frontiers | Frontiers in Communication

TYPE Perspective
PUBLISHED 11 March 2025
DOI 10.3389/fcomm.2025.1562072

OPEN ACCESS

EDITED BY
Seamus Simpson,
University of Salford, United Kingdom

REVIEWED BY
Chedza Simon,
University of Salford, United Kingdom

*CORRESPONDENCE
Francesca Musiani
francesca.musiani@gmail.com

RECEIVED 16 January 2025
ACCEPTED 10 February 2025
PUBLISHED 11 March 2025

CITATION
Musiani F (2025) Reassessing "infrastructuring digital sovereignty": digital self-determination as a set of infrastructure-embedded practices.
Front. Commun. 10:1562072.
doi: 10.3389/fcomm.2025.1562072

Reassessing "infrastructuring digital sovereignty": digital self-determination as a set of infrastructure-embedded practices

Francesca Musiani[1,2]*

[1]CNRS Centre Internet et Société, Paris, France, [2]Centre National de la Recherche Scientifique (CNRS), Paris, France

This perspective contribution takes stock of recent research conducted through the theoretical lens, grounded in science and technology studies (STS) and more specifically infrastructure studies, which I have previously defined as "infrastructuring digital sovereignty" (Musiani, 2022). With this concept, I address "digital sovereignty" beyond its strictly legal interpretations and its rhetorical uses in political discourses by understanding it "from within" as an ongoing series of negotiations, practices, struggles, and controversies embedded in infrastructures, their creation, their development, and their maintenance. The contribution will discuss how, via two recently started projects, French and global interdisciplinary teams seek to provide an empirical and theoretical understanding, informed by the social sciences, of digital sovereignty as a set of processes and co-constructed techniques, practices, and norms "in the making."

KEYWORDS

digital sovereignty, infrastructure, digital technologies, science and technology studies (STS), internet governance, infrastructure studies

1 What is meant by "digital sovereignty"? A notion in the making

The notion of "digital sovereignty" (DS) is increasingly mobilised not only by a variety of actors to describe various forms of independence, control, and autonomy by states but also by quasi-states and even less formal political entities over digital infrastructures, technologies, and data forming the internet. This kind of claim was first made by so-called "authoritarian" regimes such as China and later Russia (Zeng et al., 2017; Litvinenko, 2021). However, various actors in liberal democracies around the world are currently also mobilising the DS concept to emphasise their aim of increasing their self-determination with regard to digital technologies and services (Floridi, 2020).

In addition, over the last decades, states have made it possible to enforce national laws and undertake governmental interventions in the digital sphere—and they have successfully convinced their citizens that sovereignty is necessary to protect "vital goods" ranging from security to prosperity, cultural norms, diversity, and media control (Heidebrecht, 2023). In many countries, citizens today expect their governments to protect these goods and their rights, for instance, by strengthening privacy online or countering online disinformation and cybercrime. As a result, the DS concept has become a powerful political discourse for the state to become once more a relevant category in the development and global governance of digital infrastructures and digital services.

The DS concept is also increasingly mobilised by "quasi-states" entities such as indigenous first nations in America and Oceania, autonomous regions such as Quebec (Canada), or even civil society collectives in order to articulate their claims for increasing people's capacity for self-determination in the digital sphere both vis-à-vis powerful economic players and dominant state actors. The DS concept is acquiring yet new facets as it is increasingly associated with pervasive technologies, from artificial intelligence to the internet of things. DS discourses are attracting increasing attention by scholars of digital governance; however, with few notable exceptions (e.g., Couture and Toupin, 2019; Pohle and Thiel, 2020), we still lack systematic assessments of DS claims and their political and technological consequences, such as the possible decentring of power hegemonies concerning the internet, as well as its increased fragmentation (Pohle and Voelsen, 2022; Perarnaud et al., 2024).

2 Flows and frontiers: towards a study of practices (and technologies) of digital sovereignty

Digital services and infrastructures play a growing role in the government of populations, with implications for issues as diverse as data management, economic competition, regulation of the public sphere, or surveillance and security. "Digital governance" is the administration and design of these technologies as an extension of internet governance (DeNardis, 2014; Radu, 2019; DeNardis et al., 2020). It involves a diversity of private and public actors as well as national and international institutions, which take part in the process of direct regulation but also technical standardisation, maintenance, and innovation. Together, these shape a digital "normative order" (Kettemann, 2020), which manifests an evolving balance of power between stakeholders.

At the dawn of the digital age, both Western democracies and socialist authoritarian states perceived emerging informatisation and digitalisation technologies as a strategic issue of national sovereignty and a "soft power" tool in the Cold War competition. For example, in the 1960s and 1970s, the French state implemented industrial strategies aimed at creating a system of European computers involving East European socialist countries and the Soviet Union in order to contest US technological hegemony, considered threat to national sovereignty (Gouarné and Kirtchik, 2022). Telecommunication networks, created during this first phase, embodied distinctive cultural visions and political projects: the DARPA by the US military (Edwards, 1996), the National Automated System of Economic Information (OGAS) in the Soviet Union (Peters, 2016), and the Minitel in France (Masutti, 2020). At the same time, the postwar decades were marked by an increasing homogenisation of techniques and the formation of global standards in telecommunication and information technologies through the activities of international bodies. Multiple programmes of technical cooperation between the capitalist West and the socialist East, driven by the need to modernise and catch up with more technologically advanced nations, contributed to their alignment with global standards (Zakharova, 2020). Since the 1990s, dominant approaches to digital governance have relied on a liberal paradigm based on notions of "free flow of information" and self-organised networks (Loveluck, 2015). Such perspectives were in line with widely shared perceptions of globalisation, which assumed a liberalisation of exchanges and declining government involvement in economic, social, and political matters (Rosenau and Czempiel, 1992).

Thus, until the past 10 years, the "digital age" was generally presented as a challenge to the nation-state (Owen, 2015). However, a reshuffling of globalisation is underway, marked by economic crises, trade wars, disruption of supply chains, environmental emergencies, political upheavals, and revived geopolitical tensions. These have led to increased competition between states and shifting balances of power. Against this background, calls for a (re)assertion of government intervention in the digital realm are increasingly been voiced.

In practice, states, governments, and intergovernmental institutions have arguably always been involved in digital governance (Goldsmith and Wu, 2006; Mueller, 2010), but in recent years, several events have pointed towards "an ongoing, state-centred battle for information resources" (Powers and Jablonski, 2015) and reassessment of the role of nation-states in digital governance (Haggart et al., 2021). A key moment was the 2013 revelations by Edward Snowden of the extent of US surveillance on communications, made possible by the dominance of US companies on digital services and infrastructures. One consequence was to accelerate data localisation initiatives, requiring "that data be physically stored within a country's jurisdiction and/or not to be transferred abroad" (Sargsyan, 2016). Since then, other events have led to revised assumptions regarding digital governance, such as global interconnectivity issues with threats of fragmentation or "splinternet" (Mueller, 2017).

From Europe, Russia, and China, competing approaches to digital governance are emerging that challenge the original model of the "Silicon Valley open internet" (O'Hara et al., 2021). Retrospectively, the global internet can be seen as a key instrument of "soft-power internationalism" (McCarthy, 2015; Baykurt, 2021) serving US hegemony. Alternatives invoke self-determination, understood as "digital sovereignty": government intervention in digital governance is expected to defend citizen and consumer interests, stimulate competitive advantages and innovation, and manage security matters and strategic issues.

Digital sovereignty is, however, a polysemic notion. As mentioned earlier on, it has been subject to radically different interpretations and has entailed contrasting regulatory, policy, and technical options (Couture and Toupin, 2019; Pohle and Thiel, 2020). It has found its footing in both authoritarian countries and liberal democracies, and it often involves a defensive position vis-à-vis the US model—where such initiatives are often seen as "digital protectionism" (Aaronson, 2019). However, the US itself is currently the target of state-backed "data trafficking" (Kokas, 2022), has adopted protective measures in the face of growing Chinese digital power, e.g., banning Huawei from the 5G market (Moore, 2022), and is massively subsidising domestic research and manufacturing of semiconductors through the CHIPS and Sciences Act passed in 2022. Assertions of digital sovereignty can also provide a convenient justification for increased centralised control over domestic digital infrastructures as well as restrictions on foreign investment. Before waging war against Ukraine, Russia sustained a long-term effort to establish a "sovereign internet" (Musiani et al., 2019; Litvinenko, 2021), whereas China built a controlled digital space from the outset (Arsène, 2019).

Alternative claims to digital sovereignty have also been made, which are not based on territorial borders and state power but insist that self-determination must be firmly seated with users and civil society (Haché, 2018). Some of these approaches define

self-determination on an infrastructural level and stipulate dependencies between the architecture and design of digital platforms and the models of data sovereignty that they produce (Ermoshina et al., 2022). For instance, in the current context of the crisis of trust towards centralised social media (such as X, formerly Twitter), advocates of decentralisation (both technical and social) have spurred growing interest in the so-called "fediverse" (with Mastodon as its main project): self-hosted, open source, and federated ecosystems are promoted as an alternative both to proprietary US-based networks and state-controlled solutions. Open-source technologies are also at the heart of state-driven digital sovereignty projects developed in Europe (where Mastodon is actively used by public administrations), Russia (with its nation-level OS Astra Linux), and China (moving away from Microsoft in favour of Kylin Linux).

Several public and private actors have been key promoters of digital sovereignty, with different strategies and discourses. Russia and China have been presented as endorsing "illiberal" norms of digital content control (Flonk, 2021), whereas the EU may be seen as defending a form of "digital constitutionalism" (De Gregorio, 2022)—often in tension with member states' national security objectives. Indeed, the EU, through initiatives such as the GDPR (General Data Protection Regulation, 2016), the recent DSA and DMA (Digital Services Act and Digital Markets Act, 2023), and the very recent Artificial Intelligence Act (2024), has favoured a regulatory response whilst its industrial strategy and incentives seem unable to foster regional champions and technical solutions on the scale of the United States and China. On the other hand, since the 2000s, the design and administration of internet technology and related policymaking have been amongst the key domains where China and Russia have asserted their national brands and influence.

Indeed, the Chinese and Russian governments have co-advanced the narrative of "internet sovereignty" in opposition to the perceived technological and governance hegemony of the United States. Baidu, Alibaba, and Tencent of China and Yandex and VKontakte of Russia have been integral to the internet strategy of their countries. China and Russia have forged a public-private relationship with respective digital media champions in the context of building and branding an internet sovereignty agenda (Budnitsky and Jia, 2018), which is actively promoted as a wider model throughout the world. In the 2010s, China dramatically increased participation in global internet governance institutions (Arsène, 2021) and its promotion of digital norms in third-party countries (Erie and Streinz, 2021). The features of digital authoritarianism in Russia (Daucé et al., 2023), which emerged throughout the 2010s and culminated in the massive war against Ukraine in February 2022, are embedded in codes, knowledge, and infrastructures (Daucé and Musiani, 2021; Ermoshina et al., 2022). Since 2014 and the annexation of Crimea, and more clearly since February 2022, Russia's military aggression against Ukraine has led to a breakdown in cooperation and links with the EU, but other flows remain, notably with China, as Russia has pivoted to the East (Lupion, 2021). On the eastern borders of Russia, especially in Central Asia, exchanges are being recomposed to bypass political barriers created by the war. Ukraine, on the contrary, tries to move westwards, strengthening its digital cooperation with the EU. Looking closer at the circulation of technical norms and policy solutions, however, complicates the picture and shows how the European, Russian, and Chinese models can be permeable to each other's features.

Different actors sometimes share perspectives and policies, and points of convergence have already been noted, e.g., between China and the EU regarding anti-monopoly actions (Wang and Gray, 2022). Even in the case of Chinese behemoths, the money funding innovations often come from highly globalised actors (Jia and Winseck, 2018). Moreover, in the context of combined political, economic, and health crises, some features of the Russian and Chinese models are increasingly finding currency not only in autocracies and populist regimes but also within democracies, including in Europe. Democratic governments are interested in intrusive surveillance solutions, from facial recognition to credit scoring (Tréguer, 2021; Greitens, 2020; Werbach, 2022). Conversely, the contribution of Western tech companies to the development of authoritarian systems is well documented (Tesquet, 2020). In a context of open confrontation, practices of mimicry paradoxically develop, contributing to the circulation of oppressive practices justified by the opponent's action.

The question of the circulation of norms and practices of internet sovereignty requires considering it from different angles and enriching models based on US and European prisms. The issue of circulating digital regulations and technological solutions is particularly salient between China and Russia and is played out on different scales and in different international arenas. Indeed, Chinese and Russian norms in terms of infrastructural components are finding their way to various regions, including countries in Central Asia, Southeast Asia, and Africa.

3 DIGISOV and ClaimSov, two nascent projects

Starting in 2024 and until 2028, two research projects co-led by Centre Internet et Société, my research unit, will investigate digital sovereignty, adopting this focus based on practices and the technologies supporting them.

The first one, DIGISOV [2024–2027, *Digital Governance and Sovereignty in a Fractured World: Competing States and Circulating Norms*, funded by the French National Agency for Research (*Agence Nationale de la Recherche*, ANR), https://digisov.org] aims at moving beyond strictly legal interpretations of digital sovereignty and its rhetorical uses in political discourses by understanding it "from within" as an ongoing series of negotiations, practices, struggles, and controversies. It thus aims to provide a better empirical and theoretical understanding, informed by the social sciences, of the production and circulation of digital norms, as well as a more thorough appreciation of state involvement in shaping these norms. Our main hypothesis is that national and regional institutions are not only increasingly involved in regulating existing digital services and infrastructures but also seek to promote specific models for the digital environment. This reflects a dynamic process of competition as well as imitation between different political regimes, which we intend to document and analyse. The project focusses on three key regions and countries: Europe, China, and Russia. It aims to show how these digital models and norms are constructed and maintained in distinct contexts, investigate the role and leverage power of the different actors involved, and trace how policy initiatives, regulatory frameworks, technical infrastructures, and discourses and practices circulate between national and regional entities.

The project seeks to rely on both legal and political sociology, STS perspectives, and discourse analysis to examine the co-development of the material, institutional, and territorial components of digital sovereignty. We propose to approach digital sovereignty as a process, a set of co-constructed techniques, practices, and norms "in the making."

The second one, ClaimSov [2025–2028, *(Re-)claiming digital sovereignty in discourse, policy, and practice*, funded by the Open Research Area 8 call], considers that DS claims, policies, and practices are key expressions of shifting power relations in a world marked by digital interconnectedness and (geo)political tensions. Thus, the scientific objective of this project was to better understand these shifting relations by developing a nuanced and empirically grounded understanding of contemporary discourses and governance mechanisms (policies, regulations, practices, and infrastructures) related to DS in various political contexts and by proposing a categorisation and conceptualisation of such discourses and mechanisms.

As with the previous one, the project seeks to have an important interdisciplinary component, building on science and technology studies, communication studies, and digital governance studies. We seek to provide systematic theoretical and empirical research on DS-related discourses and governance mechanisms in national and supranational contexts pertaining to three key geopolitical blocks: (1) the European Union, both at the EU level and within France and Germany, (2) North America (with a focus on the United States and Canada), and (3) Russia and China as the two most prominent countries run by authoritarian regimes that present DS as a cornerstone of their foreign policy.

Overall, we aim for the project to provide a baseline of empirical data to assess, contextualise, and categorise how DS is enforced and practised in different contexts and countries around the world. Our findings will contribute to empirically grounded policy discussions about possible risks and hopes attached to DS initiatives as they relate to internet governance, digital democracy, and the construction of a global digital public space—or its increased fragmentation. Therefore, we aim for the findings of the project to be of great practical relevance, as they can contribute to a more robust knowledge base for policy debates and actions worldwide.

4 Looking into the "infrastructuring" of digital sovereignty: exemplars of case studies

In 2022, I published in Information, Communication, and Society the article "Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices." With this article, I suggested a roadmap for how the concept of digital sovereignty could be studied via the infrastructure-embedded "situated practices" of various political and economic projects that aim to establish autonomous digital infrastructures in a hyperconnected world (Musiani, 2022). With both projects, I now have the possibility to put to the test the research agenda outlined in this article.

Indeed, both DIGISOV and ClaimSov projects include work packages that are focussed on the exploration of practices related to the governance of/by infrastructure, e.g., modifications made to, and co-optations of, digital infrastructures for political objectives related to self-determination and digital sovereignty. We aim to examine how technical development is enacted at different infrastructural levels, how it intersects with industrial/economic (as well as regulatory) practices, and how it is affected by them. This involves a gathering of in-depth accounts of concrete practices and arrangements related to the processes of "infrastructuring" of digital sovereignty to account for (a) how technical infrastructures and architectures are developed and deployed and (b) how economic and industrial policies are drafted, implemented, and adapted to politico-economic realities.

Potential avenues for fieldwork that we have started to explore include at the level of the EU, the European "sovereign cloud" initiative GAIA-X and its alternatives (e.g., Euclidia) and the DNS4EU initiative that has, for a time, aimed to support the development of a European DNS resolver. At these different levels, controversies abound. GAIA-X is under scrutiny for its inability to move beyond the "concept" stage, the bureaucracy of its procedures, and its governance gaps. Indeed, key European actors such as Thalès have recently fallen back on partnerships with Silicon Valley "giants," such as Google (S3NS) and Microsoft Azure (for key management solutions). DNS4EU is criticised for the potentially excessive concentration of core Internet management functions that it would entail whilst claiming better cybersecurity and smoother enforcement of content regulation measures. These two projects (and their shortcomings) provide an opportunity to observe how the different normative levels at which the EU attempts to build/strengthen its digital sovereignty (physical/software infrastructure, data protection law, and market/fair competition law) interact and what are the actual "contact points" between these different levels.

Another arena that has been singled out for fieldwork is Chinese interventionism in the digital sector—by regulating heavily, picking winners, and subsidising them massively—which has served as a model for some and a "wakeup call" for many. Beijing takes the digital industry and digital economy as a key multiplier of economic development and state control over society. Digital infrastructure and data management have also been a high priority on the international stage by promoting digitisation in bilateral development projects as well as multilateral institutions, in which Chinese providers play a key role and could find themselves in a position to challenge US control over information flows and exercise surveillance. Furthermore, the United States-China geopolitical rivalry is leading to important reconfigurations of industry policies in Europe, China, and third-party countries (with high-stakes regulation measures such as investment screening, subsidies, and relocalisation), with potential controversies burgeoning around the role of sovereignty and human rights in these policies. Country-specific case studies such as Kenya, Vietnam, and Singapore reveal the ripple effects of such global reconfiguration under the impact of the Belt and Road Initiative, the Digital Silk Road, and the EU's Global Gateway project, all of which have ambitions to build key connectivity infrastructures. European industrial policies, on the other hand, are aimed at positioning European firms in this global competition, fostering, in particular, the exportation of European surveillance infrastructures in the Global South—Safe City projects, biometric identification, and equipment interference ("hacking") tools.

The dynamics surrounding international sanctions, exemplified by the responses to Russia's invasion of Ukraine in a more general

context of "sovereignisation" of the Russian Internet, also have an important focus on infrastructures, such as traffic routing, and on the export of Russian-made middleboxes and software for traffic interception and filtering. In a context marked by the withdrawal of major international suppliers of infrastructure, devices, and software, our research focusses on the infrastructural difficulties posed by the abrupt withdrawal of international actors after the Russian aggression against Ukraine but also on the reorientation of supplies and circumvention of sanctions taking place in the digital industry.

5 Conclusion and overture

The notion of "digital sovereignty" is increasingly mobilised by a variety of actors to refer to an increasingly central set of issues in both the practice of and the research exploring Internet governance. At the same time, the contours and definitions of this notion have never been more open to debate. Thus, there is a need to place a detailed analytical focus on the practices related to the governance of/by infrastructure, e.g., modifications made to, and co-optations of, digital infrastructures for political objectives related to self-determination. This short "perspective" article has sought to assess the state of the "infrastructuring digital sovereignty" approach 3 years after this research agenda was outlined and examined some concrete avenues for developing this approach through fieldwork—with the double aim of categorising the complexity of discourses and governance mechanisms surrounding digital sovereignty and understanding their "situatedness" in different political and societal contexts.

Data availability statement

The original contributions presented in the study are included in the article/supplementary material, further inquiries can be directed to the corresponding author.

Author contributions

FM: Conceptualization, Funding acquisition, Investigation, Methodology, Project administration, Writing – original draft, Writing – review & editing.

Funding

The author(s) declare that financial support was received for the research, authorship, and/or publication of this article. This research has received funding from the Project Digital Governance and Sovereignty in a Fractured World: Competing States and Circulating Norms (DIGISOV), funded by Agence Nationale de la Recherche as part of the 2023 General Call for Projects, Grant No. ANR-23-CE53-0009-02.

Conflict of interest

The author declares that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The authors declare that no Gen AI was used in the creation of this manuscript.

Publisher's note

References

Aaronson, S. A. (2019). What are we talking about when we talk about digital protectionism? *World Trade Rev.* 18, 541–577. doi: 10.1017/S1474745618000198

Arsène, S. (2019). "La Chine et le contrôle d'internet: une cybersouveraineté ambivalente" in Annuaire Français de Relations Internationales (Paris: Thucydides Center).

Arsène, S. (2021). "China, information technology, and global freedom of expression. A story of sovereignty and global capitalism" in Regardless of frontiers: global freedom of expression in a troubled world. eds. A. Callamard and L. C. Bollinger (New York: Columbia University Press), 288–308.

Artificial Intelligence Act. (2024). Regulation (EU) 2024/1689 of the European Parliament and of the Council of 13 June 2024 laying down harmonised rules on artificial intelligence and amending Regulations (EC) No 300/2008, (EU) No 167/2013, (EU) No 168/2013, (EU) 2018/858, (EU) 2018/1139 and (EU) 2019/2144 and Directives 2014/90/EU, (EU) 2016/797 and (EU) 2020/1828 (Artificial Intelligence Act). Available at: https://eur-lex.europa.eu/eli/reg/2024/1689/oj/eng

Baykurt, B. (2021). Circulating liberalism: the global internet and soft-power internationalism. B. Baykurt and GraziaV. de. Soft-power internationalism: competing for cultural influence in the 21st-century global order. Columbia University Press: New York. 60–80

Budnitsky, S., and Jia, L. (2018). Branding internet sovereignty: digital media and the Chinese-Russian cyberalliance. *Eur. J. Cult. Stud.* 21, 594–613. doi: 10.1177/1367549417751151

Couture, S., and Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media Soc.* 21, 2305–2322. doi: 10.1177/14614448198 65984

Daucé, F., Loveluck, B., and Musiani, F. (2023). Genèse d'un autoritarisme numérique. Répression et résistance sur Internet en Russie, 2012–2022. Paris: Presses des Mines.

Daucé, F., and Musiani, F. (2021). Infrastructure-embedded control, circumvention and sovereignty in the Russian Internet: an introduction. *First Monday* 26. doi: 10.5210/fm.v26i5.11685

De Gregorio, G. (2022). Digital constitutionalism in Europe: reframing rights and powers in the algorithmic society. Cambridge: Cambridge University Press.

DeNardis, L. (2014). The global war for internet governance. New Haven, CT: Yale University Press.

DeNardis, L., Cogburn, D., Levinson, N. S., and Musiani, F. (Eds.) (2020). Researching internet governance: methods, frameworks, futures. Cambridge, MA: MIT Press.

Digital Services Act and Digital Markets Act. (2023). Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market For Digital Services and amending Directive 2000/31/EC (Digital Services Act). Available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R2065

Edwards, P. N. (1996). The closed world: computers and the politics of discourse in Cold War America. Cambridge, MA: MIT Press.

Erie, M. S., and Streinz, T. (2021). The Beijing effect: China's digital silk road as transnational data governance. New York Univ. J. Int. Law Polit. 54. Available at: https://ssrn.com/abstract=3810256

Ermoshina, K., Loveluck, B., and Musiani, F. (2022). A market of black boxes: the political economy of internet surveillance and censorship in Russia. *J. Inform. Tech. Polit.* 19, 18–33. doi: 10.1080/19331681.2021.1905972

Flonk, D. (2021). Emerging illiberal norms: Russia and China as promoters of internet content control. *Int. Aff.* 97, 1925–1944. doi: 10.1093/ia/iiab146

Floridi, L. (2020). The fight for digital sovereignty: what it is, and why it matters, especially for the EU. *Philos. Technol.* 33, 369–378. doi: 10.1007/s13347-020-00423-6

General Data Protection Regulation. (2016). Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available at: https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Goldsmith, J. L., and Wu, T. (2006). Who controls the Internet?: Illusions of a borderless world. Oxford: Oxford University Press.

Gouarné, I., and Kirtchik, O. (2022). Computers for the planned economy: Franco-Soviet scientific-technical cooperation during the cold war. *Eur. Asia Stud.* 74, 545–568. doi: 10.1080/09668136.2021.2016632

Greitens, S. C. (2020). Dealing with demand for China's global surveillance exports: Brookings report. Washington, DC: Brookings.

Haché, A. (Ed.) (2018). La Souveraineté technologique. Paris: Réseau Ritimo.

Haggart, B., Tusikov, N., and Scholte, J. A. (2021). Power and authority in Internet Governance: The return of the state? London: Routledge.

Heidebrecht, S. (2023). From market liberalism to public intervention: digital sovereignty and changing European Union digital single market governance. *J. Common Mark. Stud.* 62, 205–223. doi: 10.1111/jcms.13488

Jia, L., and Winseck, D. (2018). The political economy of Chinese internet companies: financialization, concentration, and capitalization. *Int. Commun. Gaz.* 80, 30–59. doi: 10.1177/1748048517742783

Kettemann, M. C. (2020). The normative order of the internet: a theory of rule and regulation online. Oxford: Oxford University Press.

Kokas, A. (2022). Trafficking data: How China is winning the battle for digital sovereignty. Oxford: Oxford University Press.

Litvinenko, A. (2021). Re-defining borders online: Russia's strategic narrative on internet sovereignty. *Media Commun.* 9, 5–15. doi: 10.17645/mac.v9i4.4292

Loveluck, B. (2015). Réseaux, libertés et contrôle. Une généalogie politique d'internet. Paris: Armand Colin.

Lupion, M. (2021). "Sino-Russian advocacy for "internet sovereignty" and state-led internet governance" in Digital silk road in central Asia. eds. N. Kassenova and B. Duprey (Cambridge, MA: Davis Center for Russian and Eurasian Studies).

Masutti, C. (2020). Affaires Privées. Caen: C & F Éditions.

McCarthy, D. R. (Ed.) (2015). Power, information technology, and international relations theory: the power and politics of US foreign policy and the internet. London: Palgrave Macmillan.

Moore, G. J. (2022). Huawei, cyber-sovereignty and liberal norms: China's challenge to the west/democracies. *J. Chin. Polit. Sci.* 28, 151–167. doi: 10.1007/s11366-022-09814-2

Mueller, M. (2010). Networks and states: the global politics of internet governance. Cambridge, MA: MIT Press.

Mueller, M. (2017). Will the internet fragment? Sovereignty, globalization, and cyberspace. Hoboken, NJ: John Wiley & Sons.

Musiani, F. (2022). Infrastructuring digital sovereignty: a research agenda for an infrastructure-based sociology of digital self-determination practices. *Inf. Commun. Soc.* 25, 785–800. doi: 10.1080/1369118X.2022.2049850

Musiani, F., Loveluck, B., Daucé, F., and Ermoshina, K. (2019). 'Digital sovereignty': can Russia cut off its internet from the rest of the world? Melbourne, VIC: The Conversation.

O'Hara, K., Hall, W., and Cerf, V. (2021). Four internets: data, geopolitics, and the governance of cyberspace. Oxford: Oxford University Press.

Owen, T. (2015). Disruptive power: the crisis of the state in the digital age. Oxford: Oxford University Press.

Perarnaud, C., Rossi, J., Musiani, F., and Castex, L. (2024). L'avenir d'Internet: unité ou fragmentation? Bordeaux: Le Bord de l'Eau.

Peters, B. (2016). How not to network a nation: the uneasy history of the soviet internet. Cambridge, MA: MIT Press.

Pohle, J., and Thiel, T. (2020). Digital sovereignty. *Internet Policy Rev.* 9. doi: 10.14763/2020.4.1532

Pohle, J., and Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the internet and the global digital order. *Policy Internet* 14, 13–27. doi: 10.1002/poi3.296

Powers, S. M., and Jablonski, M. (2015). The real cyber war: the political economy of internet freedom. Champaign, IL: University of Illinois Press.

Radu, R. (2019). Negotiating internet governance. Oxford: Oxford University Press.

Rosenau, J. N., and Czempiel, E.-O. (Eds.) (1992). Governance without government: order and change in world politics. Cambridge: Cambridge University Press.

Sargsyan, T. (2016). Data localization and the role of infrastructure for surveillance, privacy, and security. *Int. J. Commun.* 10, 2221–2237.

Tesquet, O. (2020). À la trace. Enquête sur les nouveaux territoires de la surveillance. Paris: Premier Parallèle.

Tréguer, F. (2021). The virus of surveillance: how the COVID-19 pandemic is fuelling technologies of control. *Polit. Anthropol. Res. Int. Soc. Sci.* 2, 16–46. doi: 10.1163/25903276-bja10018

Wang, Y., and Gray, J. E. (2022). China's evolving stance against tech monopolies: a moment of international alignment in an era of digital sovereignty. *Media Int. Aust.* 185, 79–92. doi: 10.1177/1329878X221105124

Werbach, K. (2022). Orwell that ends well? Social credit as regulation for the algorithmic age. *Univ. Ill. Law Rev.* 2022:1417. doi: 10.2139/ssrn.3589804

Zakharova, L. (2020). De Moscou aux terres les plus lointaines. Communications, politique et société en URSS. Paris: EHESS.

Zeng, J., Stevens, T., and Chen, Y. (2017). China's solution to global cyber governance: unpacking the domestic discourse of "internet sovereignty". *Policy Polit.* 45, 432–464. doi: 10.1111/polp.12202