Digital Society (2025) 4:27
https://doi.org/10.1007/s44206-025-00189-4

ORIGINAL PAPER

Sovereignty in the Digital Era: Rethinking Territoriality and Governance in Cyberspace

Federico Pierucci[1]

Received: 17 January 2025 / Accepted: 26 March 2025

Abstract
This opening paper for the topical collection on digital sovereignty explores the theoretical underpinnings and practical applications of the concept. The paper gives a brief overview of the traditional concept of sovereignty, discussing its applications to the digital. Moreover, it examines the tension between the borderless nature of cyberspace and the territorial basis of traditional sovereignty. The analysis highlights different perspectives on digital sovereignty, from state-led strategies aimed at controlling data and infrastructures to Indigenous approaches emphasizing self-determination and sovereignty over data. It further investigates the application of the concept to the infrastructural components of cyberspace, including submarine cables and cross-border data flows. The possibility of entrenching rules in the code of cyberspace is analysed highlighting regulatory ambitions and digital policies from China, Russia and the EU. This paper provides a foundational framework for the topical collection, proposing interdisciplinary approaches to address the complexities of digital sovereignty and its implications for global governance and politics.

Keywords Digital sovereignty · Data sovereignty · Indigenous data sovereignty · Data

1 Introduction - Why Digital Sovereignty Matters

As an introduction to the topical collection "**Reframing Digital Sovereignty: Theoretical and Practical Dimensions of Power in Cyberspace"** this paper aims to shed light on some possible avenues of research that can give a contribution (empirical or theoretical) to some key points that remain unclear. Digital sovereignty has been

✉ Federico Pierucci
Federico.pierucci@santannapisa.it

[1] Sant'anna School of Advanced Studies, Pisa, Italy

Published online: 22 April 2025

widely discussed across various domains. The term emerged in the Chinese discourse at the turn of the 21st century, at the end of the Cold War, under the name of cyber/network sovereignty (网络主权), as a way of resisting the expansion of the U.S. digital power. During this period, the U.S. promoted "soft power" through information technologies, viewing them as tools for democratization and liberalization. This geostrategy, rooted in internet decentralization and non-territorial networks, was seen by Chinese scholars as a Western hegemonic project, exemplified by the U.S. dominance in internet governance infrastructure, such as on the Internet Corporation for Assigned Names and Numbers (ICANN) (Cong & Thumfart, 2022). A parallel trend has emerged in the recent years following from the French initiative to establish its "sovranité numerique"[1] against the penetration of US big tech, such as Google, Amazon, Facebook, Apple, and Microsoft (GAFAM). The Snowden Scandal in 2013 was a pivotal moment that boosted this debate. The Snowden case involved Edward Snowden, a former NSA contractor, who leaked classified documents in 2013 revealing extensive global surveillance programs by the NSA and its partners, including mass data collection on citizens, governments, and corporations.[2] The 2014 French National Digital Council consultations highlighted digital sovereignty's importance for national sovereignty. In response to the dominance of Big Tech, the resulting economic dependence and value transfer necessitate regulatory measures that balance free movement and freedom with the need for sovereignty in the digital domain (Gueham, 2017).

Starting from the seminal paper of Couture and Toupin (2019), a vibrant debate has burgeoned among philosophical, legal and political scholar around the question of digital sovereignty. Digital sovereignty has become an increasingly salient topic in contemporary discourse as governments, institutions, and political actors grapple with the regulation and control of digital infrastructures, data flows, and technologies.

Covid was considered among scholars (Gábriš & Hamuľák, 2021; Thumfart, 2021; Tretter, 2023) and policymakers (Madiega, 2020) as a wake-up call for the need of digital sovereignty. As Floridi points out, the failure to establish a state-based solution to contact-tracing apps for the pandemic forced European states (such as Great Britain, Germany and Italy) to lean on Google and Apple APIs (Floridi, 2020, p. 1).

Evidence of the relevance of digital sovereignty is the fact that the new designate EU Commission (2024–2029) has among its portfolios "Tech Sovereignty, Security and Democracy",[3] highlighting the cardinal role that sovereignty over technology covers within EU policymaking.

Across the Atlantic, despite hosting most major technology corporations, the United States[4] is not immune to the need of sovereignty over digital technologies. Critical events that have disrupted the global order, such as the war in Ukraine, have

[1] Les Echos - De la souveraineté en général et de la souveraineté numérique en particulier - Archives.

[2] Edward Snowden: the whistleblower behind the NSA surveillance revelations| The NSA files| The Guardian, accessed on the 1/12/2024.

[3] 3b537594-9264-4249-a912-5b102b7b49a3_en, accessed on the 1/12/2024.

[4] The United States dominates global technology with top-ranked companies like Apple, Microsoft, Alphabet, Amazon, and Nvidia leading in technological sector (Top 10 tech companies by market cap 2024 | Statista).

prompted states to reconsider the reliance on private corporations to execute their policy objectives. Elon Musk's decision of shutting down Starlink satellites to stop Ukrainian military engagement in Crimea prompted US policymakers to investigate the need for state-controlled infrastructures.[5] Even more, global challenges such as the uncertainty over the Taiwan-China tension have brought the US and the EU to invest massive resources in bolstering autonomous capacity over semiconductors and critical raw materials.[6] States and supranational entities (such as the EU) attempt to territorialise (Lambach, 2020) cyberspace, trying to adapt the elusive borders of cyberspace to the traditional territorial divisions of states.

The concept, while diverse in its interpretations, fundamentally revolves around the question of how a sovereign authority—historically tied to territorial and geographic boundaries—can be rearticulated in the digital domain. This rearticulation is not merely an abstract theoretical issue but has direct implications for economic policy, security governance, and the regulation of information flows in a globalized and interconnected world. The following sections will be devoted to discussing some critical properties of digital sovereignty from a philosophical and political angle. This investigation is far from exclusive and can be considered as a reckoning of some open issues to spur a broader investigation.

2 What Is Sovereignty?

In this section, a brief reckoning of the traditional notion of sovereignty will be carried out. Sovereignty is one of the most foundational concepts in modern political thought, serving as a bridge between politics, political philosophy, and international law. One of the first authors to discuss the concept was the French jurist Jean Bodin, who, in his book "Six Livres de la Republique", published in 1576, in which he defines it as "the most high, absolute, and perpetual power over the citizens and subjects in a Commonwealth" (in Beaulac, 2003). A tangent line to the philosophical and juridical discourse was the historical events that led to the Peace of Westphalia (1648) in which it is conventionally assumed that the European kingdoms recognized the respective borders, defining what would be later called the "Westphalian conception" (Armstrong, 1993), abiding by two principles: (1) countries must refrain from interfering in each other's internal affairs in political and religious affairs; (2) each reign holds supreme authority within its territorial boundaries.

Thus, commonly the birth of the modern notion of a "sovereign state" is attributed to the condition in which European states found themselves after the Peace of Westphalia in 1648, formalising the mutual control over their own territories vis-à-vis the

[5] Elon Musk's refusal to have Starlink support Ukraine attack in Crimea raises questions for Pentagon| AP News, accessed on the 1/12/2024.

[6] The United States and the European Union have initiated significant legislative measures to secure critical raw materials essential for their economic and strategic interests. In August 2022, the U.S. enacted the Inflation Reduction Act, which, among other provisions, offers tax incentives to bolster domestic production of critical minerals vital for clean energy technologies. Concurrently, the EU proposed the Critical Raw Materials Act in March 2023, aiming to strengthen the entire value chain—from extraction to recycling—of critical raw materials within the Union, thereby reducing dependency on external sources.

claims coming from the Emperor and the Pope, as well as from other states. While the role of Westphalia as a turning point in the origin of the "sovereign state" has been challenged multiple times on a factual basis (Croxton, 1999; Osiander, 2001; Piirimäe, 2010; Shibasaki, 2014), this is a symbolic date that international relations scholars associate with the emergence of the modern concept, in which we find the key architecture of the balance of power between European states: the extension (and mutual exclusion) of the authority and legitimacy of a state over a defined territory and people. Regardless of the historical accuracy of the Peace of Westphalia as the "origin" of the sovereign space, we can discuss, from an analytical perspective, the conceptual components of the idea of sovereignty. We can define sovereignty as "*supreme legitimate authority within a territory"* (Philpott, 1995, p. 357). Two key terms define this concept:

Authority refers to the recognized right to rule, involving a structural relationship between rulers and the ruled. Authority operates as a hierarchical relation, where legitimacy arises from the shared recognition of system in which the state possesses the monopoly over force (Weber, 1978).

Territoriality aligns political authority with spatial boundaries, consolidating hierarchies within a defined space. It replaces earlier, overlapping claims of authority in the medieval world, with centralized control by the state over political, economic, and religious activities. The territorial principle distinguishes internal from external control, reinforcing state authority over its jurisdiction and creating a mechanism of mutual recognition of the authority of a state over its territory. One central distinction in sovereignty studies is between what we could call *de jure* sovereignty, which denotes the formal authority recognized by law, and *de facto* sovereignty, which refers to the effective exercise of power on the ground (Geenens, 2016). *De jure* sovereignty reflects the legal status conferred upon a state by international law, treaties, and external recognition. This status arises from widely upheld conventions that presume each state's right to govern a delimited territory without interference. As a result, de juresovereignty is treated as indivisible and absolute, implying that a state's legitimacy flows from external acknowledgment of its rightful jurisdiction.

In contrast, *de facto* sovereignty draws attention to whether a state can effectively wield power within, and sometimes beyond, its own boundaries. This entails considering the degree to which a government can enforce laws, collect taxes, protect citizens, and provide public goods. Real-world governance is rarely so neat: the presence of powerful nonstate actors—international organizations, multinational corporations, and NGOs—complicates any assumption of exclusive control. Moreover, foreign powers may intervene militarily or economically, further diluting a government's effective command over domestic affairs. Even states with extensive formal recognition may fail to fulfill basic governance functions, revealing a discrepancy between nominal authority and on-the-ground realities (Agnew, 2005).

3 Sovereignty Applied to the Digital World

In the context of the digital world, the application of these ideas becomes more complex, as there is no universally accepted definition of digital sovereignty. Various authors have approached the concept from diverse perspectives, attempting to capture its elusive nature. The concept of sovereignty emerged (as we saw succinctly in the introduction) in the policy discourse revolving around the strategic autonomy of states over the digital. As such, the main objective was not to put forth a philosophically sharp definition, but an actionable term that could inform and influence the actions of political bodies. Although there has been attempt to clarify the term, it remains somewhat opaque.

Here, I will briefly explore existing definitions to establish a foundation for further discussion. The normative and democratic implications of digital sovereignty are explored by Couture and Toupin (2019), who analyse how governments and other actors invoke sovereignty in relation to digital technologies. They argue that the rise of digital sovereignty reflects the enduring power of nation-states, despite critiques of state authority in the face of globalization. Couture and Toupin offer two possible interpretations of sovereignty: one that pertains to the state (or the community), and one to the individual. They elaborate on the idea of sovereignty as:

> The capacity for collectivities (states, communities, social movements, etc.) to innovate and/or engage in technological development (for instance by stimulating national innovation for economic forms of nationalism in the case of state or developing free software or autonomous infrastructures for civil society organizations)

and

> The security and/or privacy of individuals or collectives, and in relation to the ownership and control over data related to oneself, citizens, or a state (Couture & Toupin, 2019, p. 2317)

Pohle and Thiel (2020) extend this analysis, identifying state autonomy, economic self-determination, and individual rights as key dimensions of the debate, as well as the tensions between an "exceptionalist" understanding of cyberspace. Their definition is:

> The idea that states should reassert their authority over the internet and protect their citizens and businesses from the manifold challenges to self-determination in the digital sphere (Pohle & Thiel, 2020).

Moerel and Timmers (2021, p. 8) connect it with the idea of strategic autonomy, which they define as "the ability to decide and act autonomously on the essential digital aspects of our longer-term future in the economy, society, and democracy".

Glasze et al. (2023) emphasize the geopolitical significance of digital sovereignty, arguing that states, both authoritarian and democratic, are increasingly adopting terri-

torial strategies to control digital infrastructures and data flows. They assert that digital sovereignty has become a tool of strategic power, enabling states to protect their digital assets from external influence. This has led to renewed interest in national control over digital spaces, challenging earlier notions of a borderless global information society.

A significant trend has focused on the EU attempt to establish digital sovereignty. Bellanova et al. (2022) examine the European Union's pursuit of digital sovereignty as part of its broader security and governance strategy. They identify three approaches to digital sovereignty—traditional, post-sovereignist, and post-traditional—each reflecting different strategies for managing digital infrastructures. Moreover, they argue that digital sovereignty has both direct and indirect effects on European security integration, as the EU seeks to build independent infrastructures and reduce reliance on foreign technologies.

Other scholars, such as Roberts et al. (2021) and Sheikh (2022), focus on the institutional dynamics within the EU. Roberts et al. (2021) argue that while the EU lacks a cohesive vision of digital sovereignty, the concept has become central to policy debates on data governance, platform regulation, and cybersecurity, investigating the quest for legitimacy in the EU discourse on digital sovereignty. Sheikh (2022) proposes a "full stack" approach to digital policy, advocating for tailored strategies that address the EU's varying capabilities across different digital sectors by considering each technological layer.

Floridi (2020) argues that digital sovereignty is more effectively implemented at the EU level extending it to AI and 5G sovereignty, covering various aspects of European technologies. This approach complements national sovereignty by establishing a supranational framework, offering harmonization and integration, counterbalancing multinational corporations. Popular sovereignty remains the ultimate source of legitimacy, but its expansion to support supranational sovereignty requires innovative mechanisms. Furthermore, Floridi conceptualises sovereignty as a relational, non-rivalrous dynamic that enables legitimacy through network topologies—confederal, federated, or hybrid—each with distinct implications for the distribution and structuring of authority.

Scholars are divided on whether digital sovereignty is a viable concept, with some arguing it is incompatible with the borderless nature of cyberspace. A marginal, although relevant, position is held by those who reject the applicability of sovereignty in cyberspace, such as Mueller (2020). Mueller argues that the technical structure of the internet fundamentally undermines traditional territorial sovereignty. Mueller contends that cyberspace should be viewed as a global common, where states cooperate based on mutual rules rather than assert unilateral sovereign control. He highlights the transnational nature of digital infrastructures and warns that attempts to impose sovereignty in this space threaten global governance structures. For Mueller, the global digital domain requires a cooperative framework for managing interactions rather than sovereign competition. Mueller in particular is highly critical of recent attempts from state actors to establish digital sovereignty, seeing it as an authoritarian push, irrespective of the arguments behind it and the modalities in which this attempt is carried out (Mueller, 2021).

From a more theoretical angle Ruohonen (2021) critiques the application of classical sovereignty to the digital realm, arguing that its territorial foundations create contradictions when applied to digital assets, which often transcend national borders. Ruohonen identifies paradoxes in policy areas such as data protection and surveillance, suggesting that new theoretical models are needed to address the unique challenges of the digital age.

4 Sovereignty and Power Over the Cyberspace: The Perspectives of Non-State Actors

Besides state actors, Indigenous peoples have also discussed the concept of digital sovereignty, particularly regarding data control. States are not the only actors that have the ambition to exert their control over cyberspace. Indigenous data sovereignty is often discussed as a subset of broader debates of digital sovereignty; however, it is a different framework with other priorities and stakeholders. Digital sovereignty, in the discussion of state-actors, emanates from the standpoint of state jurisdiction, combined with ideas of states protecting strategic autonomy considering other states and private corporation outreaches. In the case of Indigenous peoples, digital sovereignty finds its origin in the essential entitlement of self-determination for Indigenous peoples in handling the information regarding themselves and their territories. While digital sovereignty emphasizes a national or supranational governance over data, indigenous data sovereignty puts forward indigenous peoples' claims to govern data collection, access, and use to ensure that they align with their values and governance structures, principles, and models, granting Indigenous people self-determination over cyberspace.

Indigenous data sovereignty emerges from a history of data being collected from Indigenous peoples by external authorities, often without consent, reciprocity, or meaningful benefit to the communities in question (Tsosie, 2019; Walter et al., 2020). Indigenous data sovereignty seeks to restore governance rights to Indigenous communities and nations regarding information related to their populations, territories, and cultural practices. As noted by Kukutai and Taylor (2016) this movement has arisen in response to data colonialism—the long-standing pattern of external entities exerting control over Indigenous data. It challenges the legacy of externally driven research and policy-making that treat Indigenous peoples primarily as subjects of data rather than as legitimate data stewards.

Unlike state-based digital sovereignty frameworks, which rely on territorial jurisdiction and formal legal instruments, Indigenous data sovereignty is grounded in Indigenous peoples' inherent rights recognized by international legal instruments such as the United Nations Declaration on the Rights of Indigenous Peoples (United Nation, 2007). Indigenous people have created key documents to shape a framework for Indigenous data sovereignty and governance, such as the Te Mana Raranuga (Kukutai & Taylor, 2016) and the Te Kauhai Raraunga (Kukutai et al., 2023). These rights include the principle that Maori data are key to ensure the self-determination and the authority to govern their digital assets. Indigenous digital sovereignty thus aligns with principles of Indigenous governance and nationhood, extending the con-

cept of sovereignty from land and resources to data ecosystems. As Walter et al. (2020) describe, this involves recognizing data as a cultural and economic asset that Indigenous peoples have the right to control, reflecting their own value systems and priorities.

One fundamental difference between an Indigenous and a state-based model of data sovereignty can be found in their underlying motivations and objectives. While states aim to obtain digital sovereignty in order to reinforce their power and regulatory authority, Indigenous communities use sovereignty over their data and digital assets in order to fight against historical injustices. Data, under this lens, represent a tool for self-determination of indigenous people. Carroll et al., (2019) stress how Indigenous data sovereignty does not pertain solely to legal jurisdiction. Fundamentally, it is about reshaping data ecosystem in a way that reflects Indigenous values. This ensure that decisions over data are made by and for Indigenous communities, thus carrying out a process of decolonisation to overcome historical practices of exclusion and exploitation.

State-based digital sovereignty and Indigenous sovereignty diverge also in the scale and structure of the modalities in which sovereignty is realised. State-based perspectives focus on national policymaking which applies to all citizens within their jurisdiction. This top-down approach seeks to ensure that, for instance, big corporations comply with national regulations and data protection rules. On the other hand, Indigenous data sovereignty posits that Indigenous communities, far from being a regular group of citizens to which state rule apply indiscriminately, are self-determining peoples with their own claims on data sovereignty and governance. As Tsosie (2019) and Oguamanam (2020) note, the aim of Indigenous data sovereignty is to establish a localised and nation-specific data governance model that can empower Indigenous communities granting them their capacity to decide over their own data.

5 The Strange Topology of Digital Sovereignty

While in the history of the regulation of cyberspace prominent political declarations and theories, like Barlow's declaration of independence[7] and Post and Johnson (1996) cyber-exceptionalism, have fathomed the internet as a space in which the ramifications of state authority could not apply, the evolution of cyberspace has proven otherwise. Internet exceptionalism viewed cyberspace as a special type of zone, devoid of historical social relations and legal frameworks, necessitating their complete reinvention. Advocates of this perspective called for abolishing existing regulations and establishing an entirely new governance system, where the state's predominant role would be supplanted by initiatives led by individual actors (Chenou, 2014). Others, like Wu (2011) have argued that there was no exception in the first place, and that states would have easily reasserted their control over the internet. Authoritarian states such as China, Russia and North Korea have in fact shown that the cyberspace can indeed be a region of domination and control from state actors,

[7] A Declaration of the Independence of Cyberspace | Electronic Frontier Foundation, accessed on the 10/12/2024.

whose reach extends also online, and whose ability to encroach political and civic liberties enjoyed digitally is on par with their ability to limit freedom offline. As originally the absence of traditional authorities occupying the cyberspace was considered (by Barlow and the "cyberlibertarian" tradition) as a virtue of the cyberspace, envisioning a reality whose freedom was guaranteed by as well as social peculiarities (its multi-stakeholder governance), progressively waned, and the political and the debate has shifted away from this perspective. Cyberspace has in fact undertook significant changes. The unparalleled amount of personal data that have been uploaded in the cyberspace, the pervasiveness of ubiquitous computing through the Internet of Things and the cloud technologies, as well as the increasing political and economic power of big corporations, have prompted regulators to rethink the approaches to the cyberspace. Furthermore, the rapid upscale and adoption of AI technologies have nudged national, supranational and international regulators to devise a mode of countering present and anticipating future harms and safety issues of AI technologies, from pernicious application to warfare to the most remote (but nonetheless ominous) possibilities of existential risks. So, it appears in the end that the call that opens Barlow's declaration:

> Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[8]

failed to gain traction, as the camp of anti-exceptionalism is vindicated. Is there anything else to be said to revamp the exceptionalist position? Digital sovereignty appears as one avenue in which this exceptionality can be observed. This exceptionalism is, however, far narrower than before, as it pertains only to the way in which states (and supranational entities) exert their sovereignty. I posit that this exceptionality stems from the very structure of cyberspace. Two key distinctive properties define this rupture: a) the topological structure of cyberspace and its borderless nature c) how state actors have applied digital sovereignty.

What happens at the stage in which there is not only this physical space, but there is something that crosses traditional political geographies, such as trans-border (Ganz et al., 2024) and cross-border data flows (Fahey, 2023)? Since the advent of the internet and the mass diffusion of ICT technologies, this question has become central to the reflection of the political philosopher, legal and political scholar investigating the cyberspace from a political perspective.

The disruptive nature of the digital goes hand in hand with the effects that it has on categories to understand the world. In his seminal work, *The Stack: On Software and Sovereignty* (Bratton, 2015) to my knowledge, the first scholar to engage with Carl Schmitt's theory from "The Nomos of the Earth" in the context of digital sovereignty. Bratton highlights a critical issue that remains underexplored in subsequent scholarship: the topological paradox of sovereignty in relation to the global technological

[8] A Declaration of the Independence of Cyberspace | Electronic Frontier Foundation accessed om the 10/12/2024.

stack. In its theory on the origin of the European public law (*Ius publicum europeum*), Carl Schmitt (Schmitt, 2006) discusses the role of the *land* as a determinant aspect of evolution of the European laws and institution, and, in parallel, sketches the development of the conception of sovereignty. The possibility of distinguishing an inside and outside (Schmitt, 2006, p. 45) through the division of a piece of geographical territory stands, according to Schmitt, as the possibility of the legal order among states as far as Europeans have conceived it through the turmoiled history of the evolution of their nations. Much debate over sovereignty has revolved around this principle and its applications to other type of spaces (such as the sea or the inner and outer sky), as it highlights a fundamentally spatial component of sovereignty.

Cyberspace, as a unique form of space, challenges traditional notions of territorial sovereignty. The constant flow of data streams across borders creates a dynamic in which state authority is fluid and ever-expanding. Sovereignty, according to Bratton, is not confined to fixed territorial boundaries but instead continuously reshapes itself, as each crossing of digital borders extends the reach of state power. This results in an overlapping and intertwined map of sovereignties that traverse one another, blurring the lines between inside and outside. As this overlapping unfolds, a new property of the sovereign space happens. The space in which sovereign nations exert their authority becomes twisted, shaping itself around the extensions of the control of other states. As if each state operates in its pocket, the control that a state has reach a limit point when applied to the other states authority. This cut across space in a layered and multidimensional modality, from the lowest material level (control over critical materials and cables) to the more abstract layers of data, clouds and AI, creating a multi-dimensional manifold in which states operate. Traces of that can be found even in traditional, spatialised versions of offline sovereignty. States use embassies to extend the reach of their action, as those ambassies are present in the sovereign territory of other states. Or use trade to project their power further away from the borders of their recognised territories. States also employ military bases abroad to extend their influence, establishing a physical presence within the jurisdiction of another sovereign state. They leverage international law, creating frameworks like extradition treaties or trade agreements to enforce their authority across borders[9]. Where can we find this difference?

We can represent a traditionally (mostly geographical) sovereign space as a shape that engulf the territory of a state. It encompasses its border; it extends upon its skies (where a state claims control over its airspace) as well as beneath the earth (where a state exert control over its infrastructure). It goes beyond the coastline as it also contains territorial waters. This shape is not continuous, as it is interspersed by ambassies or military bases that other states control. The dimension of traditional sovereignty is predominantly *spatialised* and *territorialised*, as the presence of a physical space of fixed dimensions set the limits on which the state can exercise its control. When it comes to the digital, space behaves differently. The internet is structurally made of networks and can be properly defined as a "network of networks".[10] Every network

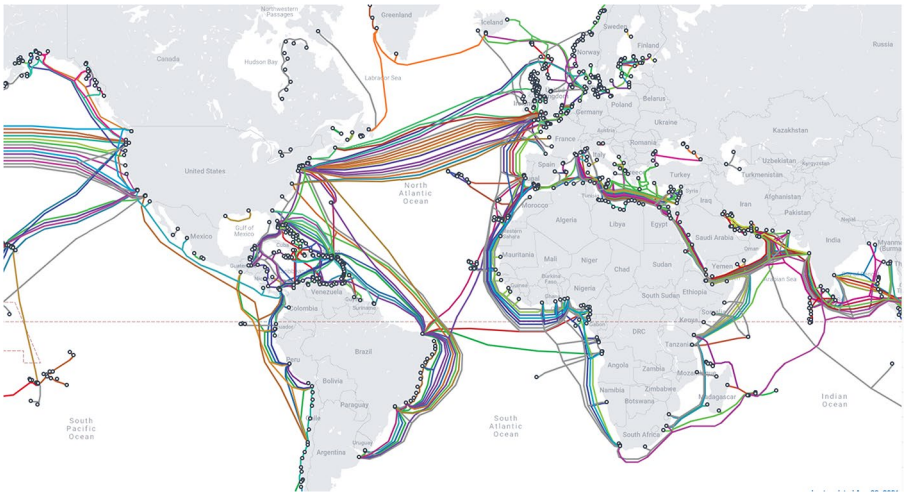
[9] I thank Prof. Juri Viehoff for pointing out the limitations of a "Westphalian" understanding of sovereignty, which confines sovereignty entirely within state territory.

[10] Basic Description, accessed on the 10/12/2024.

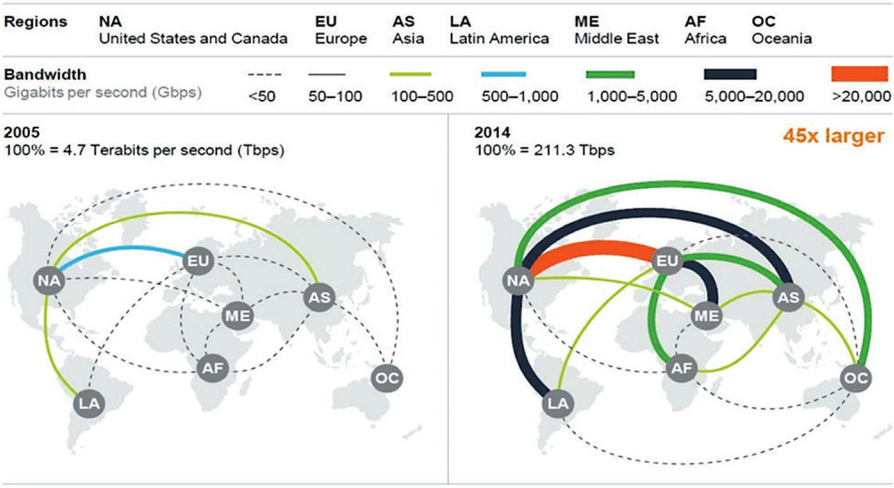
has a topology, which describes the way in which it is organised. From a mathematical perspective, this statement amount to truism, as it is trivial that the internet is a network, and that every network is organised in some way or another. What is less trivial is the fact that, I believe, this topology influences the way in which we can think of the power dynamics over the internet. And as the notion of sovereignty is primarily discussed within the extension (and limitations) of state powers, then a reflection on digital sovereignty should as well be concerned with clarifying what are the extensions (and limitations) of state power over cyberspace. How a state exercises its power over the cyberspace? How is this power limited by the presence of other states? What about the presence of other actors, such as private corporations, civic organisations and NGOs. In a nutshell: what is a state sovereign upon in cyberspace?

The physical space of the traditional pre and post Westphalian sovereignty is a space in which "things" move. Things are objects which have an extension and a position in a three-dimensional Euclidean plane: goods, animals, pilgrims, armies, borders.

The cyberspace of the digital sovereignty is a "space" in which information (data) flows through nodes connected by edges, that defy this conceptualization, traditional notions of "territories" and "borders" are hardly applicable, as there is no pre-existing spatial framework wherein entities and their relationships reside. Instead, the entities and their interconnections constitute the very essence of "space." Consequently, cyberspace is dynamically configured by the interactions and linkages among its components, with its structure defined by these relationships rather than by physical dimensions. In order to show this salient feature, the following maps will show (a) the structure of the submarine cables; (b) the evolution of cross-border data flows:



Map of submarine cables (from Ganz et al., 2024)



Changes in Global Data Flow Between Regions. Source: McKinsey Global Institute. (2016 de facto March) de facto in (Sarafanov & Shuqiang, 2017)

Submarine cables are extensive networks of undersea fiber-optic cables responsible for transmitting over 99% of global internet traffic. [11]

These infrastructures, which span oceans and connect continents, are critical for global telecommunications. Despite their significance, submarine cables present a unique challenge to digital sovereignty due to their transnational nature and ownership structure. Ganz et al. (2024) show very clearly the role that submarine cables have for sovereignty. The cross-jurisdictional nature of submarine cables, traversing multiple international territories and often lying in international waters, limits the ability of any single state to exert regulatory control. States frequently lack the authority to dictate routes, enforce standards, or implement adequate protection measures beyond their territorial waters, leaving them dependent on international cooperation and external actors. Moreover, the ownership of submarine cables is concentrated in the hands of private corporations and foreign states, creating dependencies that reduce a nation's autonomy over its telecommunications infrastructure. This dynamic not only diminishes a state's capacity to safeguard its digital infrastructure but also allows external actors to influence or intercept data traffic. Furthermore, the physical and operational vulnerabilities of submarine cables exacerbate these challenges. These infrastructures are susceptible to wiretapping, sabotage, and geopolitical manipulation, all of which pose significant risks to data privacy, security, and the continuity of digital services (Floridi et al., 2024, p. 11–13).

Data is often debated as the new "oil" of the 21st century.[12] The progressive increase in data flows across countries make data a crucial asset in the digital economy. Furthermore, data has a deeply political impact, as control over data flows enhance the capacity of a state to exercise its digital sovereignty through data sovereignty. Data sovereignty refers broadly to the authority of governments, organizations, or

[11] The deep-sea 'emergency service' that keeps the internet running, accessed on the 10/12/2024.

[12] Is data the new oil?, accessed on the 10/12/2024.

communities to control data that relates to their citizens, operations, or members. The concept has expanded beyond mere jurisdictional claims over digital information storage and processing. It now encompasses technical, legal, organizational, cultural, and ethical dimensions (Hummel et al., 2021; Von Scherenberg et al., 2024).

Initially, data sovereignty was often discussed in the context of national governments facing challenges as data cross borders via global cloud infrastructure (Irion, 2012; Nugraha & Sastrosubroto, 2015; Vaile, 2014). Governments strive to maintain exclusive jurisdiction over sensitive information, prompting data localization laws and domestic data storage solutions (De Filippi & McCarthy, 2012; Chander & Lê, 2014). These measures intend to safeguard privacy and national security. However, critics warn that strict localization may reduce cost efficiency, impede global data flows, and potentially restrict technological innovation (Ferracane, 2021).

At the supranational level, European digital sovereignty reflects efforts to maintain strategic autonomy in the digital sphere. The EU's data protection regimes, including the GDPR, represent attempts to extend data governance beyond territorial borders while shaping global standards (Christakis, 2020).

Data sovereignty thus intertwines with various governance models—state-led localization, Indigenous community-based stewardship, or European strategic autonomy—and involves negotiation between conflicting interests.

6 Embedding Control Over Digital Spaces

The cyberspace is a strange space. Kant famously remarked, in his attempt to build a republican constitution for the entire world, that humans must accept the fact that, no matter how far they wish to distance themselves, the earth is round, and they have to meet again at some point (Kant, 1991). But between two points in cyberspace can always exist a third point, as there is always new computational power that can be recruited to inflate the digital world. We cannot take the surface of the earth and create a new earth. But we can take the "surface" of cyberspace and create a new surface, and how large it will be depending on how much energy, data centre, can be utilised (thus posing serious environmental questions). A platform on the earth, from which a state exerts its sovereignty (a military outpost, an oil rig, a data centre) is always bound to the hard boundaries imposed by our inability to create new land. A platform on the cyberspace knows no such limit. What is more, the physical land can be walled, fenced, wired, bordered through military power. A state can limit the inflow and outflow of matter (goods, people) putting checkpoints and chokepoints which shape the fluxes. Cartographers can draw borders to substantiate a claim over a territory, states can create mythologies to justify the control over a portion of land. But, even against the backdrop of populist claims of sovereignty over borders in Europe and the US, humans always find always a way to defy the predicaments of states to rule over a land and cross each juncture in which two state authorities meet, at their frontiers. If the earth has a *nomos* which is grounded on land, this nomos has been violated constantly.

In this respect, cyberspace works differently. As Lessig pointed out (Lessig, 1997, 2000), a digital space has its rules embedded in it, as power over the cyberspace is

entrenched in its architecture. China and Russia serve as paradigmatic cases in examining how states structure cyberspace to consolidate control over digital interactions. In China, the Cybersecurity Law of 2017[13] mandates a real-name registration system, requiring individuals to authenticate their identities before accessing internet services such as online platforms. This policy integrates a regulatory infrastructure into the fabric of cyberspace, forging a direct link between the state's authority and the digital actions of its citizens. The real-name system removes anonymity, a cornerstone of cyberspace's early architecture, and reconfigures digital interactions to align with state objectives. Through linking online activity to verified identities, China ensures that cyberspace reflects party-sanctioned narratives and curtails the dissemination of dissenting perspectives.

This restructuring is not solely regulatory but architectural, embedding mechanisms that transform the digital realm into a space of governance. Internet service providers act as intermediaries co-opted into the state's apparatus of control. Bound by legal obligations, these entities enforce identity verification and monitor compliance with state directives. Their role, shaped by a network authoritarian model, positions them as enforcers of digital sovereignty, subordinated to the Chinese Communist Party's (CCP) directives. The CCP's influence extends further through proposals like Huawei's "New IP" (Mueller & Yoo, 2023) which envisions a redefined internet protocol system capable of enhancing state oversight.

Similarly, Russia's Sovereign Internet Law of 2019 constructs RuNet (Hu et al., 2019; Konradova, 2020), a domestically controlled internet segment capable of isolating itself from the global web. By centralizing internet traffic at state-regulated nodes and mandating ISPs to deploy deep packet inspection technology, Russia effectively reinscribes sovereignty into cyberspace. This reconfiguration enables the government to control, filter, and restrict flows of information, reasserting its dominion over a domain traditionally conceived as borderless. ISPs in Russia, like their Chinese counterparts, become instruments of the state, tasked with transforming the fluidity of the digital world into a controlled and bordered space.

The entrenchment of governance principles and rules do not pertain solely to authoritarian states. The European Union is carrying out a similar process when it comes to its digital identity and data policy. Through key pieces of legislation such as the Data Governance Act[14] and the Data Act[15], the EU aims to create an integrated data ecosystems that allows and facilitate for localised exchanged of data within the European Union territory, by crafting standards and governance bodies that create an ecosystem of common European dataspaces. When it comes to digital identity,

[13] https://digichina.stanford.edu/work/translation-cybIn%20China,%20the%20Cybersecurity%20Law%20of%202017rsecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/, accessed on the 10/12/2024.

[14] (Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA Relevance), 2022).

[15] (Regulation (EU), 2023/2854 of the European Parliament and of the Council of 13 December, 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA Relevance), 2023).

through the recent regulation on the European Digital Identity framework,[16] the EU aims to enshrine the principles of control over data and data minimisation (already present in the spirit and letter of the General Data Protection Regulation[17]) within an EU-based digital identity wallet (eIDAS Expert Group & European Commission, 2024) that uses cryptography to protect citizens' data and connections, aiming to give European citizens an enhanced control over their personal data.

7 Conclusions

This paper has investigated the contours of digital sovereignty, showcasing how the concept twists and reshapes itself to fit the goals of control and authority exerted by states, big corporations and Indigenous communities. Digital sovereignty is still a contested and multifaceted idea, which intersect both with traditional notion of territoriality and the borderless structure of cyberspace. States attempt to territorialize the digital, asserting authority over infrastructures and data flows. Their control is however limited because of the overlapping reach of other states. Further to this, the inherently transnational core of the cyberspace undermines the complete application of a traditional notion of sovereignty.

Digital sovereignty, as shown, operates across various layers: form the physical (submarine cables and data centres) to the virtual (cloud systems, artificial intelligence and control over digital platforms).[18] These layers establish a manifold of overlapping digital jurisdictions, where sovereignty is not singular neither static but continuously reshaped and reconceptualised through the actions of states, corporations and non-state actors. Further to this, the ability to entrench rules in the code that structures the cyberspace offers a window of opportunity for authoritarian states that is unparalleled in the physical realm, as well as paving the ground to democratic states to embed their values in the very fabric of the digital realm.

These findings highlight the necessity of further research, from an interdisciplinary perspective, to understand and address unresolved issues in the debate on digital sovereignty. Key questions are still to be answered. What are the practical and conceptual limits of state authorities in cyberspace? How can philosophers, legal scholars and political scientists pin down an evolving concept, addressing the unique properties of cyberspace? How the claim of indigenous communities seeking control and autonomy over their data can be addressed vis-à-vis the competing claim of states to control their (digital) borders and citizens? Engaging with these issues will bolster a conversation among scholars and policy makers in order to navigate the multifaceted and complex nature of digital sovereignty.

Authors Contribution The author is the only contributor to this manuscript.

[16] (Regulation (EU) 2024/1183 of the European Parliament and of the Council of 11 April 2024 Amending Regulation (EU) No 910/2014 as Regards Establishing the European Digital Identity Framework, 2024).

[17] (General Data Protection Regulation (GDPR), Regulation (EU) 2016/679, 2016).

[18] I thank Professor Barbara Henry for highlighting the importance of the material aspects of cyberspace in investigating power dynamics over the internet.

Funding Open access funding provided by Scuola Superiore Sant'Anna within the CRUI-CARE Agreement.
No funding applicable.

Data Availability Not applicable.

Code Availability Not applicable.

Declarations

Ethical Approval Not applicable.

Consent for Publication The author consent to the submission of this paper.

Competing Interests The authors have no financial or proprietary interests in any material discussed in this article.

References

Agnew, J. (2005). Sovereignty regimes: Territoriality and state authority in contemporary world politics. *Annals of the Association of American Geographers*, *95*(2), 437–461. https://doi.org/10.1111/j.1467-8306.2005.00468.x

Armstrong, D. (1993). The Westphalian conception of international society. In D. Armstrong (Ed.), *Revolution and world order: The revolutionary state in international society* (p. 0). Oxford University Press. https://doi.org/10.1093/0198275285.003.0002

Beaulac, S. (2003). *The social power of Bodin'S 'Sovereignty' and international law*. *4*. https://law.unimelb.edu.au/__data/assets/pdf_file/0010/1680337/Beaulac.pdf

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

Bratton, B. H. (2015). *The stack: On software and sovereignty*. MIT Press.

Carroll, S. R., Rodriguez-Lonebear, D., & Martinez, A. (2019). Indigenous data governance: Strategies from united States native nations. *Data Science Journal*, *18*(1), 31. https://doi.org/10.5334/dsj-2019-031

Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory LJ*, *64*, 677.

Chenou, J. M. (2014). From Cyber-Libertarianism to neoliberalism: internet exceptionalism, Multi-stakeholderism, and the institutionalisation of internet governance in the 1990s. *Globalizations*, *11*(2), 205–223. https://doi.org/10.1080/14747731.2014.887387

Christakis, T. (2020). *'European digital sovereignty': Successfully navigating between the 'Brussels effect' and Europe's quest for strategic autonomy* (SSRN Scholarly Paper No. 3748098). Social Science Research Network. https://doi.org/10.2139/ssrn.3748098

Cong, W., & Thumfart, J. (2022). A Chinese precursor to the digital sovereignty debate: digital Anti-Colonialism and authoritarianism from the Post–Cold war era to the Tunis agenda. *Global Studies Quarterly*, *2*(4), ksac059. https://doi.org/10.1093/isagsq/ksac059

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

Croxton, D. (1999). The peace of Westphalia of 1648 and the origins of sovereignty. *The International History Review*, *21*(3), 569.

De Filippi, P., & McCarthy, S. (2012). Cloud computing: Centralization and data sovereignty. *European Journal of Law and Technology*, *3*(2). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2167372

eIDAS Expert Group, & European Commission (2024). *European Digital Identity Wallet Architecture and Reference Framework, Version 1.1.0*. GitHub Pages. https://eu-digital-identity-wallet.github.io/eudi-doc-architecture-and-reference-framework/1.1.0/arf/

Fahey, E. (2023). Does the EU's digital sovereignty promote localisation in its model digital trade clauses? *European Papers - A Journal on Law and Integration*, *2023 8*, 503511. https://doi.org/10.15166/2499-8249/670. [Text/html,PDF].

Ferracane, M. F. (2021). The costs of data protectionism. In M. Burri (Ed.), *Big data and global trade law* (pp. 63–82). Cambridge University Press. https://doi.org/10.1017/9781108919234.005

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369–378. https://doi.org/10.1007/s13347-020-00423-6

Gábriš, T., & Hamuľák, O. (2021). Pandemics in Cyberspace – Empire in search of a sovereign? *Baltic Journal of Law & Politics*, *14*(1), 103–123. https://doi.org/10.2478/bjlp-2021-0005

Ganz, A., Camellini, M., Hine, E., Novelli, C., Roberts, H., & Floridi, L. (2024). Submarine cables and the risks to digital sovereignty. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4693206

Geenens, R. (2016). E pluribus unum? The manifold meanings of sovereignty. *Netherlands Journal of Legal Philosophy*, *45*(2), 15–36. https://doi.org/10.5553/NJLP/.000051

General Data Protection Regulation (GDPR) (2016). Regulation (EU) 2016/679, L 119 official journal of the European union. 1.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Gueham, F. (2017). *Digital sovereignty*. Fondation pour l'innovation politique. https://www.fondapol.org/app/uploads/2020/06/f-gueham-digital-sovereignty-3.pdf

Hu, X., Naiel, M. A., Wong, A., Lamm, M., & Fieguth, P. (2019). RUNet: A robust UNet architecture for image super-resolution. *Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops*, 0–0. http://openaccess.thecvf.com/content_CVPRW_2019/html/WiCV/Hu_RUNet_A_Robust_UNet_Architecture_for_Image_Super-Resolution_CVPRW_2019_paper.html?ref=https://githubhelp.com

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 205395172098201. https://doi.org/10.1177/2053951720982012

Irion, K. (2012). Government cloud computing and National data sovereignty. *Policy & Internet*, *4*(3–4), 40–71. https://doi.org/10.1002/poi3.10

Johnson, D. R., & Post, D. (1996). Law and borders: The rise of law in cyberspace. *Stanford Law Review*, *48*(5), 1367. https://doi.org/10.2307/1229390

Kant, I., Nisbet, H. B., & Reiss, H. S. (1991, January 25). *Kant: Political Writings*. Higher Education from Cambridge University Press; Cambridge University Press. https://doi.org/10.1017/CBO9780511809620

Konradova, N. (2020). The Rise of Runet and the Main Stages of Its History. In S. Davydov (Ed.), *Internet in Russia* (pp. 39–61). Springer International Publishing. https://doi.org/10.1007/978-3-030-33016-3_3

Kukutai, T., & Taylor, J. (Eds.). (2016). *Indigenous data sovereignty* (1st ed.). ANU Press. https://doi.org/10.22459/CAEPR38.11.2016

Kukutai, T., Campbell-Kamariera, K., Mead, A., Mikaere, K., Moses, K., Whitehead, J., & Cormack, D. (2023). *Māori data governance model*. Te Kāhui Raraunga.

Lambach, D. (2020). The territorialization of cyberspace**. *International Studies Review*, *22*(3), 482–506. https://doi.org/10.1093/isr/viz022

Lessig, L. (1997). Reading the constitution in cyberspace. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.41681

Lessig, L. (2000). *Code and other laws of cyberspace*. Basic Books.

Madiega, M. (2020). Digital sovereignty for Europe. *European Parliamentary Research Service*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf

Moerel, L., & Timmers, P. (2021). Reflections on Digital Sovereignty. *EU Cyber Direct - Supporting EU Cyber Diplomacy*. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3772777

Mueller, M. L. (2020). Against sovereignty in cyberspace. *International Studies Review*, *22*(4), 779–801. https://doi.org/10.1093/isr/viz044

Mueller, M. (2021). *Digital sovereignty: What does it mean?* Internet Governance Project. https://www.internetgovernance.org/wp-content/uploads/Digital-sovereignty-IGF2021.pdf

Mueller, A., & Yoo, C. S. (2023). *Crouching Tiger, Hidden Agenda? The Emergence of China in the Global Internet Standard-Setting Arena* (SSRN Scholarly Paper No. 4528546). Social Science Research Network. https://doi.org/10.2139/ssrn.4528546

Nugraha, Y., & Sastrosubroto, A. S. (2015). *Towards data sovereignty in cyberspace*. 465–471.

Oguamanam, C. (2020). Indigenous peoples, data sovereignty and self-determination: Current realities and imperatives. *The African Journal of Information and Communication*, *26*. https://doi.org/10.23962/10539/30360

Osiander, A. (2001). Sovereignty, international relations, and the Westphalian myth. *International Organization*, *55*(2), 251–287. https://doi.org/10.1162/00208180151140577

Philpott, D. (1995). Sovereignty: An introduction and brief history. *Journal of International Affairs*, *48*(2), 353–368.

Piirimäe, P. (2010). The Westphalian myth and the idea of external sovereignty. In H. Kalmo & Q. Skinner (Eds.), *Sovereignty in Fragments: The Past, Present and Future of a Contested Concept* (pp. 64–80). Cambridge University Press. https://doi.org/10.1017/CBO9780511675928.004

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

Regulation, E. U. (2022). /868 of the European Parliament and of the Council of 30 May 2022 on European Data Governance and Amending Regulation (EU) 2018/1724 (Data Governance Act) (Text with EEA Relevance), OJ L 152, 3.6.2022 PE/85/2021/REV/1 1 (2022).

Regulation, E. U. (2024). 2024/1183 of the European Parliament and of the Council of 11 April 2024 amending regulation (EU) 910/2014 as regards Establishing the European digital identity framework, L 1183. *Official Journal of the European Union* 73.

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December (2023). 2023 on Harmonised Rules on Fair Access to and Use of Data and Amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act) (Text with EEA Relevance), 2023/2854, OJ L, 2023/2854 PE/49/2023/REV/1 https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32023R2854&qid=1726838497896

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. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

Ruohonen, J. (2021). The treachery of images in the digital sovereignty debate. *Minds and Machines*, *31*(3), 439–456. https://doi.org/10.1007/s11023-021-09566-7

Sarafanov, I., & Shuqiang, B. (2017). *A study on the cooperation mechanism on digital trade within the WTO framework-based on an analysis on the status and barriers to digital trade*.

Schmitt, C. (2006). *The nomos of the earth in the international law of the Jus Publicum Europaeum* (G. L. Ulmen, Trans.; First paperback edition). Telos Press.

Sheikh, H. (2022). European digital sovereignty: A layered approach. *Digital Society*, *1*(3). https://doi.org/10.1007/s44206-022-00025-z

Shibasaki, A. (2014). Myths in a discipline: IR and the peace of Westphalia. *Journal of Global Media Studies*, *14*(March 2014), 41–52. 14, 41–52.

Thumfart, J. (2021). The COVID-Crisis as catalyst for the norm development of digital sovereignty. Building barriers or improving digital policies? *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3793530

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

Tsosie, R. A. (2019). Tribal data governance and informational privacy: Constructing 'indigenous data sovereignty'. *80 Montana Law Review*, *229*, 41.

United Nation (2007). *UN Declaration on Indigenous People*. https://www.un.org/development/desa/indigenouspeoples/wp-content/uploads/sites/19/2018/11/UNDRIP_E_web.pdf

Vaile, D. (2014). The cloud and data sovereignty after Snowden. *Journal of Telecommunications and the Digital Economy*, *2*(1), 31–31.

Von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. *Electronic Markets*, *34*(1), 15. https://doi.org/10.1007/s12525-024-00693-4

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

Weber, M., Matthews, E., & Runciman, W. G. (1978, March 30). *Max Weber: Selections in Translation*. Higher Education from Cambridge University Press; Cambridge University Press. https://doi.org/10.1017/CBO9780511810831

Wu, T. (2011). Is internet exceptionalism dead? *The next digital decade: Essays on the future of the internet*,. https://scholarship.law.columbia.edu/faculty_scholarship/1676?utm_source=scholarship.law.columbia.edu%2Ffaculty_scholarship%2F1676%26utm_medium=PDF%26utm_campaign=PDFCoverPages