, J., Dalek, J., Meletti, L., & Ermoshina, K. (2023). Not OK on VK: An analysis of in-platform censorship on Russia's VKontakt. https://hdl.handle.net/1807/129345

Kretschmer, M., Schlesinger, P., & Furgal, U. (2021). The emergence of platform regulation in the UK: An empirical-legal study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3888149

Kumar, A., & Thussu, D. (2023). Media, digital sovereignty and geopolitics: The case of the Tiktok ban in India. *Media, Culture & Society*, *45*(8), 1583–1599. https://doi.org/10.1177/01634437231174351

Leloup, D. (2023). Brazil bans Telegram in latest stage of troubled relationship with app. *Le Monde.Fr*, Retrieved April 27, 2023, from https://www.lemonde.fr/en/pixels/article/2023/04/27/brazil-bans-telegram-in-latest-stage-of-troubled-relationship-with-app_6024575_13.html

Lim, J. (2022). Digital Joseon: Digital transformation under North Korea's five-year plan. *North Korean Review*, *18*(1), 72–105. https://www.jstor.org/stable/27160576

Low, J. (2019). A pragmatic definition of the concept of theoretical saturation. *Sociological Focus*, *52*(2), 131–139. https://doi.org/10.1080/00380237.2018.1544514

Mahapatra, S. (2021). Digital surveillance and the threat to civil liberties in India. Social Science Open Access Repository. https://nbn-resolving.org/urn:nbn:de:0168-ssoar-73130-3

Malkin, A. (2018). *Made in China 2025 as a challenge in global trade governance: Analysis and recommendations*. Centre for International Governance Innovation.

Mazzucato, M. (2014). The entrepreneurial state: Debunking Public vs. Private sector myths. In *Anthem frontiers of global political economy* (Revised ed.). Anthem Press.

Moerel, L., & Timmers, P. (2021). Reflections on digital sovereignty. SSRN Scholarly Paper. Rochester, NY. https://papers.ssrn.com/abstract=3772777

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, *31*(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883

Motamedi, M. (2024). Iran unveils plan for tighter internet rules to promote local platforms. Al Jazeera. Retrieved February 24, 2024, from https://www.aljazeera.com/news/2024/2/24/iran-unveils-plan-for-tighter-internet-rules-to-promote-local-platforms

Musiani, F. (2022). *Infrastructuring* digital sovereignty: A research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, *25*(6), 785–800. https://doi.org/10.1080/1369118X.2022.2049850

Navlakha, M. (2024). Which countries have banned TikTok? Mashable. Retrieved March 14, 2024, from https://mashable.com/article/tiktok-ban-countries

Novelli, C., Casolari, F., Rotolo, A., Taddeo, M., & Floridi, L. (2023). Taking AI risks seriously: A new assessment model for the AI Act. *AI & Society*, July. https://doi.org/10.1007/s00146-023-01723-z

Novelli, C., Casolari, F., Hacker, P., Spedicato, G., & Floridi, L. (2024). *Generative AI in EU law: Liability, privacy, intellectual property, and cybersecurity*. SSRN Scholarly Paper. Rochester, NY. https://doi.org/10.2139/ssrn.4694565

NVIDIA Corporation. (2023). Form 10-Q. https://d18rn0p25nwr6d.cloudfront.net/CIK-0001045810/19771e6b-cc29-4027-899e-51a0c386111e.pdf

Plantin, J. C., & De Seta, G. (2019). WeChat as infrastructure: The techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, *12*(3), 257–273. https://doi.org/10.1080/17544750.2019.1572633

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4). https://doi.org/10.14763/2020.4.1532

Pot, W., Scherpenisse, J., & 't Hart, P. (2023). Robust governance for the long term and the heat of the moment: Temporal strategies for coping with dual crises. *Public Administration*, *101*(1), 221–235. https://doi.org/10.1111/padm.12872

Prasad, R. (2022). People as data, data as oil: The digital sovereignty of the Indian State. *Information, Communication & Society*, *25*(6), 801–815. https://doi.org/10.1080/1369118X.2022.2056498

Radu, R. (2019). Revisiting the origins: The internet and its early governance. In R. Radu (Ed.), *Negotiating internet governance* (pp. 43–74). Oxford University Press. https://doi.org/10.1093/oso/9780198833079.003.0003

Rahman, Z. (2023). Censorship and content filtering. Business Post BD. Retrieved February 18, 2023, from https://businesspostbd.com/opinion-todays-paper/2023-02-18/censorship-and-content-filtering-2023-02-18

Rao, Y. (2023). Discourse as infrastructure: How "New Infrastructure" policies re-infrastructure China. *Global Media and China*, *8*(3), 254–270. https://doi.org/10.1177/20594364231198605

Raymond, M., & DeNardis, L. (2015). Multistakeholderism: Anatomy of an inchoate global institution. *International Theory*, *7*(3), 572–616.

Raymond, M., & Sherman, J. (2023). Authoritarian multilateralism in the global cyber regime complex: The double transformation of an international diplomatic practice. *Contemporary Security Policy*, *45*(1), 110–140. https://doi.org/10.1080/13523260.2023.2269809

Rembert, R. L. (2022). TikTok, WeChat, and national security: Toward a U.S. data privacy framework. *Oklahoma Law Review*, *74*, 463–501

Roberts, H. (2024). Digital sovereignty: A normative approach. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.4699167

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3937345

Roberts, H., Hine, E., & Floridi, L. (2023). Digital sovereignty, digital expansionism, and the prospects for global AI Governance. In M. Timoteo, B. Verri, & R. Nanni (Eds.), *Quo Vadis, Sovereignty?* (Vol. 154, pp. 51–75). Philosophical Studies Series. Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-41566-1_4

Rosenau, J. N. (2018). *Turbulence in world politics: A theory of change and continuity*. Princeton University Press.

Rothstein, H., Borraz, O., & Huber, M. (2013). Risk and the limits of governance: Exploring varied patterns of risk-based governance across Europe. *Regulation & Governance*, *7*(2), 215–235. https://doi.org/10.1111/j.1748-5991.2012.01153.x

Saldaña, J. (2014). Coding and analysis strategies. In J. Saldaña & P. Leavy (Eds.), *The Oxford handbook of qualitative research* (pp. 580–598). Oxford University Press. https://doi.org/10.1093/oxfordhb/9780199811755.013.001

Schreieck, M., Wiesche, M., & Krcmar, H. (2016). Modularization of digital services for urban transportation.

Scognamiglio, F., Sancino, A., Caló, F., Jacklin-Jarvis, C., & Rees, J. (2023). The public sector and co-creation in turbulent times: A systematic literature review on robust governance in the COVID-19 emergency. *Public Administration*, *101*(1), 53–70. https://doi.org/10.1111/padm.12875

Scott, J., & Marshall, G. (2015). Ideal type. *Oxford Reference*, *2015*, https://doi.org/10.1093/oi/authority.20110803095956574

Sivetc, L. (2021, April). Controlling free expression "by Infrastructure" in the Russian Internet: The consequences of RuNet sovereignization. *First Monday*. https://doi.org/10.5210/fm.v26i5.11698

Srnicek, N. (2017). Platform capitalism. In *Theory Redux*. Polity.

Statista (2023). Number of internet users in China 2023. https://www.statista.com/statistics/265140/number-of-internet-users-in-china/

Breton, T. (2023). *Speech by Breton on the cybersecurity of 5G networks*. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_23_3314

Thumfart, J. (2021). The norm development of digital sovereignty between China, Russia, the EU and the US: From the late 1990s to the Covid-crisis 2020/21 as catalytic event. In *Data protection and privacy: enforcing rights in a changing world* (Vol. 14, pp. 1–44). Hart Publishing.

Tretter, M. (2023). Sovereignty in the digital and contact tracing apps. *Digital Society*, *2*(1), 2. https://doi.org/10.1007/s44206-022-00030-2

Truby, J., Dean Brown, R., Ibrahim, I. A., & Caudevilla Parellada, O. (2022). A sandbox approach to regulating high-risk artificial intelligence applications. *European Journal of Risk Regulation*, *13*(2), 270–294. https://doi.org/10.1017/err.2021.52

Walter, M., Kukutai, T., Russo Carroll, S., & Rodriguez-Lonebear, D. (2020). *Indigenous data sovereignty and policy* (1st ed.).Routledge. https://doi.org/10.4324/9780429273957

Washington, P. B., Ur Rehman, S., & Lee, E. (2022). Nexus between regulatory sandbox and performance of digital banks—A study on UK digital banks. *Journal of Risk and Financial Management*, *15*(12), 610. https://doi.org/10.3390/jrfm15120610

Yang, X., Yang, Q., & Wilson, C. (2021). Penny for your thoughts: Searching for the 50 cent party on Sina Weibo. In *Proceedings of the International AAAI Conference on Web and Social Media* (Vol. 9, pp. 694–697).

Zeng, J. (2021). Securitization of artificial intelligence in China. *The Chinese Journal of International Politics*, *14*(3), 417–445. https://doi.org/10.1093/cjip/poab005

Authors and Affiliations

Samuele Fratini[1,2,3] · Emmie Hine[4,5,7] · Claudio Novelli[4,7] · Huw Roberts[6] · Luciano Floridi[4,7]

✉ Samuele Fratini
samumeme37@gmail.com

1 Department of Philosophy, Sociology, Education and Applied Psychology, University of Padua, Piazza Capitaniato 3, Padua 35139, Italy

2 Institute of Media and Journalism (IMeG), Università della Svizzera Italiana, Via Buffi 13, Lugano 6900, Switzerland

3 Centre Internet et Société, Centre National de la Recherche Scientifique, 59-61 Rue Pouchet, Paris 75017, France

4 Department of Legal Studies, University of Bologna, Via Zamboni 22, Bologna 40126, Italy

5 Center for IT & IP Law, KU Leuven, Sint-Michielsstraat 6 Box 3443, Leuven 3000, Belgium

6 Oxford Internet Institute, University of Oxford, 1 St Giles', Oxford OX1 3JS, UK

7 Digital Ethics Center, Yale University, 85 Trumbull Street, New Haven, CT 06511, USA