

Pohle, Julia; Nanni, Riccardo; Santaniello, Mauro

Article — Accepted Manuscript (Postprint)

Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices

Policy & Internet

Provided in Cooperation with:

WZB Berlin Social Science Center

Suggested Citation: Pohle, Julia; Nanni, Riccardo; Santaniello, Mauro (2025) : Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices, Policy & Internet, ISSN 1944-2866, Wiley, Hoboken, NJ, Vol. 16, Iss. 4, pp. 666-671, <https://doi.org/10.1002/poi3.437>

This Version is available at:

<https://hdl.handle.net/10419/335910>

Standard-Nutzungsbedingungen:

Die Dokumente auf EconStor dürfen zu eigenen wissenschaftlichen Zwecken und zum Privatgebrauch gespeichert und kopiert werden.

Sie dürfen die Dokumente nicht für öffentliche oder kommerzielle Zwecke vervielfältigen, öffentlich ausstellen, öffentlich zugänglich machen, vertreiben oder anderweitig nutzen.

Sofern die Verfasser die Dokumente unter Open-Content-Lizenzen (insbesondere CC-Lizenzen) zur Verfügung gestellt haben sollten, gelten abweichend von diesen Nutzungsbedingungen die in der dort genannten Lizenz gewährten Nutzungsrechte.

Terms of use:

Documents in EconStor may be saved and copied for your personal and scholarly purposes.

You are not to copy documents for public or commercial purposes, to exhibit the documents publicly, to make them publicly available on the internet, or to distribute or otherwise use the documents in public.

If the documents have been made available under an Open Content Licence (especially Creative Commons Licences), you may exercise further usage rights as specified in the indicated licence.

Editorial

Unthinking Digital Sovereignty: A Critical Reflection on Origins, Objectives, and Practices

Julia Pohle¹, Riccardo Nanni², Mauro Santaniello³

¹WZB Berlin Social Science Center, Berlin, Germany

²Digital Commons Lab, Fondazione Bruno Kessler, Trento, Italy

³Department of Management & Innovation Systems (DISA-MIS), University of Salerno, Salerno, Italy

Correspondence: Julia Pohle (julia.pohle@wzb.eu)

“Digital sovereignty” is the political buzzword of the hour. Over the last decade, it has gone from being a vague idea invoked by a few policymakers and activists to a political slogan with global appeal. It was in 2016 that its growing popularity became especially clear. That year, Donald Trump was elected US president for the first time, with a protectionist agenda that included banning selected Chinese tech companies from the US market (Thumfart 2022); the EU adopted its General Data Protection Regulation (GDPR), which imposed rules that applied to actors outside EU territory for the first time (Chen, Frey, and Presidente 2020); and China adopted the Cybersecurity Law, establishing key provisions for data protection and localization and laying the groundwork for broader regulations on data, platforms and infrastructures (Creemers 2020).

While the ideas underlying digital sovereignty are much older, the adoption of regulations and stances by these three major powers prompted new political debates on sovereignty (Danet and Deforges 2020; Pohle and Thiel 2020). Over the past decade, a growing number of governments, organizations, and groups have sought to lend this term (or connected terms such as internet sovereignty, technology self-sufficiency, strategic technological autonomy, or data sovereignty) their own meaning, as illustrated throughout this special issue. These actors do not solely include major world powers with strong leverage in shaping digital markets and policies. In fact, emerging powers, private organizations, and groups such as Indigenous populations are also seeking to establish their own views on digital sovereignty and to enforce them through technical arrangements, regulations, or economic practices (Cong and Thumfart 2022; Glasze et al. 2023; Roberts et al. 2021; Walter et al. 2020). As a result, digital sovereignty has now become a much more encompassing concept, addressing issues of digital communication and connection but also the much wider digital transformation of societies. While some still criticize digital sovereignty efforts as disguised protectionism or technological nationalism, the concept is now often used as a shorthand for an ordered, regulated, and secure digital sphere—a digital sphere, in which the multifaceted problems of individual rights and freedoms, collective and infrastructural security, political and legal enforceability and fair economic competition are finally resolved. In addition, in Western democracies' discourses, there is also a growing emphasis on internal

sovereignty and democratic sovereignty with regard to the digital sphere. As such, the concept of digital sovereignty is understood as a prerequisite for citizens to be able to shape the process of digital transformation in a self-determined and democratic manner. This understanding is, however, not globally shared and thus gives rise to the ever-growing number of meanings of digital sovereignty.

This special issue, titled *Unthinking Digital Sovereignty*, explores a number of definitions and perspectives on digital sovereignty from Europe, the United States, China, India, South Africa, Uganda, and Indigenous communities, with a case study on Mexico. The articles in it offer a re-examination and critical deconstruction/reconstruction of the digital sovereignty debate through various perspectives and disciplinary approaches. Yet, this special issue is not an exhaustive anthology of critical views on digital sovereignty. Rather, the different contributions aim to offer readers a foundation for reflecting on the discourses, practices, and dynamics shaping current debates on digital sovereignty and evolving relationships within global digital governance.

1. Thinking Digital Sovereignty

While the term “digital sovereignty” dates back to the 1990s (Cong and Thumfart 2022; Glasze et al. 2023), it has only recently surged in popularity in academic and policy circles with the increasing politicization of technology. Today, it is invoked across various political and economic contexts, from more centralized and authoritarian countries to liberal democracies. Over time and across regions, it has acquired a large range of connotations. Although all understandings and narratives of digital sovereignty consistently share some core elements, they diverge based on the national contexts, the actor configurations and the forms of self-determination they prioritize (Couture and Toupin 2019). We align with Lambach and Oppermann's view that it is precisely the broad, adaptable nature of “digital sovereignty” that makes it appealing to diverse actors: its openness “is not a bug, but a feature. Digital sovereignty has not had a successful career despite its protean nature but because of it” (Lambach and Oppermann 2022).

Due to the diversity of narratives attached to digital sovereignty, the majority of the existing research on the concept and its political repercussions has focused on discourses and practices in specific regions and countries. Particular attention has been paid to the European Union and its member states (Adler-Nissen and Eggeling 2024; Carver 2024; Floridi 2020; Lambach and Monsees 2024; Monsees and Lambach 2022; Pizzul and Veneziano 2024), and for good reason: The European debate on digital sovereignty is indeed a prominent example of how the concept has different meanings in different policy realms, even within the same country or block of countries. For example, the French concept of *souveraineté numérique*, which was introduced in the mid-2000s and first mentioned in a parliamentary debate in 2012, follows a rather classical understanding of sovereignty associated with democracy, the rule of law and territoriality. It was developed primarily in opposition to the perceived hegemony of US digital technology providers and the resulting French dependence on them (Musiani 2013; Thumfart 2022). At the same time, in Germany, demands for “digital sovereignty” only emerged after the Snowden revelations in 2013 and the comprehensive surveillance, not only of ordinary users but also of top German politicians, became public knowledge (Glasze et al. 2023). While the German debate thus also focuses on independent digital infrastructures and the protection of data flows, it is less state-centered than the one in France. Instead, it also emphasizes the need for user sovereignty, that is, the capacity of each individual to be in control in the digital sphere (Pohle 2020). Both the French and the German debates thus also differ from those at EU level. For instance, Charles Michel, serving as president of the European Council at the time of writing, has described digital sovereignty as a tool for strategic autonomy, with the latter being “about being able to make choices [...] this means reducing our dependencies, to better defend our interests and our values” (European Council 2021). Similarly, the European Parliament's own think tank, the European Parliamentary Research Service (EPRS), has defined digital sovereignty as “Europe's ability to act independently in the digital world” (Madiaga 2020). Both definitions address the EU's willingness to build, retain, and protect its own decision-

making autonomy in the digital field. However, they fall short of defining what the field includes and what autonomy entails: while the often-cited objective is reducing the EU's dependence on US and Chinese technology (Dixon 2022), the establishment of an “EU stack,” in the sense of a value chain of digital technologies fully produced in Europe from semiconductors to infrastructure and the platforms that run on top of it, is an unrealistic one. Nonetheless, initiatives such as DNS4EU can be seen as part of an attempt to make the intra-EU digital infrastructure less prone to negative external influences (Kulikova 2021).

Demanding digital sovereignty to express a desire for more autonomy in times of digital interconnectedness is most certainly not a unique European feature. China began deploying its concepts of internet sovereignty and information sovereignty in the 1990s. The country's policies have thus been a focus of much academic scrutiny (Creemers 2020; Hong and Goodnight 2019; Nanni 2022; Zeng, Stevens, and Chen 2017). Information sovereignty refers to the Chinese government's attempts to control information flows within the country amid the rise of digitalization and the increasing ubiquity of internet connectivity—a major target of Chinese investment from the late 1980s onward (Cong and Thumfart 2022; Gong 2005). The 2010 White Paper on (the Status of) the Internet in China is credited in the literature as China's first attempt to formalize internet sovereignty in a policy paper (Creemers 2020). In the Chinese debate, concepts such as internet sovereignty and information sovereignty have different origins than in the European debate. While the EU is concerned by the fact that it lacks major tech companies capable of competing with the United States and Chinese giants in device production, network manufacturing, and the platform economy (Roberts et al. 2021), in China, the debate is driven by a fear of foreign interference. This fear can be subdivided into a fear that countries will interfere through foreign propaganda, the definition of which often entails dissenting, politically sensitive opinions from Communist Party dictates, and a fear of (cultural) imperialism based on China's past as a country that underwent colonialism (Cong and Thumfart 2022).

Besides addressing the popular topics of China and the EU, a growing number of studies have analyzed how the concept of digital sovereignty is applied in other authoritarian countries, most prominently Russia (Budnitsky and Jia 2018; Daucé and Musiani 2021; Litvinenko 2021), and in the countries of the so-called “Global South” (Basu 2023; Gehl Sampath and Tregenna 2022). Findings indicate that BRICS countries are increasingly prioritizing the development of cybersecurity frameworks, with a particular focus on data privacy regulations and digital policies designed to reaffirm national sovereignty and reduce the influence of foreign technology companies and governments (Belli 2021; Ifeanyi-Ajufo 2023). A similar securitarian discourse on digital sovereignty, emphasizing the need to protect the state from digital threats, can also be observed in the Euro-Mediterranean region, particularly in North Africa and West Asia (Santaniello, forthcoming). However, the actions undertaken under the auspices of digital sovereignty extend beyond mere security concerns. In Africa, for instance, the emphasis on digital sovereignty can be seen as both a form of resistance to foreign digital dominance and a tool for reinforcing and justifying authoritarian governance practices (Shaheed and Greenacre 2021).

Claims of digital sovereignty extend beyond governments and states, yet research on how nonstate actors engage with this concept—and how their claims manifest in concrete practices—remains scarce. Some existing studies focus on how Indigenous communities worldwide are interacting with digital technologies, using them to revitalize and promote cultures and educational practices that were once suppressed by colonial powers. Others examine the physical internet infrastructure and hardware production, especially when they impact ancestral lands, thus bringing into sharp focus the debate around digital colonialism as a new dimension of the pursuit of digital sovereignty by global powers (Caranto Morford and Ansloos 2021; Couture and Toupin 2019; Young 2019).

Almost all of these understandings of digital sovereignty share a common feature: digital sovereignty is framed primarily as a process rather than a status. Actors invoke digital sovereignty to articulate the objective of strengthening self-determination and the capacity to act in globally networked societies. However, while the aspiration of digital sovereignty thus indicates the path towards a brighter future,

actors rarely present it as an objective that can ever be a final, attainable endpoint. And the anticipated journey varies depending on the specific context in which the concept is applied.

2. Unthinking Digital Sovereignty

This special issue is based on a recognition that digital sovereignty is a social construct. As such, it is conveyed through a series of narratives and pursued through policies, technological practices and legislation that invoke it and, in return, derive legitimacy from this reference. Hence, when we speak of “unthinking” digital sovereignty, we draw on Wallerstein's (1991) idea of “unthinking” as the process of reversing, dismissing, and unlearning previously established concepts. The goal is not to replace the concept or its meanings with new ones but rather to critically address them from nonconventional perspectives. Consequently, “unthinking” digital sovereignty first and foremost involves disconnecting the concept of digital sovereignty from the notion of Westphalian sovereignty. As we have argued, the discourse on digital sovereignty does not solely originate from nation states, nor is it tied to them. Additionally, “unthinking” digital sovereignty suggests that scholars studying sovereignty in the digital space do not occupy a neutral position; instead, their work plays a constitutive role in those policies and practices that invoke the concept as a source of legitimacy. Hence, “unthinking” digital sovereignty places epistemology at the core of the discussion on digital governance, inviting a critical examination of the frameworks, agendas, and academic debates that shape our understanding of sovereignty in the digital realm.

Another implication of the “unthinking” approach is that the rise of digital sovereignty as a set of discourses and practices cannot be understood in isolation. Instead, it is part of a broader power struggle over digital governance, which itself is woven into fiercely contested and at times violent battles for global hegemony. This implies that a critical perspective on digital sovereignty needs to be both relational and historical. It must consider relations between world regions rather than between individual nation-states, and it must consider the dynamics between individuals, groups, and institutions rather than solely between governments. In addition, it should investigate long-term historical processes rather than isolated events, bringing path dependencies and structural relationships to the fore. As Bannerman (2022) has observed “sovereignty comes from relations,” meaning that neither individuals nor states nor platforms can be conceived of as self-contained and autonomous entities. Rather, they are the product of a network of historical and social relations that determine their sovereignty. Understanding digital sovereignty thus requires the acknowledgment of class, gender, race, and socioeconomic, colonial, material, and spatial relationships as they have evolved over centuries.

Moreover, when “unthinking” digital sovereignty, scholars must also address the much-neglected question of how digitally sovereign powers can be controlled. In many instances, the idea of strengthening digital sovereignty does not just mean actively managing dependencies but also creating central control points for digital infrastructures and applications. Therefore, much more reflection is needed on how sovereign powers can be held accountable. It is not sufficient to propose that private actors' power could be tamed by public institutions to protect user rights, as many democratic governments across the world have done. Likewise, it is too simplistic to equate sovereignty with the ability to defend liberal and democratic values, as is often the case for discourses on digital sovereignty in Europe. For centuries, there has been an ongoing struggle to organize sovereign powers in a way that allows for liberal and pluralistic societies to flourish. Thus, the “unthinking” of digital sovereignty must also include debating the procedural frameworks that structure sovereign capabilities and how they can be opened up to public reflection and control. In other words, invoking digital sovereignty also entails advocating for its constitutionalization, implying a collective effort to set limits on the exercise of digitally sovereign powers and to establish new checks and balances.

Finally, “unthinking” digital sovereignty must resist the temptation to consider the related objectives and practices in political, economic, or juridical terms alone. Understanding digital sovereignty requires

a holistic approach that escapes the artificial separation between social spheres—a separation that is constitutive of the dominant paradigm of digital governance, the multistakeholder governance approach, against which the digital sovereignty discourse is often formulated.

3. Special Issue Structure

This special issue features six articles that seek to “unthink” digital sovereignty by deconstructing and (re)conceiving it from different viewpoints. While some of the issue's contributions provide much-needed conceptual and theoretical foundations for analyzing, contextualizing, and interpreting the discourses and practices of digital sovereignty, others reexamine various concepts linked to digital sovereignty by critically assessing how policy actors have envisioned and narratively shaped it through selected case studies. Finally, this special issue also foregrounds postcolonial perspectives, exploring digital sovereignty through the lenses of emerging powers, Indigenous communities, and developing countries. All contributions, whether presenting new empirical research or commentary, apply a critical perspective to the concept of digital sovereignty, thereby offering readers new avenues for reflection.

The first contribution, by Pohle and Santaniello (2024), sets the stage by critically discussing the discursive shift from multistakeholder internet governance to digital sovereignty. The article demonstrates that digital sovereignty is not a static condition but a dynamic discourse shaped by power struggles involving both state and nonstate actors. It underscores how digital sovereignty is being redefined across various political contexts and through multiple conflicts. The dialectic between multistakeholderism and digital sovereignty explored in this article supports a relational and historical approach, as it examines how these discourses emerge, compete and evolve within broader geopolitical dynamics.

The focus on multistakeholder internet governance and geopolitical tensions also forms the background to the second contribution. This article, by ten Oever et al. (2024), presents a three-part discussion of EU sanctions against Russian media in the aftermath of Russia's invasion of Ukraine. After showing the uneven implementation of these sanctions by EU member states, the authors discuss how the sanctions align with the EU's digital sovereignty agenda. Building on these findings, they argue that EU digital sovereignty policies and sanctions mark the rise of a repressive state apparatus that operates in tandem with the ideological apparatus of multistakeholder internet governance, thus forming a metagovernance regime. All actors involved in these dialectical relationships aim to preserve the appearance of technological neutrality to continue to develop and adapt global communication networks.

Exploring yet another political dynamic, in a third contribution, Nanni et al. (2024) ask “Is individual digital sovereignty attainable for the EU?”. To do so, they compare two politically distant actors that have both engaged in strong regulatory efforts concerning data and platforms: the EU and China. In particular, this article looks at AI and data governance regulations due to their centrality in discourse and politics. The authors unpack EU digital sovereignty narratives focusing on individual empowerment by comparing EU regulations with China's legislation and argue that current EU regulatory efforts will fall short of their declared objective to uphold individual autonomy without a strong domestic digital industry. The analysis draws on Chinese legislation and the EU's burgeoning digital regulation since 2016 when the EU's GDPR and China's Cybersecurity Law spurred policy and scholarly discussions on data protection, data localization, and digital sovereignty.

Shifting the focus from the EU to other world regions, the fourth contribution, by Jiang (2025), analyzes digital sovereignty models emerging in China, India, and South Africa—three BRICS countries that collectively represent over one-third of the global population and are developing distinct digital governance approaches that diverge from those of the United States and the EU. The article aligns with the idea of “unthinking digital sovereignty” by challenging narrow and Western-centric interpretations of digital sovereignty as merely state control over digital infrastructure. Instead, it emphasizes the importance of local contexts and diverse political-economic positions by examining how these nations'

diverse models of digital sovereignty are shaped within historical center-periphery dynamics at the intersection of development, authoritarianism, and anticolonialism. For example, China's emphasis on a self-sufficient digital ecosystem, India's focus on digital public infrastructures, and South Africa's strategy of balancing foreign technology reliance with localized policies illustrate that digital sovereignty is neither uniform nor static. Instead, the article underscores how digital sovereignty is a multifaceted, relational construct that is influenced by historical processes and global power dynamics among state and nonstate actors.

Nonstate actors are also the subject of the fifth contribution, by Couture et al. (2024). The authors seek to “unthink” digital sovereignty by moving beyond state-centric narratives—in particular, those by powerful states—and instead examine civil society digital sovereignty and Indigenous digital sovereignty, with a particular focus on the concept of “data sovereignty” developed by certain Indigenous groups. The authors approach the topic from a mixed positionality: one of the authors is an Indigenous person from Mexico, while the two others are nonindigenous civil society experts. The article makes four contributions to reframing digital sovereignty: (1) The values of autonomy and self-determination extend beyond state-centric models; (2) Digital sovereignty includes an important cultural dimension; (3) The aspect of “openness” emerges as a point of tension between perspectives; and (4) The concept of “sovereignty” itself, with its complex history and varied interpretations, is central to these discussions.

The postcolonial perspective on digital sovereignty is also the main lens through which Kalema (2024) critically examines the ambitions behind digital public infrastructure projects in Africa in the sixth contribution. The author criticizes digital transformation for development (DX4D) efforts for their technocratic and depoliticized appearance, which obscures these projects' value extraction, control dynamics, and political and geoeconomic implications, especially for the involved countries' digital self-determination. Describing DX4D efforts as an “antipolitics machine,” the article highlights how digital public infrastructure projects embed infrastructural ideologies, which influence governance, algorithmic oversight, and societal well-being. It further uses the case study of Uganda's large-scale DX4D projects to explore how these projects' coercive and material effects shape the futures of low-and-lower-middle-income countries in the Global South and, ultimately, under the guise of public-sector reform, advance hegemonic interests while sidelining public values and local strategic interests.

This special issue does not aim to provide a comprehensive review of the disciplinary and theoretical viewpoints through which digital sovereignty can be revisited, deconstructed, or “unthought.” However, with its ambition to provide perspectives going beyond the mainstream focus on global digital power, the contributions mark a useful starting point for reflection on the ways in which digital sovereignty, in its many facets, can be deconstructed and (re)addressed. Our ambition as guest editors of this special issue is to launch a conversation among scholars interested in a critical perspective on ongoing and future policy debates on digital technologies and their societal implications.

Acknowledgments

The idea for this special issue stems from a workshop held in May 2023, organized by the issue's editors and hosted and funded by the Center for Advanced Internet Studies (CAIS) in Bochum, Germany. The editors wish to express their gratitude to CAIS for its generous support of both the workshop and this resulting publication.

References

Adler-Nissen, R., and K. A. Eggeling. 2024. “The Discursive Struggle for Digital Sovereignty: Security, Economy, Rights and the Cloud Project Gaia-X.” *Journal of Common Market Studies* 62, no. 4: 993–1101. <https://doi.org/10.1111/jcms.13594>.

- Bannerman, S. 2022. “Platform Imperialism, Communications Law and Relational Sovereignty.” *New Media & Society* 26, no. 4: 1461–4448. <https://doi.org/10.1177/14614448221077284>.
- Basu, A. 2023. “Defending the ‘S Word’: The Language of Digital Sovereignty Can be a Tool of Empowerment.” In *New Digital Dilemmas: Resisting Autocrats, Navigating Geopolitics, Confronting Platforms*, 19–22. Washington, DC: Carnegie Endowment for International Peace.
- Belli, L. 2021. “BRICS Countries to Build Digital Sovereignty.” In *CyberBRICS: Cybersecurity Regulations in the BRICS Countries*, edited by L. Belli, 271–280. Springer International Publishing. https://doi.org/10.1007/978-3-030-56405-6_7.
- Budnitsky, S., and L. Jia. 2018. “Branding Internet Sovereignty: Digital Media and the Chinese–Russian Cyberalliance.” *European Journal of Cultural Studies* 21: 594–613. <https://doi.org/10.1177/1367549417751151>.
- Caranto Morford, A., and J. Ansloos. 2021. “Indigenous Sovereignty in Digital Territory: A Qualitative Study on Land-Based Relations With #Nativetwitter.” *AlterNative: An International Journal of Indigenous Peoples* 17, no. 2: 293–305. <https://doi.org/10.1177/11771801211019097>.
- Carver, J. 2024. “More Bark Than Bite? European Digital Sovereignty Discourse and Changes to the European Union's External Relations Policy.” *Journal of European Public Policy* 31, no. 33: 1–37. <https://doi.org/10.1080/13501763.2023.2295523>.
- Chen, C., C. B. Frey, and G. Presidente. 2020. *Privacy Regulation and Firm Performance: Estimating the GDPR Effect Globally*. The Oxford Martin Working Paper Series on Technological and Economic Change, University of Oxford.
- Cong, W., and J. Thumfart. 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, no. 4: ksac059.
- Couture, S., and S. Toupin. 2019. “What Does the Notion of ‘Sovereignty’ Mean When Referring to the Digital?” *New Media & Society* 21, no. 10: 2305–2322. <https://doi.org/10.1177/1461444819865984>.
- Couture, S., S. Toupin, and A. Mayoral Baños. 2024. “Resisting and Claiming Digital Sovereignty: The Cases of Indigenous Nations and Civil Society Groups.” *Policy & Internet* 16, no. 4: 1–20.
- Creemers, R. 2020. *China's Approach to Cyber Sovereignty*. Berlin: Konrad Adenauer Stiftung. <https://www.kas.de/en/single-title/-/content/china-s-approach-to-cyber-sovereignty>.
- Danet, D., and A. Desforges. 2020. “Digital Sovereignty and Strategic Autonomy in Europe: From Concept to Geopolitical Reality.” *Hérodote* 177–178, no. 2: 179–195. <https://shs.cairn.info/journal-herodote-2020-2-page-179?lang=en>.
- Daucé, F., and F. Musiani. 2021. “Infrastructure-Embedded Control, Circumvention and Sovereignty in the Russian Internet: An Introduction.” *First Monday* 26: 1–10. <https://doi.org/10.5210/fm.v26i5.11685>.
- Dixon, R. B. L. 2022. “A Principled Governance for Emerging AI Regimes: Lessons From China, the European Union, and the United States.” *AI and Ethics* 3: 793–810. <https://doi.org/10.1007/s43681-022-00205-0>.
- European Council. 2021. *Digital Sovereignty is Central to European Strategic Autonomy—Speech by President Charles Michel at «Masters of Digital 2021» Online Event—Consilium*. European Council. <https://www.consilium.europa.eu/en/press/press-releases/2021/02/03/speech-by-president-charles-michel-at-the-digitaleurope-masters-of-digital-online-event/>.
- Floridi, L. 2020. “The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU.” *Philosophy & Technology* 33, no. 3: 369–378. <https://doi.org/10.1007/s13347-020-00423-6>.

- Gehl Sampath, P. and F. Tregenna, eds. 2022. *Digital Sovereignty: African Perspectives* (Version 1). DSI/NRF South African Research Chair in Industrial Development. <https://zenodo.org/record/5851685>.
- Glasze, G., A. Cattaruzza, F. Douzet, et al. 2023. "Contested Spatialities of Digital Sovereignty." *Geopolitics* 28, no. 2: 919–958. <https://doi.org/10.1080/14650045.2022.2050070>.
- Gong, W. 2005. "Information Sovereignty Reviewed." *Intercultural Communication Studies* 14, no. 1: 119–135.
- Hong, Y., and T. G. Goodnight. 2019. "How to Think About Cyber Sovereignty: The Case of China." *Chines Journal of Communication* 13, no. 4: 1–19. <https://dx.doi.org/10.2139/ssrn.3467933>.
- Ifeanyi-Ajufo, N. 2023. "Cyber Governance in Africa: At the Crossroads of Politics, Sovereignty and Cooperation." *Policy Design and Practice* 6, no. 2: 146–159. <https://doi.org/10.1080/25741292.2023.2199960>.
- Jiang, M. 2025. "Models of State Digital Sovereignty From the Global South: Diverging Experiences From China, India and South Africa." *Policy & Internet*, 16, no. 4: 1–20.
- Kalema, N. 2024. "The 'Digital Transformation for Development' (DX4D) Anti-Politics Machine." *Policy & Internet* 16, no. 4: 1–20.
- Kulikova, A. 2021. "Cyber Norms: Technical Extensions and Technological Challenges." *Journal of Cyber Policy* 6, no. 3: 340–359. <https://doi.org/10.1080/23738871.2021.2020316>.
- Lambach, D., and L. Monsees. 2024. "Beyond Sovereignty as Authority: The Multiplicity of European Approaches to Digital Sovereignty." *Global Political Economy* early view: 1–18. <https://doi.org/10.1332/26352257Y2024D000000007>.
- Lambach, D., and K. Oppermann. 2022. "Narratives of Digital Sovereignty in German Political Discourse." *Governance* 36, no. 3: 693–709. <https://doi.org/10.1111/gove.12690>.
- Litvinenko, A. 2021. "Re-Defining Borders Online: Russia's Strategic Narrative on Internet Sovereignty." *Media and Communication* 9, no. 4: 5–15. <https://doi.org/10.17645/mac.v9i4.4292>.
- Madiega, T. 2020. *Digital Sovereignty for Europe* (EPRS Ideas Paper). European Parliamentary Research Service. [https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI\(2020\)651992_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/BRIE/2020/651992/EPRS_BRI(2020)651992_EN.pdf).
- Monsees, L., and D. Lambach. 2022. "Digital Sovereignty, Geopolitical Imaginaries, and the Reproduction of European Identity." *European Security* 31, no. 3: 377–394. <https://doi.org/10.1080/09662839.2022.2101883>.
- Musiani, F. 2013. "Network Architecture as Internet Governance." *Internet Policy Review* 2, no. 4: 1–9. <https://doi.org/10.14763/2013.4.208>.
- Nanni, R. 2022. "Digital Sovereignty and Internet Standards: Normative Implications of Public-Private Relations Among Chinese Stakeholders in the Internet Engineering Task Force." *Information, Communication & Society* 25, no. 16: 2342–2362. <https://doi.org/10.1080/1369118X.2022.2129270>.
- Nanni, R., P. G. Bizzaro, and M. Napolitano. 2024. "The False Promise of Individual Digital Sovereignty in Europe: Comparing Artificial Intelligence and Data Regulations in China and the European Union." *Policy & Internet* 16, no. 4: 1–16.
- ten Oever, N., C. Perarnaud, J. Kristoff, et al. 2024. "Sanctions and Infrastructural Ideologies: Assessing the Material Shaping of EU Digital Sovereignty in Response to the War in Ukraine." *Policy & Internet* 1, no. 19: 1–19.

- Pizzul, D., and M. Veneziano. 2024. "Digital Sovereignty or Sovereignism? Investigating the Political Discourse on Digital Contact Tracing Apps in France." *Information, Communication & Society* 27, no. 5: 1008–1024. <https://doi.org/10.1080/1369118X.2023.2232840>.
- Pohle, J. 2020. Digital Sovereignty—A New Key Concept of Digital Policy in Germany and Europe. Konrad Adenauer Stiftung. <https://www.kas.de/en/single-title/-/content/digital-sovereignty>.
- Pohle, J., and M. Santaniello. 2024. "From Multistakeholderism to Digital Sovereignty: Toward a New Discursive Order in Internet Governance?" *Policy & Internet* early view: 1–16. <https://doi.org/10.1002/poi3.426>.
- Pohle, J., and T. Thiel. 2020. "Digital Sovereignty." *Internet Policy Review* 9, no. 4. <https://doi.org/10.14763/2020.4.1532>.
- Roberts, H., J. Cowsls, F. Casolari, J. Morley, M. Taddeo, and L. Floridi. 2021. "Safeguarding European Values With Digital Sovereignty: An Analysis of Statements and Policies." *Internet Policy Review* 10, no. 3: 1–19. <https://doi.org/10.14763/2021.3.1575>.
- Shaheed, A., and B. Greenacre. 2021. "Binary Threat: How Governments' Cyber Laws and Practice Undermine Human Rights in the MENA Region." *Project on Middle East Political Science* 43: 8.
- Thumfart, J. 2022. "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 *Enforcing Rights in a Changing World*, edited by D. Hallinan, R. Leenes, and P. Hert, 1–44. Hart Publishing.
- Wallerstein, I. M. 1991. *Unthinking Social Science: The Limits of Nineteenth-Century Paradigms*. Polity Press.
- Walter, M., T. Kukutai, S. R. Carroll, and D. Rodriguez-Lonebear. 2020. *Indigenous Data Sovereignty and Policy*. Routledge. <https://doi.org/10.4324/9780429273957>.
- Young, J. C. 2019. "The New Knowledge Politics of Digital Colonialism." *Environment and Planning A: Economy and Space* 51, no. 7: 1424–1441. <https://doi.org/10.1177/0308518X19858998>.
- Zeng, J., T. Stevens, and Y. Chen. 2017. "China's Solution to Global Cyber Governance: Unpacking the Domestic Discourse of 'Internet Sovereignty'." *Politics & Policy* 45, no. 3: 432–464. <https://doi.org/10.1111/polp.12202>.