Lawo, Dennis, Gunnar Stevens, and Jenny Berkholz, 2025. "Three actors, eight models: A relational lens on digital sovereignty." *communication +1*, vol. 11, issue 2, pp. 1—51.
DOI: https://doi.org/10.7275/cpo.2158

Three actors, eight models: A relational lens on digital sovereignty

Dennis Lawo, University of Siegen, GER, dennis.lawo@verbraucherinformatik.de
Gunnar Stevens, University of Siegen, GER, gunnar.stevens@uni-siegen.de
Jenny Berkholz, University of Siegen, GER, jenny.berkholz@uni-siegen.de

Digital sovereignty has gained popularity in various discourses. Political science usually refers to a nation's control over its digital policies, infrastructure, and data. In Information Systems Research (ISR), the term usually refers to an organization's control over its digital assets and operations. In Human-Computer Interaction (HCI), the concept refers to issues such as privacy, data protection, and personal autonomy on the Internet. This paper examines these multi-layered discourses through a relational lens and presents eight models of digital sovereignty based on the interplay between state, business, and individual actors. By analysing the ways in which digital sovereignty is ascribed and how the power relations between these levels are structured, the article provides a comprehensive understanding of the different approaches and the interactions between the different levels. It also illuminates the diverse discursive formations through which stakeholders articulate, negotiate, and enforce their claims to sovereignty within digital realms.

Introduction

Digital sovereignty emphasizes the importance of agency in the digital space. However, it is not a coherent concept but is used in different discourses to refer to the agency of various actors at different levels.[1] In the realm of international relations and governance, for instance, digital sovereignty refers to a nation's control over its digital policies and infrastructures. From an economic perspective, the term relates to a company's control over digital assets, business models, and operational excellence.[2] At the individual level, the term touches on privacy, data protection, and personal autonomy in the digital space.[3]

The literature usually considers the different levels in isolation, and the power relations among the levels are typically neglected. In this paper, we argue for a relational lens, which gives us a profound understanding of how the digital sovereignty of governmental, economic, and individual actors mutually shapes each other. This relational lens bridges the gap between a theoretical lens,[4] a narrative lens,[5] and the relational actor-network lens[6] used to analyse individual cases. We can identify eight different narratives of digital sovereignty constellations based on a binary model that assumes that actors either possess digital sovereignty or lack thereof. The strength of this approach is that it provides a framework that spans the discourse space within which various concepts of digital sovereignty can be situated. As an analytical model, it supports by making implicit assumptions and thought patterns visible, illustrating where individual authors position digital sovereignty and how power structures, negotiation processes, and relationships between actors are theoretically conceptualized.

---

[1] Daniel Lambach and Kai Oppermann, "Narratives of Digital Sovereignty in German Political Discourse," *Governance* 36, no. 3 (April 2022): 693–709, https://doi.org/10.1111/gove.12690; Daniel Lambach and Linda Monsees, "Beyond Sovereignty as Authority: The Multiplicity of European Approaches to Digital Sovereignty," *Global Political Economy* (February 2024): 1–18, https://doi.org/10.1332/26352257y2024d000000007.

[2] Julia Pohle et al., "Digital Sovereignty," in *Practicing Sovereignty* (transcript, 2021), 47–68, https://doi.org/10.1515/9783839457603-003.

[3] Dennis Lawo et al., "Human-Centred Digital Sovereignty: Explorative Conceptual Model and Ways Forward," in *Computer-Human Interaction Research and Applications* (Springer Nature Switzerland, 2023), 84–103, https://doi.org/10.1007/978-3-031-49368-3_6; Jane Müller et al., "Digital Sovereignty of Adolescents," *Medienjournal—Zeitschrift für Medien- und Kommunikationsforschung* 44, no. 1 (2020): 30–40, https://doi.org/10.60764/MEDIENJOURNAL-XQK1-8C15.

[4] See e.g., Pohle et al., "Digital Sovereignty."

[5] See e.g., Lambach and Oppermann, "Narratives of Digital Sovereignty."

[6] See e.g., Max Tretter, "Sovereignty in the Digital and Contact Tracing Apps," *Digital Society* 2, no. 1 (December 2022): 2, https://doi.org/10.1007/s44206-022-00030-2.

This relational model of digital sovereignty, moreover, allows for a nuanced understanding of digital sovereignty, acknowledging the complexity and interconnectedness of the state, the economy, and the individual. Comparing the different narratives highlights the various discourse structures and guides researchers, policymakers, and activists in navigating the digital sovereignty landscape.

To develop such a relational model, we first provide a short overview on the history of digital sovereignty as well as an introduction into the most prominently discussed actors in the field—governmental, economical, and individual actors. Based on this background of literature, we present the development of our relational model. This entails a description of our approach and line of thinking when developing the model, as well as a detailed description of the eight narratives. Moreover, we discuss the implications of our model afterward.

Digital Sovereignty: A Short History

> *Today, sovereignty always primarily means a state's independence vis-à-vis other states (external sovereignty) as well as its supreme power to command all powers within the territory of the state (internal sovereignty).*[7]

Sovereignty as a general concept has a long history, rooted in intellectual ideas such as social contract theories, mercantilist economic theories, and civic rights theories. In the 16th century, Jean Bodin attributed sovereignty to the ruler's (the sovereign) ability to make decisions and execute them.[8] A pivotal role in the ruler's sovereignty was his power over the state's territory and geographical expanse.[9]

The digital sphere, however, needs to be a more clearly defined territory in the sense of Bodin. In the early days of the Internet, cyber exceptionalism was prominent, which argues that the digital sphere is fundamentally different. As governments are too slow, too inefficient, and too bound by traditional territorial borders, states cannot control the digital sphere.[10] In contrast to this view, China, Russia, and Iran are trying to achieve national digital sovereignty by restricting the open Internet and promoting territorially closed networks.[11] It remains to be

[7] Pohle et al., "Digital Sovereignty."

[8] Ibidem.

[9] Dieter Grimm, *Sovereignty: The Origin and Future of a Political and Legal Concept* (Columbia University Press, 2015), https://doi.org/10.7312/grim16424.

[10] Pohle et al., "Digital Sovereignty."

[11] Ilona Stadnik, "Internet Governance in Russia–Sovereign Basics for Independent Runet," in *TPRC47: The 47th Research Conference on Communication, Information and Internet Policy*, 2019; Margarita Grinko et al., "Nationalizing the Internet to Break a Protest Movement: Internet

determined whether digital sovereignty will be achieved in the future by reclaiming geographical borders or through new types of extraterritorial measures.

During the era of absolutism, it was unmistakably clear that only the king was the sovereign. Yet, in the wake of the Enlightenment, modern thought has been significantly influenced by the doctrine of Popular Sovereignty, which emphasizes that the ultimate source of all authority exercised through the state's public institutions originates from the people.[12] So, in modern view, sovereignty is not limited to the ruler or the state but is attributed to other actors as well.

Nowadays, digital sovereignty is used as a normative[13] and empirical category[14] to study companies and individuals. States, companies, and individuals claim and bargain for sovereignty within different power constellations and political contexts, each with distinct goals, capabilities, and resources, leading to an uncertain outcome. Some scholars also characterize this situation as a "tech war."[15]

Despite its origins in military technology, the Internet, for instance, has evolved into a primarily commercial domain. As power becomes concentrated among a few large tech corporations, these companies are seen as true sovereigns in the digital age.[16] At the same time, liberal democracies are increasingly demanding that digital sovereignty be in the population's hands. Following the idea that all power should emanate from the people, safeguarding and promoting the digital sovereignty of the individuals presents an essential guiding principle of the new digital humanism.[17]

Shutdown and Counter-Appropriation in Iran of Late 2019," *Proceedings of the ACM on Human-Computer Interaction* 6, no. CSCW2 (November 2022): 1–21, https://doi.org/10.1145/3555205.

[12] Daniel Lee, *Popular Sovereignty in Early Modern Constitutional Thought* (Oxford University Press, 2016), https://doi.org/10.1093/acprof:oso/9780198745167.001.0001.

[13] Antoinette Rouvroy and Yves Poullet, "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy," in *Reinventing Data Protection?*, ed. Serge Gutwirth et al. (Springer Netherlands, 2009), 45–76, https://doi.org/10.1007/978-1-4020-9498-9_2.

[14] Riccardo Nanni,"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 (October 2022): 2342–62, https://doi.org/10.1080/1369118x.2022.2129270.

[15] Theodore Christakis, "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy," *SSRN Electronic Journal*, 2020, https://doi.org/10.2139/ssrn.3748098.

[16] Shoshana Zuboff, *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power* (Profile Books, 2019).

[17] Igor Calzada, "Pandemic Citizenship Amidst Stateless Algorithmic Nations: Digital Rights and Technological Sovereignty at Stake" 10 (2021), https://doi.org/10.13140/RG.2.2.36196.19849/3; Erich

This brief overview of digital sovereignty highlights the necessity of conceptualizing the term in the plural, considering the various actors at different levels.[18] While the goal of digital sovereignty applies equally to all actors, its meaning varies at each level.[19]

Digital Sovereignty at Different Levels

Governmental Level

Digital sovereignty at the governmental level refers to the ability and authority of a state to control and regulate critical infrastructures and technologies independently, have authority over digital assets, and protect the data of its citizens and businesses.[20]

Given the historical connotation of sovereignty in the last century as governmental sovereignty, it is unsurprising that the nation is the most prominent actor in claiming digital sovereignty. Regarding governmental sovereignty, Pohle et al. identified two different lines of thinking.[21] The first line of thinking is represented by authoritarian, non-liberal governments, which perceive free speech and self-organization using digital channels as a threat to the political systems.[22] Those states are ambitious in gaining control over social media and the Internet on their territory while benefiting from other parts of global connectivity. Countries such as China[23] and Russia[24] are typically named in this context.

The other side is represented by liberal democracies, where the notion of digital sovereignty mainly refers to national authority and security concerns. For example, the global connectivity of cyberspace creates new vulnerabilities and threats to infrastructures that must be secured by state action.[25] Security issues pose challenges for authoritarian states, too. However, government security actions can clash with the values of freedom important to civil societies. For this reason, the

---

Prem, "Principles of Digital Humanism: A Critical Post-Humanist View," *Journal of Responsible Technology* 17 (March 2024), https://doi.org/10.1016/j.jrt.2024.100075.

[18] Tretter, "Sovereignty in the Digital"; Pohle et al., "Digital Sovereignty"; Lawo et al., "Human-Centred Digital Sovereignty: Explorative Conceptual Model and Ways Forward."

[19] Lambach and Oppermann, "Narratives of Digital Sovereignty."

[20] Pohle et al., "Digital Sovereignty."

[21] Ibidem.

[22] Ibidem.

[23] Rogier Creemers, "The Chinese Cyber-Sovereignty Agenda," in *Connectivity Wars: Why Migration, Finance and Trade Are the Geo-Economic Battlegrounds of the Future* (JSTOR, 2019).

[24] Stadnik, "Internet Governance in Russia."

[25] Pohle et al., "Digital Sovereignty."

debate about cyber-security is framed differently in liberal democracies, where both security and liberty need to be supported equally.[26]

While the term state is used in a singular sense, it is essential to acknowledge state in its plural form. This plurality is relevant both horizontally, in the pursuit of sovereignty among states, and vertically, between supranational entities like the EU, and the federal states, considered as partial sovereigns.[27] Here, competencies and decision-making powers are shared, e.g., the federal states have their own digital agenda, while the EU plays a significant role too, through its digital acts and its ambitions to promote a single data market.[28]

To increase autarky and national security, governmental actors focus on keeping data and technological capabilities within the local territory of nations or supranational states, such as the EU, with limited access to foreign nations or companies.[29] With measures to protect data, states also aim to enforce a fundamental right of their citizens. This example shows that governmental power can strengthen the sovereignty of individuals as users, consumers, and citizens.[30] Conversely, the inability of a government to exercise sovereignty over its data and technological domains can lead to several risks and vulnerabilities for its citizens and the national economy.[31]

While regulation for data protection presents a legitimate objective regarding civic rights, these efforts can also have economic policy undertones, primarily if they are used to promote protectionist goals.[32] This shows the interrelation of the different

---

[26] Norma Möllers, "Making Digital Territory: Cybersecurity, Techno-Nationalism, and the Moral Boundaries of the State," *Science, Technology, & Human Values* 46, no. 1 (January 2020): 112–38, https://doi.org/10.1177/0162243920904436.

[27] Lambach and Oppermann, "Narratives of Digital Sovereignty"; Yaniv Benhamou, Frédéric Bernard, and Cédric Durand, "Digital Sovereignty in Switzerland: The Laboratory of Federalism," *Risiko & Recht*, no. 1 (October 2023): 65–101, https://doi.org/10.36862/eiz-rr202301-03.

[28] Sebastian Heidebrecht, "From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance," *JCMS: Journal of Common Market Studies* 62, no. 1 (April 2023): 205–23, https://doi.org/10.1111/jcms.13488.

[29] Pohle et al., "Digital Sovereignty."

[30] Ibidem; Luciano Floridi, "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU," *SSRN Electronic Journal* 33, no. 3 (2021): 369–78, https://doi.org/10.2139/ssrn.3827089; Lambach and Oppermann, "Narratives of Digital Sovereignty."

[31] Renata Avila Pinto, "Digital Sovereignty or Digital Colonialism," *Sur: International Journal on Human Rights* 27 (2018): 15.

[32] Anupam Chander and Uyen P Le, "Data Nationalism," *Emory LJ* 64 (2014): 677; Jonah Hill, "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for Us Policymakers and Business Leaders," in *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, 2014; Francesca Musiani, "Infrastructuring Digital Sovereignty: A Research Agenda for

levels, even though the connection can be very differently structured. Governmental sovereignty can manifest itself in solid economic intervention, as in the case of state capitalism.[33] However, it can also manifest itself in a laissez-faire approach, generally intended to stimulate economic growth, but can also lead to phenomena like surveillance capitalism.[34]

Economic Level

Digital sovereignty at the economic level refers to issues such as data authority, digital capabilities, operational excellence, and innovative strength of companies.[35] In addition, enterprises need cyber-security competencies to ensure the availability of business processes, the protection of data integrity, and the keeping of sensible business data secret.[36] Companies' digital sovereignty enables them to make strategic decisions free from external influences and protects them from dependencies that could arise through external technologies or platforms.

In Information System Research (ISR) various facets of enterprise sovereignty are delineated to encompass distinct, yet interrelated dimensions.[37] In ISR, the term "data sovereignty" refers to data control, while "technological sovereignty" emphasizes control over resources and IT infrastructures. In ISR, "digital sovereignty" narrowly focuses on actions, expertise, and control mechanisms in the digital world to gain strategic autonomy.[38]

The economic sphere does not exist in isolation from governmental influence, particularly concerning the digital economic policies of states and supranational

---

an Infrastructure-Based Sociology of Digital Self-Determination Practices," *Information, Communication & Society* 25, no. 6 (March 2022): 785–800, https://doi.org/10.1080/1369118x.2022.2049850.

[33] Ian Bremmer, *The End of the Free Market: Who Wins the War Between States and Corporations? Who Wins the War Between States and Corporations?* (East Rutherford: Penguin Publishing Group, 2010), https://doi.org/10.1007/s12290-010-0129-z.

[34] Zuboff, *The Age of Surveillance Capitalism*.

[35] Malte Hellmeier and Franziska von Scherenberg, "A Delimitation of Data Sovereignty from Digital and Technological Sovereignty," in *ECIS 2023 Research Papers*, 2023, https://aisel.aisnet.org/ecis2023_rp/306/.

[36] Yudhistira Nugraha, Kautsarina, and Ashwin Sasongko Sastrosubroto, "Towards Data Sovereignty in Cyberspace," *2015 3rd International Conference on Information and Communication Technology (ICoICT)*, 2015, 465–71, https://doi.org/10.2139/ssrn.2610314.

[37] Hellmeier and von Scherenberg, "A Delimitation of Data Sovereignty."

[38] Ibidem.

entities.[39] It should be noted, however, that the economic policies and narratives differ, e.g., when we compare China, the EU, and the U.S. as dominant digital empires.[40] The ambition of states to strengthen the local economy[41], regulate digital trade flows,[42] or push digital technologies and infrastructures[43] has an impact on the digital capabilities of enterprises. An example is the European Gaia-X project,[44] which enforces consumer and data protection standards.[45]

Sometimes, the economy will be equated with a de facto singular entity due to state capitalistic mechanisms[46] or oligopoly formation.[47] This perspective, however, risks oversimplifying the economy as a homogeneous field. An alternative lens is to understand the economy as a complex and dynamic network of heterogeneous actors—ranging from large corporations to small enterprises and even individual entrepreneurs—each with distinct interests, resources, and agencies. Within and as part of this network, individual actors strive to establish their digital sovereignty, both in competition and in cooperation with each other.

Individual Level

Digital sovereignty at the individual level focuses on personal self-determination in the digital sphere and the autonomy of individuals in its various roles, such as users,

---

[39] Ansgar Baums, "Digitale Standortpolitik in der Post-Snowden-Welt," in *Digitale Souveränität* (Springer Fachmedien Wiesbaden, 2016), 223–35, https://doi.org/10.1007/978-3-658-07349-7_20.

[40] Stefan Steiger, Wolf J. Schünemann and Katharina Dimmroth, "Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany," *Media and Communication* 5, no. 1 (March 2017): 7–16, https://doi.org/10.17645/mac.v5i1.814.

[41] Francesca Bria, "Public Policies for Digital Sovereignty;" *Ours to Hack and to Own: The Rise of Platform Cooperativism, A New Vision for the Future of Work and a Fairer Internet*, ed. Trebor Scholz and Nathan Schneider, New York/London: OR Books, no. 1a (2017): 218–22.

[42] Pohle et al., "Digital Sovereignty."

[43] Simona Autolitano and Agnieszka Pawlowska, "Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study," *IAI Papers* 21, no. 14 (2021): 1–22; Arnaud Braud et al., "The Road to European Digital Sovereignty with Gaia-X and IDSA," *IEEE Network* 35, no. 2 (March 2021): 4–5, https://doi.org/10.1109/mnet.2021.9387709.

[44] Autolitano and Pawlowska, "Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study"; Braud et al., "The Road to European Digital Sovereignty."

[45] Hill, "The Growth of Data Localization Post-Snowden"; Tim Maurer et al., "Technological Sovereignty: Missing the Point?," in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace* (IEEE, 2015), 53–68, https://doi.org/10.1109/cycon.2015.7158468.

[46] Bremmer, *The End of the Free Market?*.

[47] Zuboff, *The Age of Surveillance Capitalism*.

consumers, employees, citizens, etc.[48] The aim is to empower people to develop freely in a digital world that encompasses both the positive and negative meanings of freedom: In the sense of positive freedom ('*freedom to*'), this refers to the capability of individuals to engage with the digital society.[49] This encompasses the capacity to access information, utilize digital resources for personal purposes, and participate in online discourses without undue restrictions. Nowadays, data literacy and the ability to maintain control over autonomous systems have become essential parts of personal digital sovereignty because of the advent of datafication and the advancements in AI.[50]

Regarding negative freedom ('*freedom from*'), digital sovereignty refers to protecting personal integrity from potential harms and risks associated with online activities.[51] Various parties can compromise the integrity of individuals, such as governmental surveillance practices,[52] criminal and hacking activities,[53] or companies' manipulative practices.[54]

The individual level is mainly addressed by HCI research,[55] where the main research topics are the accessibility of online services,[56] the design of self-protection tools,[57] and the training of users to protect themselves against cyber-attacks, malicious

[48] Dennis Lawo et al., "Digital Sovereignty: What It Is and Why It Matters for HCI," in *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, CHI '23 (ACM, 2023), 1–7, https://doi.org/10.1145/3544549.3585834; Lawo et al., "Human-Centred Digital Sovereignty."

[49] Anne Weibert et al., "Geteilt Vernetzt: Ausprägungen des Digital Divide unter Älteren Migrantinnen in Deutschland," *Medien & Altern* 11 (2017): 75–91.

[50] Ronda Ringfort-Felner et al., "Kiro: A Design Fiction to Explore Social Conversation with Voice Assistants," *Proceedings of the ACM on Human-Computer Interaction* 6, no. GROUP (January 2022): 1–21, https://doi.org/10.1145/3492852.

[51] Gunnar Stevens et al., "Wie Gehen Verbraucher:Innen Mit Onlinebetrug Um? – Eine Literaturübersicht," in *Handbuch Cyberkriminologie* 2, ed. Thomas-Gabriel Rüdiger and P. Saskia Bayerl (Springer Fachmedien Wiesbaden, 2023), 533–54, https://doi.org/10.1007/978-3-658-35442-8_42.

[52] A. Champagne, "Netznutzer: Software Für Diktatoren," *Le Monde Diplomatique*, 2012.

[53] Stevens et al., "Wie gehen Verbraucher:Innen mit Onlinebetrug um?"

[54] Zuboff, *The Age of Surveillance Capitalism*.

[55] Lawo et al., "Digital Sovereignty."

[56] Susanne Iwarsson and Agneta Ståhl, "Accessibility, Usability and Universal Design—Positioning and Definition of Concepts Describing Person-Environment Relationships," *Disability and Rehabilitation* 25, no. 2 (January 2003): 57–66, https://doi.org/10.1080/dre.25.2.57.66.

[57] Alma Whitten and J. Doug Tygar, "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0," in *USENIX Security Symposium*, vol. 348, 1999, 169–84.

technologies,[58] and manipulation attempts.[59] A positivistic stance is common in HCI research, where the average user presents the norm. The diversity of everyday practices, lifestyles, and cultures is often neglected in positivistic research and only becomes visible as a deviation from the norm.[60] The discourse about marginalized groups[61] and the digital divide[62] makes the risk of talking about users in singular evident. Instead, we should speak from users in the plural form. Moreover, this plurality also refers to the manifold of civic actors, including hacktivists, influencers, boycott movements, civic organizations, etc. They contribute as a collective to the digital sovereignty of civil society, too.[63]

From an Actor-Centric to a Relational Digital Sovereignty Model

The brief overview in the previous section shows that the discourses at the different levels have their own focus, yet they are not independent of each other. On the contrary, sovereignty is constituted in relational ways through cooperation and competition among the actors. In HCI, for instance, the discourse on appropriate measures and strategies to protect and promote personal digital sovereignty relies on assumptions about governmental and economic actors.[64] Yet, these assumptions are typically not made explicit. This poses the risk of unverified assumptions being included in the analysis. To prevent this, we should focus on more than just a single actor but explicitly consider the relationship between the levels.

---

[58] Lena Recki et al., "'You Can Either Blame Technology or Blame a Person... ' - A Conceptual Model of Users' AI-Risk Perception as a Tool for HCI," *Proceedings of the ACM on Human-Computer Interaction* 8, no. CSCW2 (7 November 2024): 1–25, https://doi.org/10.1145/3686996; Lena Recki et al., "A Qualitative Exploration of User-Perceived Risks of AI to Inform Design and Policy," in *Fröhlich, Cobus (Hg.): Mensch Und Computer 2023–Workshopband, 03.-06. September 2023, Rapperswil (SG)* (GI, 2023), https://doi.org/10.18420/MUC2023-MCI-WS16-383.

[59] Michelle Walther et al., "A Systematic Literature Review about the Consumers' Side of Fake Review Detection – Which Cues Do Consumers Use to Determine the Veracity of Online User Reviews?," *Computers in Human Behavior Reports* 10 (May 2023), https://doi.org/10.1016/j.chbr.2023.100278.

[60] Dennis Lawo et al., "Buying the 'Right' Thing: Designing Food Recommender Systems with Critical Consumers," in *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 2021, 1–13.

[61] Reem Talhouk et al., "HCI and Refugees: Experiences and Reflections," *Interactions* 25, no. 4 (June 2018): 46–51, https://doi.org/10.1145/3215846.

[62] Weibert et al., "Geteilt Vernetzt."

[63] Sebastian Kubitschko, "The Role of Hackers in Countering Surveillance and Promoting Democracy," *Media and Communication* 3, no. 2 (September 2015): 77–87, https://doi.org/10.17645/mac.v3i2.281.

[64] Lawo et al., "Digital Sovereignty."

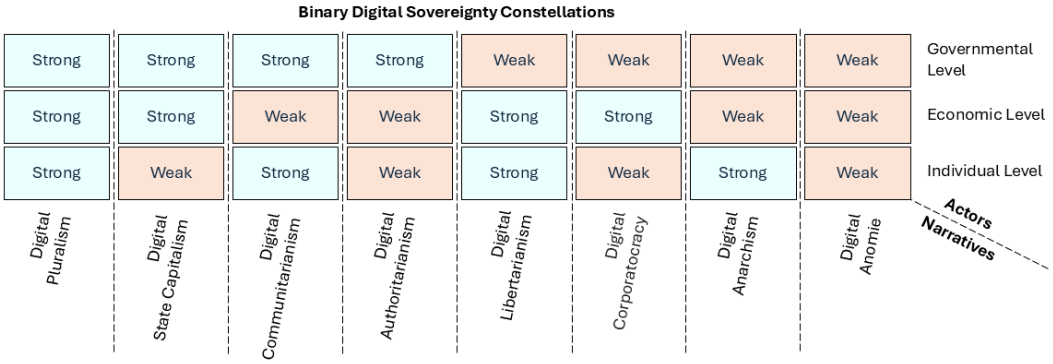

Figure 1: Overview of the Digital Sovereignty Narratives of our Model

From this relational stance, we explore various narratives of digital sovereignty to offer insights into how the relationship between the state, the economy, and the individual could be conceptualized. From this standpoint, the three levels—governmental, economic, and individual—formally constitute eight binary narratives, each representing different digital sovereignty constellations.

Method

We began developing a relational model by considering the manifold actors, organizations, and power relations. However, we quickly realized that accounting for nuanced power relationships, e.g., analysed by Tretter,[65] would result in a combinatorial explosion, making the complexity of the combinations unmanageable. A similar issue arose when attempting further differentiation of actors, such as distinguishing between various governmental agencies, corporate structures, civil society organizations, and consumer collectives. To balance thoroughness with simplicity, we use Occam's razor to create a parsimonious model, which aims to simplify discourses without losing critical details by focusing on overarching themes. The resulting model should be simple and of analytical value to orientation and provide insides about linking the various discourses.

The outcome was a binary model, where each actor (level) is either strong or weak (1 or 0) and thus a total of eight combinations as narrative categories, e.g., digital anomie. Based on this first assumption we conducted a workshop among the authors to map common economical/political ideas to our binary narrative categories.

[65] Tretter, "Sovereignty in the Digital."

At this point, we had a coarse structure for our model, but important aspects were still open, e.g., anomie as an idea was missing or we faced uncertainties regarding anarchism and libertarianism. To resolve these issues and enrich the categories we conducted a narrative literature review[66] focusing on research analysing the economical/political ideas in general as well as in combination with *digital*, *online*, or *cyber*, e.g., *digital communitarism.* We carefully reviewed the literature to analyse the portrayal of power among different actors and the explicit or implicit assumptions about their relationships. This targeted search provided further insights into the various discourse formations and argumentation patterns, as well as the naming of the categories. For instance, in this step, we became aware that the category of digital anomie is connected to post-colonial discourses in which old forms of colonial power relations are replaced by new forms of digital power relations through imperialist tech corporations that suppress the domestic digital economy.

Following from this, we iteratively shaped our binary categories, based on several workshops that helped to resolve different inner- and intra-categorial conflicts. We finalized the report after all authors were satisfied with the content of the model.

A Relational Model of Digital Sovereignty

Our binary model of digital sovereignty narratives aims to entangle the complex web of actors and power dynamics to shed light on essential ideas and systemic interdependencies. Although some authors argue for the primacy of the governmental level,[67] we reflect on the relation without any vertical dependency or hierarchy. In terms of power distribution among levels, we can distinguish between absolutist and shared narratives.

Absolutist narratives focus on concentrated power within a single level (one 'strong' actor), assuming a zero-sum game where one's gain is another's loss. For example, digital authoritarianism ('strong' government). Shared narratives advocate for distributed digital sovereignty across multiple levels, forming vertical alliances to strengthen power (more than one 'strong' actor). This includes, e.g., digital state capitalism ('strong' government as well as 'strong' economic sovereignty). Digital pluralism, which spans three levels, suggests that complexity and diversity bolster societal resilience, but require checks and balances. Digital anomie represents the

[66] Guy Paré et al., "Synthesizing Information Systems Knowledge: A Typology of Literature Reviews," *Information & Management* 52, no. 2 (March 2015): 183–99, https://doi.org/10.1016/j.im.2014.08.008.

[67] Jukka Ruohonen, "The Treachery of Images in the Digital Sovereignty Debate," *Minds and Machines* 31, no. 3 (July 2021): 439–56, https://doi.org/10.1007/s11023-021-09566-7.

opposite, where no entity or level holds digital sovereignty, leading to powerlessness, unpredictability, fragmentation, and inequalities.[68] In the following, we describe the different narratives of our model in detail.

Digital Authoritarianism

"Sovereignty is the absolute and perpetual power of a state."—Jean Bodin

Digital authoritarianism is a term that has gained prominence in the discourse on the digital politics of authoritarian regimes.[69] A characteristic of digital authoritarianism is the attempt to re-territorialize the Internet, also called splinternet,[70] which presents an expression of Westphalian sovereignty in the digital age.[71]

Even if corporations are important agents in the implementation and stabilization of digital authoritarian regimes, the regimes are the central actors in digital authoritarianism.[72] Generally, free digital markets are perceived as a threat to the regime's grip on power, leading to strict regulation and close intertwining of companies with governmental structures. To achieve comprehensive surveillance, for instance, companies must comply with authoritarian regimes by granting access to user data or enforcing state censorship.[73] Furthermore, the digital sovereignty of the economic sector is always at risk in authoritarian regimes. For example, when the power of big-tech companies appears to be a threat, regimes can extend their control over them through significant interventions aimed at bringing them into line with state policy.[74]

---

[68] Avila Pinto, "Digital Sovereignty or Digital Colonialism."

[69] Dara Conduit, "Digital Authoritarianism and the Devolution of Authoritarian Rule: Examining Syria's Patriotic Hackers," *Democratization* 31, no. 5 (March 2023): 979–97, https://doi.org/10.1080/13510347.2023.2187781; Tiberiu Dragu and Yonatan Lupu, "Digital Authoritarianism and the Future of Human Rights," *International Organization* 75, no. 4 (2021): 991–1017, https://doi.org/10.1017/s0020818320000624.

[70] Scott Malcomson, *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web* (OR books, 2016).

[71] Stadnik, "Internet Governance in Russia."

[72] Alina Polyakova and Chris Meserole, "Exporting Digital Authoritarianism: The Russian and Chinese Models," *Policy Brief, Democracy and Disorder Series*, 2019, 1–22, https://doi.org/20.500.12592/rwbp8q.

[73] Marcus Michaelsen, "Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran," *Surveillance & Society* 15, no. 3/4 (August 2017): 465–70, https://doi.org/10.24908/ss.v15i3/4.6635.

[74] Megha Shrivastava, "Emerging Dynamics Between the Chinese State and Big-Tech: The Case of Alibaba," *Strategic Analysis* 47, no. 1 (January 2023): 19–29, https://doi.org/10.1080/09700161.2023.2181424.

Civil rights and a strong digital sovereignty of individuals present another thread to authoritarian regimes. For this reason, regimes aim to marginalize the sovereignty of people by retaining control of digital technologies through surveillance, repression, censoring, and manipulating domestic populations within their borders and even beyond.[75] Online activities will be monitored, communications will be censored, and personal data will be collected without consent.[76] This poses a serious threat to individual freedom and privacy and emphasizes the need to develop and strengthen mechanisms to protect citizens' digital rights.

While digital authoritarianism does not manifest as a pure observable narrative within the real world, we can see certain characteristics in actual practice. An example presents the Iranian digital agenda about surveillance technology.[77] The state manages to have access to the global market of surveillance technologies to exercise control over the communication (infrastructure) within the country.[78] This measure can be considered an important pillar of the authoritarian regime, suppressing civic freedoms, e.g., free speech, freedom of expression, or free access to information.[79] This restrictive policy prioritizes state control over economic concerns, even if it may be at the sacrifice of economic efficiency. Another example is the Pakistani control over their network infrastructure, allowing them to shut down the network completely, block websites, and conduct surveillance operations. At the same time, the governance exercises a regime of restrictive governance over the digital economy, e.g., enforcing governmental control over data or banning non-cooperative corporations.[80]

Digital Corporatocracy

> *"The liberty of a democracy is not safe if the people tolerate the growth of private power to a point where it becomes stronger than the democratic state itself."*—Franklin D. Roosevelt

Digital corporatocracy is another absolutist narrative, yet this narrative does not locate digital sovereignty with the state or the individual but with the overwhelming

[75] Polyakova and Meserole, "Exporting Digital Authoritarianism."

[76] Grinko et al., "Nationalizing the Internet to Break a Protest Movement."

[77] Marcus Michaelsen, "Exit and Voice in a Digital Age: Iran's Exiled Activists and the Authoritarian State," *Globalizations* 15, no. 2 (2018): 248–64; Michaelsen, "Far Away, So Close."

[78] Michaelsen, "Far Away, So Close."

[79] Michaelsen, "Exit and Voice in a Digital Age."

[80] Yilmaz Ihsan and Raja Ali M. Saleem, *The Nexus of Religious Populism and Digital Authoritarianism in Pakistan*, *Populism & Politics* (European Center for Populism Studies (ECPS), 2022), https://doi.org/10.55271/pp0016.

corporate power over government and people at every level and in every possible form.[81] The concept has been utilized in the criticism of globalization and neoliberal ideologies,[82] where corporatocracy presents a pathological form of democracy, wherein corporations aim to control and exploit democratic institutions for their business interests.[83]

The erosion of state power was accelerated by various factors such as the neoliberal ideology criticizing inefficient and sluggish governments, but advocating for the privatization of sovereign duties;[84] the globalization and multinational markets enabling corporations to bypass national regulations;[85] the concentration of power through cartels and oligopolies, where beyond a certain tipping point "too big to fail" means too powerful to govern;[86] and the commodification of public discourses, where mass media controlled by large corporations enables the spread of corporatist propaganda on an unprecedented scale.[87]

This brief outline shows that corporatocracy is not an entirely new concept, yet it has taken on an unprecedented form and power in the digital age. The inherent global and decentralized governance structure of the Internet, combined with the rapid pace of technological innovation, challenges the regulation of cyberspace by national authorities.[88] In addition, the commercialization of the Internet in the late 1980s coincided with the rise of the neoliberal, free-market ideology, which further delayed state regulation.[89] The digital economy, with its lock-in effects, external network effects, and zero marginal costs, has further facilitated the emergence of oligopolies and market concentration.[90] Due to their market capitalization, big tech companies can also use extensive lobbying and PR campaigns to influence regulations to their advantage.[91] Moreover, the popularity of social media gives platform providers

[81] Luis Suarez-Villa, *Globalization and Technocapitalism: The Political Economy of Corporate Power and Technological Domination* (Routledge, 2016), https://doi.org/10.4324/9781315585123.
[82] Patricia Ventura, *Neoliberal Culture: Living with American Neoliberalism* (Routledge, 2016).
[83] Suarez-Villa, *Globalization and Technocapitalism*.
[84] David Michael Kotz, *The Rise and Fall of Neoliberal Capitalism* (Harvard University Press, 2015), https://doi.org/10.4159/harvard.9780674735880.
[85] Zuboff, *The Age of Surveillance Capitalism*.
[86] Kotz, *The Rise and Fall of Neoliberal Capitalism*.
[87] Suarez-Villa, *Globalization and Technocapitalism*.
[88] Pohle et al., "Digital Sovereignty."
[89] Bradford, *Digital Empires*.
[90] Reiner Clement and Dirk Schreiber, *Internet-Ökonomie* (Springer Berlin Heidelberg, 2016), https://doi.org/10.1007/978-3-662-49047-1.
[91] Zuboff, *The Age of Surveillance Capitalism*.

the power to steer public discourse through the design of algorithms and their content curation policies.[92]

The power of digital oligopolies furthermore leads to a lack of digital sovereignty for individuals. Due to digital technology and the commodification of digital behaviour, corporations gain the power to monitor and manipulate people on an industrial scale—a practice that Zuboff has called surveillance capitalism.[93] Corporations, armed with sophisticated data analytics and vast resources, engage in data collection and processing on a scale unattainable by individual users.

The capacity of corporations to predict and influence user actions undermines individual agency.[94] This manipulation, achieved through targeted advertising, curated news feeds, and algorithmic sorting represents a deep intrusion into personal decision-making processes. This power disparity leads to a digital panopticon,[95] where user data will be exploited without adequate transparency or consent, directly contradicting the libertarian idea of individual autonomy.

In her work, Zuboff's description of the exploitation of digital consumers is based on a wealth of empirical evidence. Yet, her main argument about the lack of personal sovereignty is a theoretical one. The lack is not merely a consequence of asymmetric power relations at the empirical level, but it stems from her behaviourist perspective on human nature.[96] Because of this nature, human behaviour is not a product of free will but a predictable reaction to external stimuli. Surveillance capitalism merely exploits the mechanism, which is inherent in human nature, and transforms it into a commodity.

The American market-driven regulatory idea is sometimes characterized as corporatocracy.[97] Yet, it is more precise to link corporatocracy with a particular nation, but with multi-national tech-oligopolies such as the GAFAM,[98] which dominate not just the US but also Europe and developing countries. This oligopoly operates with relatively little regulation exploiting peoples' digital behaviour to maximize their profits. In the past, governments exhibited limited interest in and

---

[92] Emilee Rader and Rebecca Gray, "Understanding User Beliefs About Algorithmic Curation in the Facebook News Feed," in *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, CHI '15 (ACM, 2015), 173–82, https://doi.org/10.1145/2702123.2702174.

[93] Zuboff, *The Age of Surveillance Capitalism*.

[94] A fundamental concern that cyber-libertarianism seems ill-equipped to confront (see below).

[95] Ihsan and Saleem, *The Nexus of Religious Populism*.

[96] Zuboff, *The Age of Surveillance Capitalism*.

[97] Bradford, *Digital Empires*.

[98] GAFAM is the acronym for Google (Alphabet), Apple, Facebook (Meta), Amazon, and Microsoft.

capacity to regulate the developing digital economy.[99] However, the relationship between governments and Big Tech is not static—especially regarding the EU's current ambition to reclaim digital sovereignty at the regulatory level or China's strategy to build infrastructures of and under state control.[100]

Digital Anarchism

> *"The history of human evolution is the record of technological innovation. Expensive machinery requiring large group efforts for operation becomes a tool of social repression by the state. The tower clock. The galley shop. The cannon. The tank. Instruments that can be owned and operated by individuals inevitably produce democratic revolutions."*—Timothy Leary [101]

Digital anarchism represents the antithesis of digital authoritarianism, which fears government and corporate surveillance.[102] This narrative understands the cyberspace as an extra-territorial, authority-free space without legal restrictions, state regulation, and commercial interests. This view is echoed in the legal debate on the cyberspace as being separated from the real world, such that legal authorities do not and should not have control over cyberspace.[103] Moreover, it directly relates to digital libertarianism, but instead of favouring free markets and property rights, anarchists' thinking is based on collective ownership, solidarity, and collaborative action.[104]

Digital anarchism distrusts state power due to the risks of regulation and censorship. Instead, it advocates for free thinking and the concept of self-regulation and self-governance within the community. Moreover, questioning established norms, dogmas, and power structures is seen not just as a right but a responsibility. Controversial or unpopular avenues of thought present the engine for societal progress, so they should not be suppressed by public authorities.[105] The scepticism is

---

[99] Bradford, *Digital Empires*.

[100] See also section 'Digital Pluralism.'

[101] Timothy Leary, *Chaos & Cyber Culture* (Grupo Editorial Norma, 1994).

[102] Roderick Graham and Brian Pitman, "Freedom in the Wilderness: A Study of a Darknet Space," *Convergence: The International Journal of Research into New Media Technologies* 26, no. 3 (October 2018): 593–619, https://doi.org/10.1177/1354856518806636.

[103] Lawrence Lessig, "The Zones of Cyberspace," *Stanford Law Review* 48, no. 5 (May 1996): 1403, https://doi.org/10.2307/1229391.

[104] Damian Finbar White and Gideon Kossoff, "Anarchism, Libertarianism and Environmentalism: Anti-Authoritarian Thought and the Search for Self-Organizing Societies," in *The SAGE Handbook of Environment and Society* (SAGE Publications Ltd, 2007), 50–65, https://doi.org/10.4135/9781848607873.n3.

[105] White and Kossoff, "Anarchism, Libertarianism and Environmentalism.".

also expressed by a libertarian, techno-centric aversion to bureaucracies, viewing them as flawed systems that are slow and dysfunctional and merely represent a misuse of power.[106]

Digital anarchism rejects the capitalist system, as its emphasis on profit maximization and private ownership does not contribute to human well-being but is a threat to people's privacy and freedom.[107] Commercialization also impedes the free exchange of information as companies will try to manipulate, instrumentalize, and exploit them to maximize profits. Moreover, they will try to restrict access to information due to copyright rights, proprietary software, and inaccessible data silos, to gain an unfair advantage over competitors. Instead, digital anarchism is based on two fundamental technical principles: *decentralization organization* and *zero-cost data copies to facilitate collective ownership and sharing*.

The first principle is based on the decentral architecture of the Internet and Distributed Ledger Systems (DLS). Decisions, service offerings, and information are distributed among individuals within the network. This promotes autonomy and prevents monopolies of power. Everyone is able to actively participate in the network and contribute to collective decision-making. The second principle refers to the inherent capability of digital technology to produce exact copies of data at virtually no cost and distribute them over the Internet in milliseconds. This principle is expressed in the common phrase that information wants to be free.[108] Moreover, this phrase refers to information as an actant with an anarchistic agency, where any attempt to regulate its freedom by national laws or exploit it by capitalistic means would be absurd for technical reasons.

These examples demonstrate that digital anarchism is primarily a techno-centric utopia, anchored in the belief in technological progress to enhance the life of the individual.[109] This technological base is supplemented by an ideological superstructure that champions the unrestricted freedom of the collective and the individual. The manifest of this ideology was Steven Levy's book about Hacker Ethics,

---

[106] David J. Betz, *Cyberspace and the State: Towards a Strategy for Cyber-Power* (Routledge, 2017).

[107] White and Kossoff, "Anarchism, Libertarianism and Environmentalism."

[108] Aaron Swartz and Lawrence Lessig, *A Web of Extended Metaphors in the Guerilla Open Access Manifesto of Aaron Swartz* (University of California, Santa Barbara, 2017), December 12, 2024, https://search.proquest.com/openview/ae4a63af9ed1cfbf50895b45dec91fbf/1?pq-origsite=gscholar&cbl=18750.

[109] Majid Yar, "Computer Hacking: Just Another Case of Juvenile Delinquency?," *The Howard Journal of Criminal Justice* 44, no. 4 (September 2005): 387–99, https://doi.org/10.1111/j.1468-2311.2005.00383.x.

from 1984 with its mantra to distrust authorities but promote decentralization[110] or Timothy Leary's post-humanist thoughts from 1994 on self-determination in the digital age.[111]

The idea of the Internet as a free, authority-free space was also resonated enthusiastically by the technical, academic elite.[112] This enthusiasm was caused by the fact that the idea was compatible with the academic canon of values, which includes the free exchange and discussion of ideas, the principle of judging issues by argument rather than by authority, and the spirit of inquiry that welcomes open-ended experimentation, modification, and technological innovations.

According to Selzer[113] the vibrant anarchic spirit of the early day, however, has largely diminished in the mainstream digital world. It has shifted to the darknet as a countercultural space that deliberately seeks to operate beyond the reach of state regulation and surveillance. In addition, the spirit continues to influence a diverse array of NGOs, activists, and collaborative, non-commercial, and privacy-preserving technology projects, such as Wikileaks, the Chaos Computer Club, the Linux project, the Tor project, and the Bitcoin movement. Still, all of them face the paradox of success: as they grow and gain wider acceptance, there is a constant risk of commercialization that could dilute their original anarchistic ethos.

Digital State Capitalism

> *„Now that the free market has failed, what do you think is the proper role for the state in the economy?"*—He Yafei (China's Vice Foreign Minister)[114]

The twenty-first-century state capitalism presents "*a system in which the state plays the role of leading economic actor and uses markets primarily for political gain.*"[115] State economic interventions do not just realize economic goals, but preserve and even extend political control.[116]

---

[110] Steven Levy, *Hackers: Heroes of the Computer Revolution*, vol. 14 (Anchor Press/Doubleday Garden City, NY, 1984), December 12, 2024, https://www.usenix.org/legacy/publications/login/2010-10/openpdfs/bookreviews1010.pdf.

[111] Leary, *Chaos & Cyber Culture*.

[112] Jochim Selzer, "Die Rückkehr des Dezentralen: Wie sich Internetaktive gegen Regulierung wehren," *Informatik Spektrum* 43, no. 3 (May 2020): 192–96, https://doi.org/10.1007/s00287-020-01273-4.

[113] Ibidem.

[114] Quoted by Bremmer, *The End of the Free Market*.

[115] Ibidem.

[116] Polyakova and Meserole, "Exporting Digital Authoritarianism."

The term has a certain analytical vagueness[117] but presents a spectrum without a clear boundary, where Ian Bremmer[118] distinguishes between two ideological poles: the free-market pole and the state capitalism pole. So, rather than defining the term by a set of predefined criteria, we understand digital state capitalism within our conceptual framework as a discursive ideology. This ideology is based on the state's primacy, that yet views economic sovereignty not foremost as a threat but as an instrument for achieving digital sovereignty.

On the individual level, Ian Bremmer[119] notes that the free-market traditionally emphasizes liberal values, while state-capitalism emphasizes authoritarian leadership with central control and limited individual freedoms in favour of national security, social stability, and power preservation. Just like cyber-authoritarianism, digital state capitalism expresses scepticism towards the liberal concept of the Internet as a free, ungoverned space, but practices widespread surveillance of digital activities, censorship of online content, and the use of digital means to suppress dissent.[120] In addition, with the uprise of IoT and AI technologies, the state uses digitalization to monitor and regulate physical activities.[121]

On the economic level, digital state capitalism aims to create a robust and resilient national economy that can compete on a global scale, support national security, and ensure digital supremacy.[122] To reach these goals, mercantilist concepts will be merged with capitalist principles without adopting its liberal ideological framework.[123] Like mercantilism, state capitalism focuses on economic nationalism, emphasizing the dominance in key technologies such as 5G technology, big data, the internet of things, artificial intelligence, and robotics, as well as in critical platforms such as social media, marketplaces, and search engines.[124]

In contrast to Soviet socialism, state capitalism acknowledges the productive role of entrepreneurship and the private sector in driving innovation and economic growth. By liberalizing certain market segments, the government also facilitates the

---

[117] Ilias Alami and Adam D Dixon, "Uneven and Combined State Capitalism," *Environment and Planning A: Economy and Space* 55, no. 1 (August 2021): 72–99, https://doi.org/10.1177/0308518x211037688.

[118] Bremmer, *The End of the Free Market*.

[119] Ibidem.

[120] Bradford, *Digital Empires*.

[121] Ibidem.

[122] Qingxiu Bu, "'Behind the Huawei Sanction: National Security, Ideological Prejudices or Something Else?," *International Cybersecurity Law Review* 5, no. 2 (March 2024): 263–300, https://doi.org/10.1365/s43439-024-00112-6.

[123] Bremmer, *The End of the Free Market*.

[124] Ibidem.

inflow of external knowledge and technology.[125] Yet, this liberalisation is not ideologically motivated, but a pragmatic decision to build domestic expertise and capabilities, which are crucial for staying at the forefront of technological advances.[126] In particular, this liberalisation is safeguarded by mercantilist measures, such as controlling and owning enterprises[127] as well as regulating and asserting authority over digital infrastructures.[128] In addition, the national economy profits from direct investment and promoting domestic industries in strategic sectors through state contracts and subsidies.[129] Within the toolbox of state capitalism are also protectionist policies, which are used to shield the domestic economy from foreign competition.[130] These measures can include tariffs, import restrictions, and other regulatory barriers. In addition, economic protectionism and national security motives are intertwined, sometimes mutually reinforcing each other.[131]

This balance between openness and protection is designed to nurture and stabilize the domestic market until it can compete on a global scale. This balance also exists between the state and corporations. If individual companies threaten excessive market power or if their loyalty is not secured, the state may find itself compelled to take countermeasures and curtail its sovereignty.[132]

China is usually named a paradigmatic example of digital state capitalism.[133] The government employs restrictive censorship and surveillance regimes over individuals and society, reflecting the cyber authoritarian attitude towards civic rights and freedom of expression.[134] Measures in this regard include the Chinese Great Firewall to create a nationalized and controlled sub-network.[135] Still, China allows its digital economy to operate under (controlled) capitalistic rules, including private ownership, international operations, and platform monopolies.[136]

---

[125] Ibidem.
[126] Ibidem.
[127] Xin Zhang and Martin Pfeiffer, "Nach dem Neoliberalismus: Staatskapitalismus in China und Russland," *Osteuropa*, no. 5/6 (2015): 21–32.
[128] Bradford, *Digital Empires*.
[129] Bremmer, *The End of the Free Market*.
[130] Ibidem.
[131] Bu, "Behind the Huawei Sanction."
[132] Shrivastava, "Emerging Dynamics."
[133] Zhang and Pfeiffer, "Nach dem Neoliberalismus."
[134] Polyakova and Meserole, "Exporting Digital Authoritarianism."
[135] James Griffiths, "The Great Firewall of China," 2021.
[136] Zhang and Pfeiffer, "Nach dem Neoliberalismus"; Steve Rolf and Seth Schindler, "The US–China Rivalry and the Emergence of State Platform Capitalism," *Environment and Planning A: Economy and Space* 55, no. 5 (January 2023): 1255–80, https://doi.org/10.1177/0308518x221146545.

This results in shared sovereignty over the digital sphere, coming with beneficial cooperative yet symbiotic scenarios, e.g., governmental subsidies or beneficial policies, if the market supports strategic governmental goals.[137] However, an increased sovereignty of economic actors also comes with examples of conflict. For instance, the Chinese attempt to regain control over their big tech (e.g., Alibaba) by fining them and setting new regulations.[138] Another thread for companies such as Huawei and TikTok is that in the cyber competition among digital empires like China and the USA, they face the risk of being excluded from the global market due to their alleged connections to the regime.[139]

Digital Communitarism

> *"While the distribution of wealth and income need not be equal, it must be to everyone's advantage, and at the same time, positions of authority and offices of command must be accessible to all."*—John Rawls[140]

The central theme of communitarism as a sociological idea is the voluntary collaboration of individuals and non-profit sectors to contribute to the public good and individuals' interests.[141] This stance is linked to criticism of capitalist market logic and the associated isolation. In doing so, communitarianism takes a critical distance from liberalism and its ideology of a competitive societal idea that produces a few winners but a disproportionately large number of losers.[142]

Digital communitarianism seeks to reinterpret the stance on voluntary collaboration and public goods in the digital age.[143] In this school of thought, the individual is not perceived as a self-contained entity in isolation from the community, but rather portrays people as naturally part of given collectives where individual

[137] Rolf and Schindler, "The US–China Rivalry."

[138] Nathalie Marechal, "From Russia With Crypto: A Political History of Telegram," in *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)* (USENIX Association, 2018); Shrivastava, "Emerging Dynamics."

[139] Bu, "Behind the Huawei Sanction."

[140] John Rawls, *A Theory of Justice: Original Edition*, (Harvard University Press, 1971), https://doi.org/10.4159/9780674042605.

[141] Lian Yuming, "Digital Identity," in *Sovereignty Blockchain 2.0* (Springer Nature Singapore, 2022), 87–125, https://doi.org/10.1007/978-981-19-3862-7_3; Robert Wuthnow, "Between the State and Market: Voluntarism and the Difference It Makes," *Rights and the Common Good. The Communitarian Perspective*, 1995.

[142] Emanuel Richter, "Kommunitarismus und Republikanismus," in *Handbuch Kommunitarismus* (Springer Fachmedien Wiesbaden, 2019), 567–89, https://doi.org/10.1007/978-3-658-16859-9_27.

[143] Yuming, "Digital Identity."

freedom is constituted and expressed through communal relationships and responsibilities.[144] With its emphatic communal concept of the individual, it represents a narrative of digital sovereignty that rejects both authoritarian narratives, such as digital authoritarianism and digital state capitalism, as well as libertarian narratives, such as digital anarchism and digital libertarianism.

In the tradition of classical communitarian thinking,[145] digital communitarianism emphasizes society's values as a community of free individuals. From this stance, it advocates that the community should control and govern digitization and that digital means should be used to support collaborative action and civic engagement. [146] Advocates of this narrative emphasize protecting vulnerable groups and preventing a digital divide in society.[147] While digital anarchism focuses on individualistic measures for self-empowerment, communitarian critique this focus as insufficient to overcome the digital divide. Moreover, the digital divide is seen as a consequence of the individualism of society and the deregulation of public policies.[148] Thus, achieving digital inclusion requires community engagement[149] encompassed by public policies and democratic regulation.[150]

To protect vulnerable groups, strict regulations must be enacted for the digital sector, along with measures to strengthen the power of collectives and associations.[151] Moreover, since being 'too big to regulate' threatens civil society, economic

[144] Henrik P. Bang et al., "The State and the Citizen: Communitarianism in the United States and Denmark," *Administrative Theory & Praxis* 22, no. 2 (June 2000): 369–90, https://doi.org/10.1080/10841806.2000.11643456.

[145] Richter, "Kommunitarismus und Republikanismus."

[146] Michael Rushton, "Communitarianism," in *The Moral Foundations of Public Funding for the Arts* (Springer International Publishing, 2023), 93–113, https://doi.org/10.1007/978-3-031-35106-8_5.

[147] Cristina Kiomi Mori, "'Digital Inclusion': Are We All Talking about the Same Thing?," in *ICTs and Sustainable Solutions for the Digital Divide* (IGI Global, 2011), 45–64, https://doi.org/10.4018/978-1-61520-799-2.ch003.

[148] Ibidem.

[149] Anne Weibert and Volker Wulf, "'All of a Sudden We Had This Dialogue… ': Intercultural Computer Clubs' Contribution to Sustainable Integration," in *Proceedings of the 3rd International Conference on Intercultural Collaboration*, ICIC '10 (ACM, 2010), 93–102, https://doi.org/10.1145/1841853.1841868.

[150] Mori, "Digital Inclusion."

[151] Heiko Dünkel, "Kollektiver Rechtsschutz bei Datenschutzrechtsverstößen: Durchsetzung der DSGVO durch Deutsche Verbraucherverbände," *Datenschutz Und Datensicherheit - DuD 43*, no. 8 (July 2019): 483–87, https://doi.org/10.1007/s11623-019-1148-9.

sovereignty must be restricted to ensure both individual and governmental sovereignty.[152]

The strong emphasis on civic sovereignty, which combines individual and governmental powers, in digital communitarianism is further reflected in its focus on citizen participation and community engagement. This engagement is not exclusively focused on the digital sphere, e.g., for free software policies. Still, it can be seen as a broader mix of social justice, digital rights, and active engagement in the design of the digitization megatrend.[153]

Contrary to a technophobic stance, digital communitarianism views the digitalization of society not as a threat to communal values but rather as an opportunity to reinforce these values through enhanced democratic engagement. Through digital means for e-democracy[154] services, e-voting,[155] and e-participation,[156] democratic processes can become more accessible, inclusive, and responsive. Furthermore, digital communitarianism emphasizes the importance of digital literacy,[157] highlighting the potential of digitalization to provide free, accessible educational opportunities for the masses, e.g., collaboratively created encyclopaedias, online tutorials, and Mass Open Online Courses (MOOCs).[158] In short, individuals leverage their values through democratic participation in governmental organizations and democratic structures.

The concept of communitarianism does not present a coherent narrative. It is instead interpreted in different ways depending on the historical context. For example, Bang et al. study the American roots of this concept and compare it with the

---

[152] Bernard Arogyaswamy, "Big Tech and Societal Sustainability: An Ethical Framework," *AI & SOCIETY* 35, no. 4 (March 2020): 829–40, https://doi.org/10.1007/s00146-020-00956-6.

[153] John L Sullivan, "Free, Open Source Software Advocacy as a Social Justice Movement: The Expansion of F/OSS Movement Discourse in the 21st Century," *Journal of Information Technology & Politics* 8, no. 3 (July 2011): 223–39, https://doi.org/10.1080/19331681.2011.592080.

[154] Lincoln Dahlberg, "Democracy via Cyberspace: Mapping the Rhetorics and Practices of three Prominent Camps," *New Media & Society* 3, no. 2 (2001): 157–77, https://doi.org/10.1177/14614440122226038.

[155] J Paul Gibson et al., "A Review of E-Voting: The Past, Present and Future," *Annals of Telecommunications* 71, no. 7–8 (2016): 279–86, https://doi.org/10.1007/s12243-016-0525-8.

[156] Herbert Kubicek, "E-Participation," in *E-Government* (Springer, 2010), 195–225, https://doi.org/10.1007/978-3-8349-6343-7_10.

[157] Moonsun Choi, "A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age," *Theory & Research in Social Education* 44, no. 4 (2016): 565–607, https://doi.org/10.1080/00933104.2016.1210549.

[158] Ebba Ossiannilsson, "MOOCS for Lifelong Learning, Equity, and Liberation," in *MOOC (Massive Open Online Courses)* (IntechOpen, 2022), https://doi.org/10.5772/intechopen.99659.

communitarian, social-democratic thinking of Denmark and Scandinavian societies.[159] Concerning digital communitarianism, such influences can also be recognized in the European Union and its digital policy. With its regulatory measures, for instance, the AI Act, General Data Protection Regulation (GDPR), the Digital Services Act (DSA), or the Digital Markets Act (DMA) aim to create a safer digital space with fundamental rights of individuals and equitable regulated conditions for all businesses.[160] In the fight for digital sovereignty among the different levels, Heidebrecht et al. conclude that in the EU, "*[s]takeholders and public authorities rather than business actors have become more important in governance processes, and more market-correcting instruments have been introduced*."[161]

Digital Libertarianism

"Don't be evil"—Google

Digital libertarianism is considered one of the formative ideologies in the early days of Silicon Valley.[162] It is rooted in libertarian thinking of the individual as a free economic agent.

At first glance, the libertarian narrative appears identical to the anarchist narrative, and also historically both schools of thought stem from a shared anti-authoritarian foundation.[163] Anarchism emphasizes individual freedom, which manifests in resistance against all forms of oppression, which includes not only governmental oppression but also resistance against capitalistic power and surveillance. Contrary to this, the libertarian school of thought advocates for free markets and the rights to private property as sources of societal prosperity and growth.[164] This also shaped the tech culture of Silicon Valley, where, e.g., the Google mantra "Don't be evil" aims to express an ethos of innovating technology to make the world a better place.[165]

---

[159] Bang et al., "The State and the Citizen."

[160] Matthias Leistner, "The Commission's Vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a Critical Primer," *Journal of Intellectual Property Law & Practice* 16, no. 8 (2021): 778–84.

[161] Heidebrecht, "From Market Liberalism to Public Intervention."

[162] Pohle et al., "Digital Sovereignty."

[163] White and Kossoff, "Anarchism, Libertarianism and Environmentalism."

[164] Ibidem.

[165] Shirin Ghaffary, "'Don't Be Evil' Isn't a Normal Company Value. But Google Isn't a Normal Company," 2021, https://www.vox.com/recode/2021/2/16/22280502/google-dont-be-evil-land-of-the-giants-podcast [accessed: 2024-04-23].

Concerning the governmental level, a weak state is seen as a benefit. The absence of state control and regulation is seen as a prerequisite for individual freedom and social progress: "Libertarian and neoliberal ideologies defend the hegemony of the market over other social institutions."[166] Thus, libertarian economists such as Ludwig van Mises stress that the economic sector is prosperous only if state intervention in the economic sphere is avoided.[167]

Similarly, cyber-libertarians distrust governmental control but advocate for the Internet as a space autonomous from the state and other authoritarian forms of control.[168] The Internet is seen as a perfect marketplace, not just for ideas,[169] but also for commodities,[170] with the liberty of individuals to satisfy private interests through technologically mediated participation and consumerism. Government intervention in the digital sphere is seen sceptically because of the risk that such interventions can hinder the flourishing of innovative ideas, lead to over-regulation, and inefficient resource allocation, thereby negatively impacting the prosperity of society as a whole.[171]

In cyber-libertarianism, the relationship between the individual and economic levels is not very pronounced. This results from the fact that in cyber-libertarianism thinking, people and organizations are conceptualized as equal market participants equipped with the same set of rights, capabilities, and resources. From this stance, independent bloggers and multinational social media corporations are regarded as individual agents, each endowed with the same natural rights, freedoms, and protections against state intrusion.[172] Accordingly, companies per se are not seen

---

[166] Aitor Jiménez, "The Silicon Doctrine," *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 18, no. 1 (2020): 322–36, https://doi.org/10.31269/triplec.v18i1.1147.

[167] Ludwig Mises, *Liberalism* (Ludwig von Mises Institute, 1985).

[168] Lincoln Dahlberg, "Cyber-Libertarianism 2.0: A Discourse Theory/Critical Political Economy Examination," *Cultural Politics* 6, no. 3 (2010): 331–56, https://doi.org/10.2752/175174310x12750685679753.

[169] Ibidem.

[170] Jane P. Laudon and Kenneth C. Laudon, *Management Information Systems: Managing the Digital Firm* (Pearson Educacion, 2004).

[171] Jiménez, "The Silicon Doctrine."

[172] Karl Widerquist, "A Dilemma for Libertarianism," *Politics, Philosophy & Economics* 8, no. 1 (2009): 43–72, https://doi.org/10.1177/1470594x08098871; Samuel Freeman, "Illiberal Libertarians: Why Libertarianism Is Not a Liberal View," *Philosophy & Public Affairs* 30, no. 2 (2001): 105–51, https://doi.org/10.1111/j.1088-4963.2001.00105.x.

as a threat to personal sovereignty, as the informed individual actor could enforce its rights in court.[173]

Cyber-libertarian advocates also argue that the Internet brings a new era of consumer sovereignty: Today, consumers have access to the global market, where digitalization reduces transaction costs, increases access to information, and allows easy comparison of products and prices.[174] This leads to unprecedented power, where buyers can avoid goods and services they do not want.[175]

According to the cyber-libertarian argument, an increase in consumer and privacy regulations would not increase individual sovereignty but only increase bureaucracy.[176] Instead, people can satisfy their privacy and security needs through the growth of the security and privacy industry, which provides the needed commercial tools and services, such as using commercial virus and malware scanners,[177] taking out cyber-insurance policies,[178] managing their digital identities, and circumventing censorship with commercial reputation managers[179] and VPN services.[180] Opponents of libertarianism, however, argue that such commodification of security neglects the special protection needs of vulnerable groups and the power inequalities of digital oligopolies and aristocracies.[181]

The tech culture of Silicon Valley is heavily influenced by digital libertarianism.[182] This influence extends beyond Silicon Valley to the United States as a whole, which is shaped significantly by liberal ideas of free speech as well as an

---

[173] Todd J Zywicki, "Libertarianism, Law and Economics, and the Common Law," *SSRN Electronic Journal* 16 (2012): 309, https://doi.org/10.2139/ssrn.2174534.

[174] Laudon and Laudon, *Management Information Systems*.

[175] Alan Shipman, "Privatized Production, Socialized Consumption? Old Producer Power Behind the New Consumer Sovereignty," *Review of Social Economy* 59, no. 3 (2001): 331–52, https://doi.org/10.1080/00346760110053932.

[176] "Unternehmen beklagen Bürokratie durch DSGVO," March 2024, https://www.security-insider.de/unternehmen-beklagen-buerokratie-durch-dsgvo-a-f352e3d7414efcfb862ac47e5742f49c/ [accessed: 2024-04-23].

[177] "The Best Antivirus Software for 2024," April 2024, https://au.pcmag.com/antivirus/8949/the-best-antivirus-protection [accessed: 2024-04-23].

[178] BaFin, "Cyber Insurance," 2022, https://www.bafin.de/EN/Verbraucher/Versicherung/Produkte/Cyber/cyberversicherung_node_en.html [accessed: 2024-04-23].

[179] "The Best Services for Deleting Yourself from the Internet in 2024," 2024, https://www.zdnet.com/article/best-data-removal-services/ [accessed: 2024-04-23].

[180] "10 Best VPN Services of 2024–Forbes Advisor," 2024, https://www.forbes.com/advisor/business/software/best-vpn/ [accessed: 2024-04-23].

[181] Widerquist, "A Dilemma for Libertarianism"; Zywicki, "Libertarianism, Law and Economics."

[182] Pohle et al., "Digital Sovereignty."

economic policy characterized by a preference for industry self-regulation and resistance to heavy-handed government control.[183] This ideology is also seen as an essential factor in the rise of the United States as a digital empire, which has led to the global dominance of its digital sector.[184] Yet, in recent years, there have been increasing calls for stronger regulation of the digital economy to address the risk of forming digital trusts and monopolies,[185] as well as the practices of companies to surveil and manipulate their users.[186]

Digital Pluralism

"Inefficiency is to be our safeguard against despotism."—Garry Wills[187]

Digital pluralism is based on a finely balanced equilibrium of checks and balances, in which the digital sphere should reflect a broad spectrum of voices, interests, and perspectives.

Pluralistic ideas of digital sovereignty are discussed at various levels, such as nationally, concerning digital media pluralism,[188] or internationally, regarding a multi-stakeholder approach to digital governance.[189] Specifically, Internet and AI technologies are recognized as shared global resources where pluralistic principles should be applied to ensure their equitable and ethical use.[190] Guggenberger also delves into pluralistic concepts by addressing the systemic threat of digital oligopolies, stressing that "contemporary antitrust doctrine alone cannot hope to provide sufficient relief to the digital public sphere."[191]

---

[183] Bradford, *Digital Empires*.

[184] Ibidem.

[185] Diane Bartz, "Bipartisan US Lawmakers Introduce Bill Aimed at Google, Facebook Ad Clout," *Reuters*, March 2023, https://www.reuters.com/world/us/bipartisan-us-lawmakers-introduce-bill-aimed-google-facebook-ad-clout-2023-03-30/ [accessed: 2024-04-23].

[186] Zuboff, *The Age of Surveillance Capitalism*.

[187] Garry Wills, *A Necessary Evil: A History of American Distrust of Government* (Simon and Schuster, 2002).

[188] Nicola Lucchi, "Digital Media Pluralism," *In Transition*, n.d., 91; Elda Brogi, "The Media Pluralism Monitor: Conceptualizing Media Pluralism for the Online Environment," *El Profesional de La Información* 29, no. 5 (2020), https://doi.org/10.3145/epi.2020.sep.29.

[189] Huw Roberts, Emmie Hine, and Luciano Floridi, "Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance," in *Quo Vadis, Sovereignty?* (Springer Nature Switzerland, 2023), 51–75, https://doi.org/10.1007/978-3-031-41566-1_4.

[190] Sebastian Berg and Jeanette Hofmann, "Digital Democracy," *Internet Policy Review* 10, no. 4 (2021), https://doi.org/10.14763/2021.4.1612.

[191] Nikolas Guggenberger, "Moderating Monopolies," *Berkeley Tech. LJ* 38 (2023): 119, https://doi.org/10.15779/Z389K45T9Q.

Digital Pluralism emphasizes that the digital sphere must not be dominated by a few actors but shared by all stakeholders.[192] The balanced distribution of power ensures that single actors do not threaten the sovereignty of others, be it the state (see *digital authoritarianism*), corporate oligopolies (see *digital corporatocracy*), or the boundless freedom of the individual (see *digital anarchism*). Such power imbalances harbour the risk of systemic fragility, the suppression of opinions, and a decline in innovative strength.[193]

For this reason, digital pluralism advocates for an inclusive and more resilient approach that ensures that all stakeholders, including marginalized and underrepresented communities, have a voice in the design and use of digital technologies.[194] It extends the horizontal approach of multi-state governance into the vertical by expanding it into a pluralistic approach between the vertical levels.[195] It also favours technological pluralism instead of a monoculture of a few platforms and services for the same reasons.[196]

Accordingly, the power of the government should be restricted and justified. Nevertheless, governments should play an active role in shaping regulations and infrastructures rather than being passive observers.[197] This reflects the growing recognition of the government's involvement in the digital world, which extends beyond its traditional regulatory role and requires active participation in shaping the digital landscape, e.g., to ensure cyber security based on new economic policies[198] or founding own infrastructures.[199]

Similarly, the power of companies presents an important building block for the balance of forces. This implies not expropriating companies but restricting their

---

[192] Nisha Holla, "Democratising Technology for The Next Six Billion," *Digital Debates*, 2020, 12; Guggenberger, "Moderating Monopolies."

[193] Guggenberger, "Moderating Monopolies. "

[194] Gregory Rolan et al., "Digital Equity through Data Sovereignty: A Vision for Sustaining Humanity," *iConference 2020 Proceedings*, 2020, http://hdl.handle.net/2142/106548.

[195] Jeremy Malcolm, *Multi-Stakeholder Governance and the Internet Governance Forum* (Terminus Press, 2008).

[196] Divya Siddarth et al., "How AI Fails Us," *arXiv Preprint arXiv:2201.04200*, 2021.

[197] Huw Roberts et al., "Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies," *SSRN Electronic Journal*, 2021, https://doi.org/10.2139/ssrn.3937345.

[198] Benjamin Farrand and Helena Carrapico, "Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity," *European Security* 31, no. 3 (2022): 435–53, https://doi.org/10.1080/09662839.2022.2102896.

[199] Braud et al., "The Road to European Digital Sovereignty with Gaia-X and IDSA;" Pohle et al., "Digital Sovereignty."

power due to the tendency of digital monopolies.[200] This view recognizes the autonomy of companies, but, at the same time, emphasizes their social responsibility, as rights and opportunities are granted by society.[201] The shared sovereignty in the pluralistic concept prevents corporations from gaining excessive power based on democratically justified regulations[202] and technical measures such as interface compatibility and open standards to prevent lock-in effects.[203]

This dual view, for example, can be observed in the realm of digital infrastructures. Companies are both beneficiaries of public (infra-)structures and creators of such digital spaces, which contributes to the independence of the system as a whole from external actors by providing innovation.[204] This highlights the role of companies as a driving force for digital innovation and economic growth.[205] However, this is not achieved due to a weak state, but is instead enabled by a strong state, as it provides the public infrastructures for economic success.[206]

At the individual level, like digital communitarianism, digital pluralism argues for digital inclusion, where all people should be empowered to participate actively in a digital pluralistic society.[207] This includes the right to access digital services and information,[208] and the right to control personal data, deciding how and when it is used.[209] In this sense, digital pluralism is closely related to concepts of digital equity, which highlight equal access and rights,[210] as well as digital citizenship as an

---

[200] Herbert Hovenkamp, "Antitrust and Platform Monopoly," *SSRN Electronic Journal* 130 (2020): 1952, https://doi.org/10.2139/ssrn.3639142; Daniel McIntosh, "We Need to Talk about Data: How Digital Monopolies Arise and Why They Have Power and Influence," *Journal of Technology Law & Policy* 23, no. 2 (2018): 185.

[201] Rutger Claassen, "Political Theories of the Business Corporation," *Philosophy Compass* 18, no. 1 (2022), https://doi.org/10.1111/phc3.12892.

[202] Anke S. Obendiek, "Take Back Control? Digital Sovereignty and a Vision for Europe," Policy Paper (Hertie School, 2021), https://opus4.kobv.de/opus4-hsog/frontdoor/deliver/index/docId/4540/file/Policy-Paper_Obendiek.pdf.

[203] Siddarth et al., "How AI Fails Us."

[204] Lokke Moerel and Paul Timmers, "Reflections on Digital Sovereignty," *EU Cyber Direct, Research in Focus Series*, January 2021.

[205] Claassen, "Political Theories."

[206] Paul Keller, "European Public Digital Infrastructure Fund White Paper," *Open Future*, December 2022; "The Case for Investing in Digital Public Infrastructure," n.d., https://hbr.org/2023/05/the-case-for-investing-in-digital-public-infrastructure.

[207] Sullivan, "Free, Open Source Software Advocacy"; Choi, "A Concept Analysis."

[208] Gwen Solomon, "Digital Equity: It's Not Just about Access Anymore," *Technology & Learning* 22, no. 9 (2002): 18–20.

[209] Rolan et al., "Digital Equity through Data Sovereignty."

[210] Solomon, "Digital Equity"; Rolan et al., "Digital Equity through Data Sovereignty."

advanced form of digital literacy.[211] At the same time, the power and rights of the individual are not unrestricted but regulated in relation to the legitimate interests of other actors and society as a whole.

This highlights the complexity of balancing digital sovereignties within the pluralistic concept. The power constellations are fragile, dynamic, and reciprocal.[212] The relationships among the actors are characterized by cooperation and conflict, leading to ongoing dialogue and negotiation of rules, norms, and resources.[213] The digital ecosystem with a multitude of agencies and power distributions comes with a complex web of interests, goals, and dynamics in managing digital sovereignty.[214] Due to these dynamics, the finely tuned balance of digital sovereignty is always at risk of destabilization.

Empirically, elements of pluralistic sovereignties can be observed everywhere, as no actor is entirely powerless or possesses complete sovereignty, as assumed for our binary model. However, pluralistic sovereignty as an ideology means that all actors have power in some sense but respect each other's digital sovereignty and recognize the constant adjustment of checks and balances. Regarding this, Estonia is an interesting example of a balanced relationship between state control, a robust digital economy, and individual freedom. Through advanced digital infrastructures and services, Estonia has achieved digital sovereignty, enabling citizens to control personal data while facilitating access to government services. For example, they have ensured high digital literacy among individuals, broad access to digital public services,[215] and high privacy standards in their service offerings, e.g., the health portal.[216] In addition, with its e-Residency service, Estonia aims to unlock every world citizen's entrepreneurial potential.[217] This service enables business owners worldwide to run an

---

[211] Choi, "A Concept Analysis."

[212] Tretter, "Sovereignty in the Digital."

[213] Lambach and Monsees, "Beyond Sovereignty as Authority: The Multiplicity of European Approaches to Digital Sovereignty"; Lambach and Oppermann, "Narratives of Digital Sovereignty."

[214] Roberts, Hine, and Floridi, "Digital Sovereignty"; Bradford, *Digital Empires*; Lawo et al., "Human-Centred Digital Sovereignty."

[215] Marju Himma-Kadakas and Ragne Kõuts-Klemm, "Developing an Advanced Digital Society: An Estonian Case Study," in *Internet in the Post-Soviet Area* (Springer International Publishing, 2023), 109–33, https://doi.org/10.1007/978-3-031-32507-6_6.

[216] Jaan Priisalu and Rain Ottis, "Personal Control of Privacy and Data: Estonian Experience," *Health and Technology* 7, no. 4 (June 2017): 441–51, https://doi.org/10.1007/s12553-017-0195-1.

[217] Taavi Kotka, Carlos Vargas, and Kaspar Korjus, "Estonian E-Residency: Redefining the Nation-State in the Digital Era," *University of Oxford Cyber Studies Programme Working Paper* 3 (2015), https://www.raulwalter.com/prod/wp-content/uploads/2015/10/Working_Paper_No.3_Kotka_Vargas_Korjus.pdf.

EU business, complete with essential administrative and banking tasks, entirely online without the need to visit physically. In this multitude of measures, Estonia demonstrates that it does not view digital sovereignty as a zero-sum game but understands societal and economic progress in respecting and promoting digital sovereignty at various levels.

Digital Anomie

> *"Africa is currently experiencing a cultural void akin to anomie and precipitating toward eventual death in a digital world."*—Moses Ofome Asak[218]

Digital anomie refers to a scenario in which none of the actors in vertical relationships—the government, businesses, or individuals—exert significant control over the digital sphere. It reflects a fragmented and chaotic digital landscape characterized by minimal regulation, limited business influence, and individuals facing challenges asserting their rights and maintaining control over their digital experiences.

Anomic conditions create a legal vacuum and law enforcement, so people operate based on personal interests without regard for communal rules. Anarchist and anomic thinking interpret this situation in a fundamentally different way. Anarchist thinking emphasizes freedom from domination as the liberation of the individual. On the other hand, an anomic lens sees this situation as dangerous and harmful to society, in which the individual is helplessly at the mercy of foreign powers on the horizontal level.[219] Because of the lack of digital sovereignty at the level, people find themselves neither protected nor supported by the state or the economy.

In postcolonial studies, anomic perspectives are closely associated with the critique of digital colonialism, which describes the digital dominance of the Global North over the Global South.[220] This dominance is seen as a form of neo-colonialism where powerful countries and corporations from the Global North use digital technologies to maintain and expand their exploitation of developing countries.[221] This critique aligns with concerns about cultural imperialism, economic exploitation,

---

[218] Moses Ofome Asak, "Sovereignty and the Scramble for the Heart of Africa in a Digitalized World," in *The Russia-Ukraine War from an African Perspective* (Langaa RPCIG, 2023), 347–74, https://doi.org/10.2307/jj.8784618.14.

[219] Bradford, *Digital Empires*; Pinto, "Digital Sovereignty or Digital Colonialism."

[220] Michael Kwet, "Digital Colonialism: US Empire and the New Imperialism in the Global South," *Race & Class* 60, no. 4 (2019): 3–26, https://doi.org/10.1177/0306396818823172.

[221] Ibidem.

and the imposition of foreign values and systems on local cultures and economies through digital means.

While developing countries find themselves in digital dependence on the Global North, the latter exercises complete control over both them and their access to digital goods and infrastructure. Asak contends that "*the West uses data from the internet to watch and control everything Africans do*,"[222] indicating that new media serves not solely surveillance purposes but also as a tool to promote the dominating and hegemonic Western (cyber-)culture.[223] Elmimouni et al. further note that political activists in the Global South accuse US social media platforms of unfairness and censorship regarding their content moderation policies, as these practices suppress, e.g., legitimate positions in the Israeli-Palestinian conflict.[224] The activists, nevertheless, must use foreign platforms due to lack of alternatives.

Since its introduction during the colonial era, media technology has been a strategic move to consolidate control and influence over the colonized regions.[225] Today, multinational corporations, e.g., the GAFANG from the Global North, use their monopoly over the digital ecosystem in the Global South to perpetuate their economic domination[226] and use it as a fertile field for data mining as new material.[227] As noted by Avila Pinto, the Global South "*are the disputed territory of tech empires, because whoever gets them locked into their digital feudalism, holds the key to the future*".[228] In contrast to the state capitalistic power, e.g., of China, this situation could not be overcome by establishing its own national digital economy.

Postcolonial activists emphasize that the exploitation and imbalances inherent in current global power distributions must be addressed. Yet, it is striking that the marginalized position of the Global South is also reflected in the discourse on digital sovereignty. For instance, Anu Bradford largely ignores the postcolonial

---

[222] Asak, "Sovereignty."

[223] Artwell Nhemachena, Nokuthula Hlabangane, and Maria B. Kaundjua, "Relationality or Hospitality in Twenty-First Century Research? Big Data, Internet of Things, and the Resilience of Coloniality on Africa," *Modern Africa: Politics, History and Society* 8, no. 1 (2020): 105–39, https://doi.org/10.26806/modafr.v8i1.278; Asak, "Sovereignty."

[224] Houda Elmimouni et al., "Shielding or Silencing?: An Investigation into Content Moderation during the Sheikh Jarrah Crisis," *Proceedings of the ACM on Human-Computer Interaction* 8, no. GROUP (February 2024): 1–21, https://doi.org/10.1145/3633071.

[225] Elaine Windrich and Louise Bourgault, "Mass Media in Sub-Saharan Africa," *African Studies Review* 39, no. 3 (1996): 200, https://doi.org/10.2307/524952.

[226] Kwet, "Digital Colonialism."

[227] Nhemachena, Hlabangane, and Kaundjua, "Relationality or Hospitality."

[228] Pinto, "Digital Sovereignty or Digital Colonialism."

perspective in her extensive analysis of today's digital empires.[229] This omission is significant because it illustrates a lack of economic digital power as well as the regulatory power of the Global South. This lack of autonomy and control can cascade down to individual citizens from the national and economic levels, potentially leaving them more vulnerable in the digital domain. As a result, digital policies and strategies of digital empires such as the USA, EU, and China continue to exert control and exploit the digital landscapes of less powerful regions. As such, the Anomie does not exist as a vacuum of power, but a space where the local society, due to a lack of power, is controlled by extraterritorial powers resulting in anomie at intra-societal level, but, e.g., corporatocracy at the international or intersocietal level.

Discussion

Our model enriches current research on digital sovereignty by bridging the gap between the theoretical,[230] narrative,[231] as well as actor-network lens.[232] The narrative lens focuses on analysing existing political narratives. In similar, ways the actor-network lens analyses existing constellations of power but focuses on the practices within a certain context or based on a certain event. Our binary model provides analytical, yet theoretical, narratives, based on abstract actor-network relations. In this sense, the model is theoretic in nature but still extends the existing theoretical lens that focuses on the concept and its meaning over time as such, by uncovering the often-implicit assumptions about the relational character of digital sovereignty. For example, the two-dimensional empirical model of Fratini et al. makes such assumption by focusing on market regulation from a governmental perspective only.[233] The economic actor especially its agency is neglected. Our lens embeds this view, in more detailed narratives and thus ties a connection to existing political/economical ideas.

The differences between the various narratives become visible through the binary lens of weak and strong actors. However, this binary concept comes at the price of being a significant simplification. The hierarchy of the levels is a further simplification as horizontal dependencies must also be considered.[234] Real-world

[229] Bradford, *Digital Empires*.
[230] Pohle et al., "Digital Sovereignty."
[231] Lambach and Oppermann, "'Narratives of Digital Sovereignty."
[232] Tretter, "Sovereignty in the Digital."
[233] Samuele Fratini et al., "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models," *Digital Society* 3, no. 3 (2024): 59, https://doi.org/10.1007/s44206-024-00146-7.
[234] Bradford, *Digital Empires*.

sovereignty manifests itself in many shades, characterized by manifold actors within a flat, complex network of conflicts and cooperation.[235]

Thus, as empirical categories, our model, at its best, presents under-complex ideal types in the sense of Max Weber, which glosses over the shades in reality to give orientation. In this matter, countries such as China, Russia, or Iran are representative of digital authoritarian regimes with a tendency to state capitalistic concepts, where the economy is seen as a tool to increase the regime's sovereignty. In contrast, the USA tends to be associated with anarchist-libertarian ideas, the EU with communitarian-pluralist ideas, and the Global South is typically seen as a representative of digital anomie. This contrasts with the mapping of Fratini et al., which also visualizes nuances between (supra-)national states by comparing their policies based on empirical categories from literature.[236] On the one hand, this approach allows for a detailed comparison of governmental actors, but this distinctive power, on the other hand, comes for the cost of analytical, yet theoretical power, as, e.g., narratives of pluralism or anomie are missing. As narrative categories, our model highlights the diverse discourses and ideologies shaping the fight for digital sovereignty. Our work demonstrates that digital sovereignty is not merely a battleground of competing technologies and strategies but a complex field of discursive formations, each acting as both a repository of knowledge and a mechanism of power. Our analysis reconstructed competing discursive formations in the sense of Michael Foucault,[237] which are reflected as systems of power and knowledge in the fight for digital sovereignty. It shows how different discourses converge and adapt in the field of digital sovereignty, reshaping the epistemic landscape and influencing the governance of digital spaces. In this manner, the outlined narratives do not provide concrete regulatory or individual measures to implement digital sovereignty but present discursive strategies to legitimate or critique them.

The outlined narratives are rhetoric figures that mobilize ideological support, framing the digital sovereignty debate to suit their strategic objectives best. The apparent under-complexity of the narratives is not an accidental defect but rather a deliberate act of strategic essentialism to shape arguments and dominate discourses. Omitting nuances, contradictions, and objections but using metaphors, polemics, and narratives is necessary to gain ground and secure terrain.

---

[235] Tretter, "Sovereignty in the Digital."

[236] Fratini et al., "Digital Sovereignty."

[237] Reiner Keller, *Doing Discourse Research: An Introduction for Social Scientists*, ed. Bryan Jenner (SAGE, 2013).

For example, in the battle against corporate power Shoshana Zuboff[238] notably employs the metaphor of "surveillance capitalism" to compare the data practices of corporations to those of state surveillance regimes. While this notion is polemic, as GAFAM is not imprisoning misbehaving citizens, the metaphor presents a powerful tool in her critique to gain popularity. Her work also provides another example of simplifying arguments to be effective. For instance, although Zuboff highly values individual autonomy, she decides not to view consumerism as an expression of individual sovereignty for strategic reasons. Instead, she frames it as the consequence of targeted commercial manipulation techniques. As a result, personal freedom in surveillance capitalism will be impossible, which presents a kind of collateral damage to the narrative in the fight against capitalistic suppression.

The rhetoric of digital anarchism adopts a different approach to achieve its goals. Here, too, individual autonomy is threatened by authorities and central institutions such as the state and economy. In opposition to the behaviouristic metaphor of users a lab rat controlled by external forces, digital anarchism chooses a narrative of self-empowerment and, extending Nietzsche's ideal, it promotes the concept of the digital Übermensch—a superhuman figure emblematic of utmost independence and self-determination.[239] This discursive strategy does more than vaporize individuality; it constructs an archetype of personal sovereignty that transcends the limitations of any form of centralized control. In this configuration, the narrative becomes particularly seductive to an academic techno-elite, among whom self-realization, the free exchange of ideas, and a devout faith in technology are highly esteemed. Simultaneously, this discursive formation complicates digital anarchism's ability to argue for the digital inclusion of vulnerable and marginalized groups by state interventions.

Moreover, the technological or infrastructural perspective as an important branch of research[240] is strongly interdependent with the uncovered narratives. Yet, one could argue that a dualism of infrastructures and narratives exists. Infrastructures are used as a tool to establish mechanisms of sovereignty and vice-versa shape power structures. The narratives described in the model manifest themselves through infrastructural actions as path dependencies. One example of this is the narrative of digital anomie.

---

[238] Zuboff, *The Age of Surveillance Capitalism*.

[239] Douglas Kellner, "Metaphors of Cyberspace and Digital Technologies," in *Technology and Democracy: Toward A Critical Theory of Digital Technologies, Technopolitics, and Technocapitalism* (Springer Fachmedien Wiesbaden, 2021), 35–66, https://doi.org/10.1007/978-3-658-31790-4_2.

[240] Musiani, "Infrastructuring Digital Sovereignty"; Möllers, "Making Digital Territory."

Adopting post-colonialist narratives, the narrative of digital anomie, draws attention to the imbalances and disruptions caused by digital practices and connects these to broader historical and social contexts. The post-colonial perspectives about digital sovereignty shape the discourse by critically examining how colonial legacies continue to shape power dynamics and access in the digital world, emphasizing the exploitation and digital divide that persist on a global scale. *Don't be evil,* as the mantra of Silicon Valley here appears as historical amnesia and Western arrogance, as today's global platform economy, as an infrastructure, means that users from the Global South must submit to policies and terms of condition written with Western[241] (or Chinese[242]) values and interests in mind. Here, infrastructural supremacy is converted to continuous political and economic supremacy and hard to escape path dependencies. The missionary zeal of the mantra glosses over the colonial legacies and ongoing economic exploitation that are part of the West's interactions with other regions, suggesting a selective memory regarding past and present injustices.

The discourse on liberal-democratic ideas of digital sovereignty shows the other side of the coin. It illustrates how societies create infrastructures at various levels to establish values of freedom based on technological sovereignty and thus free themselves from the sovereignty claims of third parties.[243] Regarding this, two lines of thought can be identified: The first line of thought stresses that sovereignty should be placed in the hands of citizens rather than in companies or governmental institutions,[244] to prevent governments from exercising power via infrastructures, e.g., internet shutdowns to suppress other narratives.[245] Thus, there is a strong focus on measures to increase self-empowerment, digital literacy, and self-protection tools. The second line of thought views the digital sovereignty of the individual as a human right. Respecting and protecting it shall be the duty of all state authorities. This position favours stricter regulatory measures and the demand for transparency concerning algorithms and business models.[246] Here, the narratives, as outlined, can be understood as rhetoric figures of dual character. They mobilize infrastructuring[247]

[241] Kwet, "Digital Colonialism."
[242] Folashadé Soulé, "Digital Sovereignty in Africa: Moving beyond Local Data Ownership," *Centre for International Governance Innovation Policy Brief* No. 185, 2024, https://www.cigionline.org/static/documents/PB_no.185.pdf.
[243] Musiani, "Infrastructuring Digital Sovereignty."
[244] Pohle et al., "Digital Sovereignty"; Lambach and Oppermann, "Narratives of Digital Sovereignty."
[245] Ihsan and Saleem, *The Nexus of Religious Populism*.
[246] Pohle et al., "Digital Sovereignty"; Lambach and Oppermann, "Narratives of Digital Sovereignty."
[247] Musiani, "Infrastructuring Digital Sovereignty."

activities to create nationalized or monopolized information infrastructure[248] or prevent discourses to flourish to keep a monopoly.

Conclusion

In this article we examined digital sovereignty as a dynamic phenomenon in the field of tension between state institutions, economic actors, and individuals. Our model enriches research on digital sovereignty by emphasising the interdependence between state, economic and individual actors. Through a binary model with eight narratives of digital sovereignty, the relational character is revealed and a gap between theoretical and actor-network perspectives is closed. The model serves as a tool to grasp the complexity of the topic and to analyse the discourses in the struggle for digital sovereignty. It sheds light on the interplay between infrastructure and discursive formations in the stabilisation of power in the digital space. Analysing rhetorical strategies such as metaphors and polemics contributes to a deeper understanding of the dynamics.

Although the narratives do not provide concrete instructions for action, they serve as strategies to legitimise or criticise measures in the digital space. Simplifying narratives by juxtaposing weak and strong actors is a deliberate strategy to sharpen arguments and gain interpretative sovereignty to mobilize practices to monopolize digital infrastructure. Moreover, this paper did not to outline which concept of digital sovereignty is correct, beneficial, or even the best one. Instead, our goal was to make discursive structures visible. For instance, the review of the discourse landscape shows that it is common in the literature to equate digital sovereignty with the Western ideal of individual freedom. However, this narrow focus risks fostering a silo mentality that excludes alternative narratives from mainstream discourse, neglecting how other societies envision their digital futures, especially those that do not share the same historical and ideological backgrounds.

[248] Möllers, "Making Digital Territory."

Bibliography

"10 Best VPN Services of 2024 – Forbes Advisor," 2024. https://www.forbes.com/advisor/business/software/best-vpn/ [accessed: 2024-04-23].

Alami, Ilias, and Adam D Dixon. " Uneven and Combined State Capitalism." *Environment and Planning A: Economy and Space* 55, no. 1 (August 2021): 72–99. https://doi.org/10.1177/0308518x211037688.

Arogyaswamy, Bernard. "Big Tech and Societal Sustainability: An Ethical Framework." *AI & SOCIETY* 35, no. 4 (March 2020): 829–40. https://doi.org/10.1007/s00146-020-00956-6.

Asak, Moses Ofome. "Sovereignty and the Scramble for the Heart of Africa in a Digitalized World." In *The Russia-Ukraine War from an African Perspective*, 347–74. Langaa RPCIG, 2023. https://doi.org/10.2307/jj.8784618.14.

Autolitano, Simona, and Agnieszka Pawlowska. "Europe's Quest for Digital Sovereignty: GAIA-X as a Case Study." *IAI Papers* 21, no. 14 (2021): 1–22.

Avila Pinto, Renata. "Digital Sovereignty or Digital Colonialism." *Sur: International Journal on Human Rights* 27 (2018): 15.

BaFin. "Cyber Insurance," 2022. https://www.bafin.de/EN/Verbraucher/Versicherung/Produkte/Cyber/cyberversicherung_node_en.html [accessed: 2024-04-23].

Bang, Henrik P., Richard C. Box, Anders Peter Hansen, and Jon Jay Neufeld. "The State and the Citizen: Communitarianism in the United States and Denmark." *Administrative Theory & Praxis* 22, no. 2 (June 2000): 369–90. https://doi.org/10.1080/10841806.2000.11643456.

Bartz, Diane. "Bipartisan US Lawmakers Introduce Bill Aimed at Google, Facebook Ad Clout." *Reuters*, March 2023. https://www.reuters.com/world/us/bipartisan-us-lawmakers-introduce-bill-aimed-google-facebook-ad-clout-2023-03-30/ [accessed: 2024-04-23].

Baums, Ansgar. "Digitale Standortpolitik in Der Post-Snowden-Welt." In *Digitale Souveränität*, 223–35. Springer Fachmedien Wiesbaden, 2016. https://doi.org/10.1007/978-3-658-07349-7_20.

Benhamou, Yaniv, Frédéric Bernard, and Cédric Durand. "Digital Sovereignty in Switzerland: The Laboratory of Federalism." *Risiko & Recht*, no. 1 (October 2023): 65–101. https://doi.org/10.36862/eiz-rr202301-03.

Berg, Sebastian, and Jeanette Hofmann. "Digital Democracy." *Internet Policy Review* 10, no. 4 (2021). https://doi.org/10.14763/2021.4.1612.

Betz, David J. *Cyberspace and the State: Towards a Strategy for Cyber-Power*. Routledge, 2017.

Bradford, Anu. *Digital Empires: The Global Battle to Regulate Technology*. Oxford University PressNew York, 2023. https://doi.org/10.1093/oso/9780197649268.001.0001.

Braud, Arnaud, Gael Fromentoux, Benoit Radier, and Olivier Le Grand. "The Road to European Digital Sovereignty with Gaia-X and IDSA." *IEEE Network* 35, no. 2 (March 2021): 4–5. https://doi.org/10.1109/mnet.2021.9387709.

Bremmer, Ian. *The End of the Free Market: Who Wins the War Between States and Corporations? Who Wins the War Between States and Corporations?* East Rutherford: Penguin Publishing Group, 2010. https://doi.org/10.1007/s12290-010-0129-z.

Bria, Francesca. "Public Policies for Digital Sovereignty." *Ours to Hack and to Own: The Rise of Platform Cooperativism, A New Vision for the Future of Work and a Fairer Internet*. New York/London: OR Books, no. 1a (2017): 218–22.

Brogi, Elda. "The Media Pluralism Monitor: Conceptualizing Media Pluralism for the Online Environment." *El Profesional de La Información* 29, no. 5 (November 2020). https://doi.org/10.3145/epi.2020.sep.29.

Bu, Qingxiu. "Behind the Huawei Sanction: National Security, Ideological Prejudices or Something Else?" *International Cybersecurity Law Review* 5, no. 2 (March 2024): 263–300. https://doi.org/10.1365/s43439-024-00112-6.

Calzada, Igor. "Pandemic Citizenship Amidst Stateless Algorithmic Nations: Digital Rights and Technological Sovereignty at Stake" 10 (2021). https://doi.org/10.13140/RG.2.2.36196.19849/3.

Champagne, A. "Netznutzer: Software Für Diktatoren." *Le Monde Diplomatique*, 2012.

Chander, Anupam, and Uyen P Le. "Data Nationalism." *Emory LJ* 64 (2014): 677.

Choi, Moonsun. "A Concept Analysis of Digital Citizenship for Democratic Citizenship Education in the Internet Age." *Theory & Research in Social Education* 44, no. 4 (August 2016): 565–607. https://doi.org/10.1080/00933104.2016.1210549.

Christakis, Theodore. "'European Digital Sovereignty': Successfully Navigating Between the 'Brussels Effect' and Europe's Quest for Strategic Autonomy." *SSRN Electronic Journal*, 2020. https://doi.org/10.2139/ssrn.3748098.

Claassen, Rutger. "Political Theories of the Business Corporation." *Philosophy Compass* 18, no. 1 (December 2022): e12892. https://doi.org/10.1111/phc3.12892.

Clement, Reiner, and Dirk Schreiber. *Internet-Ökonomie*. Springer Berlin Heidelberg, 2016. https://doi.org/10.1007/978-3-662-49047-1.

Conduit, Dara. "Digital Authoritarianism and the Devolution of Authoritarian Rule: Examining Syria's Patriotic Hackers." *Democratization* 31, no. 5 (March 2023): 979–97. https://doi.org/10.1080/13510347.2023.2187781.

Creemers, Rogier. "The Chinese Cyber-Sovereignty Agenda." In *Connectivity Wars: Why Migration, Finance and Trade Are the Geo-Economic Battlegrounds of the Future*. JSTOR, 2019. http://www.jstor.com/stable/resrep21667.18.

Dahlberg, Lincoln. "Cyber-Libertarianism 2.0: A Discourse Theory/Critical Political Economy Examination." *Cultural Politics* 6, no. 3 (November 2010): 331–56. https://doi.org/10.2752/175174310x12750685679753.

———. "Democracy via Cyberspace: Mapping the Rhetorics and Practices of Three Prominent Camps." *New Media & Society* 3, no. 2 (June 2001): 157–77. https://doi.org/10.1177/14614440122226038.

Dragu, Tiberiu, and Yonatan Lupu. "Digital Authoritarianism and the Future of Human Rights." *International Organization* 75, no. 4 (2021): 991–1017. https://doi.org/10.1017/s0020818320000624.

Dünkel, Heiko. "Kollektiver Rechtsschutz Bei Datenschutzrechtsverstößen: Durchsetzung Der DSGVO Durch Deutsche Verbraucherverbände." *Datenschutz Und Datensicherheit - DuD* 43, no. 8 (July 2019): 483–87. https://doi.org/10.1007/s11623-019-1148-9.

Elmimouni, Houda, Yarden Skop, Norah Abokhodair, Sarah Rüller, Konstantin Aal, Anne Weibert, Adel Al-Dawood, Volker Wulf, and Peter Tolmie. "Shielding or Silencing?: An Investigation into Content Moderation during the

Sheikh Jarrah Crisis." *Proceedings of the ACM on Human-Computer Interaction* 8, no. GROUP (February 2024): 1–21. https://doi.org/10.1145/3633071.

Farrand, Benjamin, and Helena Carrapico. "Digital Sovereignty and Taking Back Control: From Regulatory Capitalism to Regulatory Mercantilism in EU Cybersecurity." *European Security* 31, no. 3 (July 2022): 435–53. https://doi.org/10.1080/09662839.2022.2102896.

Floridi, Luciano. "The Fight for Digital Sovereignty: What It Is, and Why It Matters, Especially for the EU." *SSRN Electronic Journal* 33, no. 3 (2021): 369–78. https://doi.org/10.2139/ssrn.3827089.

Fratini, Samuele, Emmie Hine, Claudio Novelli, Huw Roberts, and Luciano Floridi. "Digital Sovereignty: A Descriptive Analysis and a Critical Evaluation of Existing Models." *Digital Society* 3, no. 3 (December 2024): 59. https://doi.org/10.1007/s44206-024-00146-7.

Freeman, Samuel. "Illiberal Libertarians: Why Libertarianism Is Not a Liberal View." *Philosophy & Public Affairs* 30, no. 2 (April 2001): 105–51. https://doi.org/10.1111/j.1088-4963.2001.00105.x.

Ghaffary, Shirin. "'Don't Be Evil' Isn't a Normal Company Value. But Google Isn't a Normal Company," 2021. https://www.vox.com/recode/2021/2/16/22280502/google-dont-be-evil-land-of-the-giants-podcast [accessed: 2024-04-23].

Gibson, J Paul, Robert Krimmer, Vanessa Teague, and Julia Pomares. "A Review of E-Voting: The Past, Present and Future." *Annals of Telecommunications* 71, no. 7–8 (June 2016): 279–86. https://doi.org/10.1007/s12243-016-0525-8.

Graham, Roderick, and Brian Pitman. "Freedom in the Wilderness: A Study of a Darknet Space." *Convergence: The International Journal of Research into New Media Technologies* 26, no. 3 (October 2018): 593–619. https://doi.org/10.1177/1354856518806636.

Griffiths, James. "The Great Firewall of China." Bloomsbury, 2021.

Grimm, Dieter. *Sovereignty: The Origin and Future of a Political and Legal Concept*. Columbia University Press, 2015. https://doi.org/10.7312/grim16424.

Grinko, Margarita, Sarvin Qalandar, Dave Randall, and Volker Wulf. "Nationalizing the Internet to Break a Protest Movement: Internet Shutdown

and Counter-Appropriation in Iran of Late 2019." *Proceedings of the ACM on Human-Computer Interaction* 6, no. CSCW2 (November 2022): 1–21. https://doi.org/10.1145/3555205.

Guggenberger, Nikolas. "Moderating Monopolies." *Berkeley Tech. LJ* 38 (2023): 119. https://doi.org/10.15779/Z389K45T9Q.

Heidebrecht, Sebastian. "From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance." *JCMS: Journal of Common Market Studies* 62, no. 1 (April 2023): 205–23. https://doi.org/10.1111/jcms.13488.

Hellmeier, Malte, and Franziska von Scherenberg. "A Delimitation of Data Sovereignty from Digital and Technological Sovereignty." In *ECIS 2023 Research Papers*, 2023. https://aisel.aisnet.org/ecis2023_rp/306/.

Hill, Jonah. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for Us Policymakers and Business Leaders." In *The Hague Institute for Global Justice, Conference on the Future of Cyber Governance*, 2014.

Himma-Kadakas, Marju, and Ragne Kõuts-Klemm. "Developing an Advanced Digital Society: An Estonian Case Study." In *Internet in the Post-Soviet Area*, 109–33. Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-32507-6_6.

Holla, Nisha. "Democratising Technology for The Next Six Billion." *Digital Debates*, 2020, 12.

Hovenkamp, Herbert. "Antitrust and Platform Monopoly." *SSRN Electronic Journal* 130 (2020): 1952. https://doi.org/10.2139/ssrn.3639142.

Ihsan, Yilmaz, and Raja Ali M. Saleem. *The Nexus of Religious Populism and Digital Authoritarianism in Pakistan*. *Populism & Politics*. European Center for Populism Studies (ECPS), 2022. https://doi.org/10.55271/pp0016.

Iwarsson, Susanne, and Agneta Ståhl. "Accessibility, Usability and Universal Design—Positioning and Definition of Concepts Describing Person-Environment Relationships." *Disability and Rehabilitation* 25, no. 2 (January 2003): 57–66. https://doi.org/10.1080/dre.25.2.57.66.

Jiménez, Aitor. "The Silicon Doctrine." *tripleC: Communication, Capitalism & Critique. Open Access Journal for a Global Sustainable Information Society* 18, no. 1 (March 2020): 322–36. https://doi.org/10.31269/triplec.v18i1.1147.

Keller, Paul. "European Public Digital Infrastructure Fund White Paper." *Open Future*, December 2022.

Keller, Reiner. *Doing Discourse Research: An Introduction for Social Scientists*. Edited by Bryan Jenner. Los Angeles, Calif. [u.a.]: SAGE, 2013.

Kellner, Douglas. "Metaphors of Cyberspace and Digital Technologies." In *Technology and Democracy: Toward A Critical Theory of Digital Technologies, Technopolitics, and Technocapitalism*, 35–66. Wiesbaden: Springer Fachmedien Wiesbaden, 2021. https://doi.org/10.1007/978-3-658-31790-4_2.

Kotka, Taavi, Carlos Vargas, and Kaspar Korjus. "Estonian E-Residency: Redefining the Nation-State in the Digital Era." *University of Oxford Cyber Studies Programme Working Paper* 3 (2015).

Kotz, David Michael. *The Rise and Fall of Neoliberal Capitalism*. Cambridge, Massachusetts: Harvard University Press, 2015. https://doi.org/10.4159/harvard.9780674735880.

Kubicek, Herbert. "E-Participation." In *E-Government*, 195–225. Springer, 2010. https://doi.org/10.1007/978-3-8349-6343-7_10.

Kubitschko, Sebastian. "The Role of Hackers in Countering Surveillance and Promoting Democracy." *Media and Communication* 3, no. 2 (September 2015): 77–87. https://doi.org/10.17645/mac.v3i2.281.

Kwet, Michael. "Digital Colonialism: US Empire and the New Imperialism in the Global South." *Race & Class* 60, no. 4 (January 2019): 3–26. https://doi.org/10.1177/0306396818823172.

Lambach, Daniel, and Linda Monsees. "Beyond Sovereignty as Authority: The Multiplicity of European Approaches to Digital Sovereignty." *Global Political Economy*, February 2024, 1–18. https://doi.org/10.1332/26352257y2024d000000007.

Lambach, Daniel, and Kai Oppermann. "Narratives of Digital Sovereignty in German Political Discourse." *Governance* 36, no. 3 (April 2022): 693–709. https://doi.org/10.1111/gove.12690.

Laudon, Jane P., and Kenneth C. Laudon. *Management Information Systems: Managing the Digital Firm*. Pearson Educacion, 2004.

Lawo, Dennis, Thomas Neifer, Margarita Esau, and Gunnar Stevens. "Buying the 'Right'Thing: Designing Food Recommender Systems with Critical Consumers." In *Proceedings of the 2021 CHI Conference on Human Factors in Computing Systems*, 1–13, 2021.

———. "Human-Centred Digital Sovereignty: Explorative Conceptual Model and Ways Forward." In *Computer-Human Interaction Research and Applications*, 84–103. Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-49368-3_6.

Lawo, Dennis, Thomas Neifer, Margarita Esau-Held, and Gunnar Stevens. "Digital Sovereignty: What It Is and Why It Matters for HCI." In *Extended Abstracts of the 2023 CHI Conference on Human Factors in Computing Systems*, 1–7. CHI '23. ACM, 2023. https://doi.org/10.1145/3544549.3585834.

Leary, Timothy. *Chaos & Cyber Culture*. Grupo Editorial Norma, 1994.

Lee, Daniel. *Popular Sovereignty in Early Modern Constitutional Thought*. Oxford Constitutional Theory Ser. Oxford: Oxford University Press USA - OSO, 2016. https://doi.org/10.1093/acprof:oso/9780198745167.001.0001.

Leistner, Matthias. "The Commission's Vision for Europe's Digital Future: Proposals for the Data Governance Act, the Digital Markets Act and the Digital Services Act—a Critical Primer." *Journal of Intellectual Property Law & Practice* 16, no. 8 (2021): 778–84.

Lessig, Lawrence. "The Zones of Cyberspace." *Stanford Law Review* 48, no. 5 (May 1996): 1403. https://doi.org/10.2307/1229391.

Levy, Steven. *Hackers: Heroes of the Computer Revolution*. Vol. 14. Anchor Press/Doubleday Garden City, NY, 1984. https://www.usenix.org/legacy/publications/login/2010-10/openpdfs/bookreviews1010.pdf.

Lucchi, Nicola. "Digital Media Pluralism." *In Transition*, n.d., 91.

Malcolm, Jeremy. *Multi-Stakeholder Governance and the Internet Governance Forum*. Perth: Terminus Press, 2008.

Malcomson, Scott. *Splinternet: How Geopolitics and Commerce Are Fragmenting the World Wide Web*. OR books, 2016.

Marechal, Nathalie. “From Russia With Crypto: A Political History of Telegram.” In *8th USENIX Workshop on Free and Open Communications on the Internet (FOCI 18)*. USENIX Association, 2018.

Maurer, Tim, Isabel Skierka, Robert Morgus, and Mirko Hohmann. “Technological Sovereignty: Missing the Point? ” In *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, 53–68. IEEE, 2015. https://doi.org/10.1109/cycon.2015.7158468.

McIntosh, Daniel. “We Need to Talk about Data: How Digital Monopolies Arise and Why They Have Power and Influence.” *Journal of Technology Law & Policy* 23, no. 2 (2018): 185.

Michaelsen, Marcus. “Exit and Voice in a Digital Age: Iran’s Exiled Activists and the Authoritarian State.” *Globalizations* 15, no. 2 (2018): 248–64.

———. “Far Away, So Close: Transnational Activism, Digital Surveillance and Authoritarian Control in Iran.” *Surveillance & Society* 15, no. 3/4 (August 2017): 465–70. https://doi.org/10.24908/ss.v15i3/4.6635.

Mises, Ludwig. *Liberalism*. Ludwig von Mises Institute, 1985.

Moerel, Lokke, and Paul Timmers. “Reflections on Digital Sovereignty.” *EU Cyber Direct, Research in Focus Series*, January 2021.

Möllers, Norma. “Making Digital Territory: Cybersecurity, Techno-Nationalism, and the Moral Boundaries of the State.” *Science, Technology, & Human Values* 46, no. 1 (January 2020): 112–38. https://doi.org/10.1177/0162243920904436.

Mori, Cristina Kiomi. “‘Digital Inclusion’: Are We All Talking about the Same Thing?” In *ICTs and Sustainable Solutions for the Digital Divide*, 45–64. IGI Global, 2011. https://doi.org/10.4018/978-1-61520-799-2.ch003.

Müller, Jane, Mareike Thumel, Katrin Potzel, and Rudolf Kammerl. “Digital Sovereignty of Adolescents.” *Medienjournal-Zeitschrift Für Medien-Und Kommunkiationsforschung* 44, no. 1 (2020): 30–40. https://doi.org/10.60764/MEDIENJOURNAL-XQK1-8C15.

Musiani, Francesca. “Infrastructuring Digital Sovereignty: A Research Agenda for an Infrastructure-Based Sociology of Digital Self-Determination Practices.” *Information, Communication & Society* 25, no. 6 (March 2022): 785–800. https://doi.org/10.1080/1369118x.2022.2049850.

Nanni, Riccardo. "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 (October 2022): 2342–62. https://doi.org/10.1080/1369118x.2022.2129270.

Nhemachena, Artwell, Nokuthula Hlabangane, and Maria B. Kaundjua. "Relationality or Hospitality in Twenty-First Century Research? Big Data, Internet of Things, and the Resilience of Coloniality on Africa." *Modern Africa: Politics, History and Society* 8, no. 1 (June 2020): 105–39. https://doi.org/10.26806/modafr.v8i1.278.

Nugraha, Yudhistira, Kautsarina, and Ashwin Sasongko Sastrosubroto. "Towards Data Sovereignty in Cyberspace." *2015 3rd International Conference on Information and Communication Technology (ICoICT)*, 2015, 465–71. https://doi.org/10.2139/ssrn.2610314.

Obendiek, Anke S. "Take Back Control? Digital Sovereignty and a Vision for Europe." Resreport. Hertie School, 2021.

Ossiannilsson, Ebba. "MOOCS for Lifelong Learning, Equity, and Liberation." In *MOOC (Massive Open Online Courses)*. IntechOpen, 2022. https://doi.org/10.5772/intechopen.99659.

Paré, Guy, Marie-Claude Trudel, Mirou Jaana, and Spyros Kitsiou. "Synthesizing Information Systems Knowledge: A Typology of Literature Reviews." *Information & Management* 52, no. 2 (March 2015): 183–99. https://doi.org/10.1016/j.im.2014.08.008.

Pohle, Julia, Thorsten Thiel, and others. "Digital Sovereignty." In *Practicing Sovereignty*, 47–68. transcript Verlag, 2021. https://doi.org/10.1515/9783839457603-003.

Polyakova, Alina, and Chris Meserole. "Exporting Digital Authoritarianism: The Russian and Chinese Models." *Policy Brief, Democracy and Disorder Series*, 2019, 1–22. https://doi.org/20.500.12592/rwbp8q.

Prem, Erich. "Principles of Digital Humanism: A Critical Post-Humanist View." *Journal of Responsible Technology* 17 (March 2024): 100075. https://doi.org/10.1016/j.jrt.2024.100075.

Priisalu, Jaan, and Rain Ottis. "Personal Control of Privacy and Data: Estonian Experience." *Health and Technology* 7, no. 4 (June 2017): 441–51. https://doi.org/10.1007/s12553-017-0195-1.

Rader, Emilee, and Rebecca Gray. "Understanding User Beliefs About Algorithmic Curation in the Facebook News Feed." In *Proceedings of the 33rd Annual ACM Conference on Human Factors in Computing Systems*, 173–82. CHI '15. Seoul Republic of Korea: ACM, 2015. https://doi.org/10.1145/2702123.2702174.

Rawls, John. *A Theory of Justice: Original Edition*. *Cambridge (Mass.)*. Harvard University Press, 1971. https://doi.org/10.4159/9780674042605.

Recki, Lena, Dennis Lawo, Veronika Krauss, and Dominik Pins. "A Qualitative Exploration of User-Perceived Risks of AI to Inform Design and Policy." In *Fröhlich, Cobus (Hg.): Mensch Und Computer 2023–Workshopband, 03.-06. September 2023, Rapperswil (SG)*. GI, 2023. https://doi.org/10.18420/MUC2023-MCI-WS16-383.

Recki, Lena, Dennis Lawo, Veronika Krauß, Dominik Pins, and Alexander Boden. "'You Can Either Blame Technology or Blame a Person...' - A Conceptual Model of Users' AI-Risk Perception as a Tool for HCI." *Proceedings of the ACM on Human-Computer Interaction* 8, no. CSCW2 (7 November 2024): 1–25. https://doi.org/10.1145/3686996.

Richter, Emanuel. "Kommunitarismus und Republikanismus." In *Handbuch Kommunitarismus*, 567–89. Springer Fachmedien Wiesbaden, 2019. https://doi.org/10.1007/978-3-658-16859-9_27.

Ringfort-Felner, Ronda, Matthias Laschke, Shadan Sadeghian, and Marc Hassenzahl. "Kiro: A Design Fiction to Explore Social Conversation with Voice Assistants." *Proceedings of the ACM on Human-Computer Interaction* 6, no. GROUP (January 2022): 1–21. https://doi.org/10.1145/3492852.

Roberts, Huw, Josh Cowls, Federico Casolari, Jessica Morley, Mariarosaria Taddeo, and Luciano Floridi. "Safeguarding European Values with Digital Sovereignty: An Analysis of Statements and Policies." *SSRN Electronic Journal*, 2021. https://doi.org/10.2139/ssrn.3937345.

Roberts, Huw, Emmie Hine, and Luciano Floridi. "Digital Sovereignty, Digital Expansionism, and the Prospects for Global AI Governance." In *Quo Vadis, Sovereignty?*, 51–75. Springer Nature Switzerland, 2023. https://doi.org/10.1007/978-3-031-41566-1_4.

Rolan, Gregory, Sue McKemmish, Gillian Oliver, Joanne Evans, and Shannon Faulkhead. "Digital Equity through Data Sovereignty: A Vision for Sustaining Humanity." *iConference 2020 Proceedings*, 2020.

Rolf, Steve, and Seth Schindler. "The US–China Rivalry and the Emergence of State Platform Capitalism." *Environment and Planning A: Economy and Space* 55, no. 5 (January 2023): 1255–80. https://doi.org/10.1177/0308518x221146545.

Rouvroy, Antoinette, and Yves Poullet. "The Right to Informational Self-Determination and the Value of Self-Development: Reassessing the Importance of Privacy for Democracy." In *Reinventing Data Protection?*, edited by Serge Gutwirth, Paul Hert, Sjaak Nouwt, Yves Poullet, and Cécile De Terwangne, 45–76. Springer eBook Collection. Dordrecht: Springer Netherlands, 2009. https://doi.org/10.1007/978-1-4020-9498-9_2.

Ruohonen, Jukka. "The Treachery of Images in the Digital Sovereignty Debate." *Minds and Machines* 31, no. 3 (July 2021): 439–56. https://doi.org/10.1007/s11023-021-09566-7.

Rushton, Michael. "Communitarianism." In *The Moral Foundations of Public Funding for the Arts*, 93–113. Cham: Springer International Publishing, 2023. https://doi.org/10.1007/978-3-031-35106-8_5.

Selzer, Jochim. "Die Rückkehr des Dezentralen: Wie Sich Internetaktive Gegen Regulierung Wehren." *Informatik Spektrum* 43, no. 3 (May 2020): 192–96. https://doi.org/10.1007/s00287-020-01273-4.

Shipman, Alan. "Privatized Production, Socialized Consumption? Old Producer Power Behind the New Consumer Sovereignty." *Review of Social Economy* 59, no. 3 (September 2001): 331–52. https://doi.org/10.1080/00346760110053932.

Shrivastava, Megha. "Emerging Dynamics Between the Chinese State and Big-Tech: The Case of Alibaba." *Strategic Analysis* 47, no. 1 (January 2023): 19–29. https://doi.org/10.1080/09700161.2023.2181424.

Siddarth, Divya, Daron Acemoglu, Danielle Allen, Kate Crawford, James Evans, Michael Jordan, and E Weyl. "How AI Fails Us." *arXiv Preprint arXiv:2201.04200*, 2021.

Solomon, Gwen. "Digital Equity: It's Not Just about Access Anymore." *Technology | Learning* 22, no. 9 (April 2002): 18–20.

Soulé, Folashadé. “Digital Sovereignty in Africa: Moving beyond Local Data Ownership,” https://www.cigionline.org/static/documents/PB_no.185.pdf, n.d.

Stadnik, Ilona. “Internet Governance in Russia–Sovereign Basics for Independent Runet.” In *TPRC47: The 47th Research Conference on Communication, Information and Internet Policy*, 2019.

Steiger, Stefan, Wolf J. Schünemann, and Katharina Dimmroth. “Outrage without Consequences? Post-Snowden Discourses and Governmental Practice in Germany.” *Media and Communication* 5, no. 1 (March 2017): 7–16. https://doi.org/10.17645/mac.v5i1.814.

Stevens, Gunnar, Alexander Boden, Fatemeh Alizadeh, Timo Jakobi, Michelle Walther, and Jana Krüger. “Wie Gehen Verbraucher:Innen Mit Onlinebetrug Um? – Eine Literaturübersicht.” In *Handbuch Cyberkriminologie 2*, edited by Thomas-Gabriel Rüdiger and P. Saskia Bayerl, 533–54. Wiesbaden: Springer Fachmedien Wiesbaden, 2023. https://doi.org/10.1007/978-3-658-35442-8_42.

Suarez-Villa, Luis. *Globalization and Technocapitalism: The Political Economy of Corporate Power and Technological Domination*. Routledge, 2016. https://doi.org/10.4324/9781315585123.

Sullivan, John L. “Free, Open Source Software Advocacy as a Social Justice Movement: The Expansion of F/OSS Movement Discourse in the 21st Century.” *Journal of Information Technology & Politics* 8, no. 3 (July 2011): 223–39. https://doi.org/10.1080/19331681.2011.592080.

Swartz, Aaron, and Lawrence Lessig. *A Web of Extended Metaphors in the Guerilla Open Access Manifesto of Aaron Swartz*. University of California, Santa Barbara, 2017. https://search.proquest.com/openview/ae4a63af9ed1cfbf50895b45dec91fbf/1?pq-origsite=gscholar&cbl=18750.

Talhouk, Reem, Ana Bustamante, Konstantin Aal, Anne Weibert, Koula Charitonos, and Vasilis Vlachokyriakos. “HCI and Refugees: Experiences and Reflections.” *Interactions* 25, no. 4 (June 2018): 46–51. https://doi.org/10.1145/3215846.

“The Best Antivirus Software for 2024,” April 2024. https://au.pcmag.com/antivirus/8949/the-best-antivirus-protection [accessed: 2024-04-23].

"The Best Services for Deleting Yourself from the Internet in 2024," 2024. https://www.zdnet.com/article/best-data-removal-services/ [accessed: 2024-04-23].

"The Case for Investing in Digital Public Infrastructure," n.d. https://hbr.org/2023/05/the-case-for-investing-in-digital-public-infrastructure.

Tretter, Max. "Sovereignty in the Digital and Contact Tracing Apps." *Digital Society* 2, no. 1 (December 2022): 2. https://doi.org/10.1007/s44206-022-00030-2.

"Unternehmen Beklagen Bürokratie Durch DSGVO," March 2024. https://www.security-insider.de/unternehmen-beklagen-buerokratie-durch-dsgvo-a-f352e3d7414efcfb862ac47e5742f49c/ [accessed: 2024-04-23].

Ventura, Patricia. *Neoliberal Culture: Living with American Neoliberalism*. Routledge, 2016.

Walther, Michelle, Timo Jakobi, Steven James Watson, and Gunnar Stevens. "A Systematic Literature Review about the Consumers' Side of Fake Review Detection – Which Cues Do Consumers Use to Determine the Veracity of Online User Reviews?" *Computers in Human Behavior Reports* 10 (May 2023): 100278. https://doi.org/10.1016/j.chbr.2023.100278.

Weibert, Anne, Konstantin Aal, David Unbehaun, and Volker Wulf. "Geteilt Vernetzt: Ausprägungen des Digital Divide unter Älteren Migrantinnen in Deutschland." *Medien & Altern* 11 (2017): 75–91.

Weibert, Anne, and Volker Wulf. "'All of a Sudden We Had This Dialogue… ': Intercultural Computer Clubs' Contribution to Sustainable Integration." In *Proceedings of the 3rd International Conference on Intercultural Collaboration*, 93–102. ICIC '10. Copenhagen Denmark: ACM, 2010. https://doi.org/10.1145/1841853.1841868.

White, Damian Finbar, and Gideon Kossoff. "Anarchism, Libertarianism and Environmentalism: Anti-Authoritarian Thought and the Search for Self-Organizing Societies." In *The SAGE Handbook of Environment and Society*, 50–65. SAGE Publications Ltd, 2007. https://doi.org/10.4135/9781848607873.n3.

Whitten, Alma, and J. Doug Tygar. "Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0." In *USENIX Security Symposium*, 348:169–84, 1999.

Widerquist, Karl. "A Dilemma for Libertarianism." *Politics, Philosophy & Economics* 8, no. 1 (February 2009): 43–72. https://doi.org/10.1177/1470594x08098871.

Wills, Garry. *A Necessary Evil: A History of American Distrust of Government*. Simon and Schuster, 2002.

Windrich, Elaine, and Louise Bourgault. "Mass Media in Sub-Saharan Africa." *African Studies Review* 39, no. 3 (December 1996): 200. https://doi.org/10.2307/524952.

Wuthnow, Robert. "Between the State and Market: Voluntarism and the Difference It Makes." *Rights and the Common Good. The Communitarian Perspective*, 1995.

Yar, Majid. "Computer Hacking: Just Another Case of Juvenile Delinquency?" *The Howard Journal of Criminal Justice* 44, no. 4 (September 2005): 387–99. https://doi.org/10.1111/j.1468-2311.2005.00383.x.

Yuming, Lian. "Digital Identity." In *Sovereignty Blockchain 2.0*, 87–125. Springer Nature Singapore, 2022. https://doi.org/10.1007/978-981-19-3862-7_3.

Zhang, Xin, and Martin Pfeiffer. "Nach dem Neoliberalismus: Staatskapitalismus in China Und Russland." *Osteuropa*, no. 5/6 (2015): 21–32.

Zuboff, Shoshana. *The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power*. Profile Books, 2019.

Zywicki, Todd J. "Libertarianism, Law and Economics, and the Common Law." *SSRN Electronic Journal* 16 (2012): 309. https://doi.org/10.2139/ssrn.2174534.