https://ejournal-nawalaedu.com/index.php/SG/index
Volume 3 Nomor 1, 2026
E-ISSN : 3047-9339
https://doi.org/10.62872/c2rjcb45

Digital Sovereignty in International Relations: The Contest for Data Control in Global Politics

Submitted: May 02, 2026; Revised: May 20. 2026; Accepted: May 30, 2026

Aan Herdiana
Universitas Peradaban, Indonesia
aan.herdian89@gmail.com

Abstrak
Kedaulatan digital telah muncul sebagai salah satu isu paling kontroversial dalam hubungan internasional kontemporer, mencerminkan persaingan geopolitik baru yang berpusat pada kendali atas data, infrastruktur teknologi, dan ruang siber. Artikel ini mengkaji konsep kedaulatan digital melalui perspektif ilmu hubungan internasional, menganalisis bagaimana negara-negara besar, khususnya Amerika Serikat, Uni Eropa, Tiongkok, dan aktor-aktor negara berkembang, mengonstruksi dan mempertandingkan klaim kedaulatan digital dalam arena global. Melalui tinjauan sistematis terhadap 20 artikel jurnal bereputasi (2021–2024), penelitian ini mengidentifikasi tiga dimensi utama: (1) kontestasi normatif dalam pendefinisian kedaulatan digital; (2) regulasi data sebagai instrumen kekuasaan geopolitik; dan (3) fragmentasi internet (splinternet) sebagai konsekuensi persaingan kedaulatan digital. Temuan menunjukkan bahwa kedaulatan digital bukan sekadar retorika kebijakan, melainkan medan pertarungan nyata antara kepentingan keamanan nasional, dominasi teknologi korporasi, dan hak-hak digital warga negara.
Kata Kunci: kedaulatan digital; data; geopolitik; hubungan internasional; regulasi siber.

Abstract
Digital sovereignty has emerged as one of the most contested issues in contemporary international relations, reflecting a new geopolitical competition centered on the control of data, technological infrastructure, and cyberspace. This article examines the concept of digital sovereignty through the lens of international relations theory, analyzing how major actors, particularly the United States, the European Union, China, and emerging economies, construct and contest claims of digital sovereignty in the global arena. Through a systematic review of 20 peer-reviewed journal articles (2021–2024), this study identifies three principal dimensions: (1) normative contestation in the definition of digital sovereignty; (2) data regulation as an instrument of geopolitical power; and (3) internet fragmentation (splinternet) as a consequence of competing sovereignty claims. The findings demonstrate that digital sovereignty is not merely policy rhetoric but a genuine arena of contestation between national security interests, corporate technological dominance, and citizens' digital rights.
Keywords: digital sovereignty; data; geopolitics; international relations; cyber regulation

INTRODUCTION

The governance of cyberspace has become one of the most consequential arenas of twenty-first-century international politics. What was once conceived as a borderless, decentralized global commons has increasingly become a site of fierce interstate competition, regulatory fragmentation, and geopolitical projection. At the heart of this transformation lies the concept of digital sovereignty, the assertion by states, regional blocs, and increasingly non-state actors that they possess rightful authority over data flows, digital infrastructure, and the technological systems that mediate social, economic, and political life (Hummel et al., 2021; Liu, 2021).

The salience of digital sovereignty has intensified dramatically in the decade since the Snowden revelations exposed the scope of extraterritorial surveillance by major intelligence agencies, accelerating demands from governments worldwide for greater control over their national data environments. These demands have converged with the extraordinary concentration of technological power in a small number of United States-headquartered platform corporations, like Google, Amazon, Meta, Apple, Microsoft, whose data infrastructure spans continents and whose algorithmic governance shapes information environments across the globe (Gu, 2023; Nost & Goldstein, 2021). For many states, particularly in the Global South, the aspiration to digital sovereignty reflects anxieties not only about foreign state surveillance, but about structural dependencies on foreign corporate infrastructure that are perceived to compromise national autonomy in the information age.

The European Union has emerged as the most institutionally sophisticated actor in the field of digital sovereignty, enacting landmark regulatory frameworks including the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), the Digital Markets Act (DMA), and pursuing the Gaia-X cloud initiative as a European alternative to US and Chinese cloud dominance (Roberts et al., 2021; Adler-Nissen & Eggeling, 2024). Yet the EU's digital sovereignty project is internally contested, with critical scholarship questioning whether European digital sovereignty reproduces the exclusionary logics of state sovereignty or constitutes a genuinely progressive model of rights-based digital governance (Calderaro & Blumfelde, 2022; Falkner et al., 2024).

China presents a contrasting model, one in which digital sovereignty is articulated as the inalienable right of states to govern their national cyberspace according to domestic law and values, operationalized through the Great Firewall, platform nationalism, and an assertive data localization regime. Liu (2021) characterizes China's approach as "data politics", the systematic deployment of data governance as an instrument of both domestic political control and international influence, most visibly through the Digital Silk Road component of the Belt and Road Initiative. The competition between the US liberal-market model, the EU rights-based regulatory model, and the Chinese state-sovereignty model has created what many scholars now describe as a "splinternet", a fragmented global information environment organized around competing geopolitical blocs (Glasze et al., 2022; Monsees & Lambach, 2022).

Research on digital sovereignty has proliferated rapidly since 2020, yet the field remains fragmented across disciplinary silos, political science, law, information systems, and geography, with insufficient synthesis across these perspectives. This article addresses that gap by conducting a systematic review of 20 recent peer-reviewed studies to construct an integrative account of digital sovereignty as a contested phenomenon in international relations. The review asks: How is digital sovereignty conceptualized across the literature? What geopolitical dynamics structure its contestation? And what are the implications for international order in the digital age? The paper contributes to the emerging field of digital geopolitics by providing an analytical framework that integrates normative, regulatory, and infrastructural dimensions of the digital sovereignty contest.

METHODOLOGY

This study employs a systematic literature review (SLR) methodology, following PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) guidelines, adapted for interpretive social science research. The aim of the review is to synthesize empirical and theoretical scholarship on digital sovereignty in international relations published between 2021 and 2024, ensuring currency and relevance to the rapidly evolving policy and geopolitical context.

Searches were conducted across Scopus, Web of Science, and Google Scholar using keyword strings including "digital sovereignty," "data sovereignty," "internet governance," "cyber geopolitics," "data localization," "splinternet," "EU digital sovereignty," "platform governance," and "technology sovereignty." Initial searches returned 287 records. After deduplication and screening of titles and abstracts, 67 articles were selected for full-text review. Application of inclusion criteria, peer-reviewed articles in indexed journals, empirical or theoretical studies with substantive engagement with digital sovereignty in international or comparative perspective, published 2021–2024, yielded a final corpus of 20 articles for detailed synthesis.

Qualitative data extraction was conducted using a structured coding scheme comprising: (1) theoretical framework (realism, liberalism, constructivism, critical IR, political economy); (2) geographic focus and actor(s) examined; (3) primary conceptualization of digital sovereignty; (4) key mechanisms and dynamics analyzed; (5) normative position (critical, affirmative, neutral); and (6) key findings and implications. Thematic synthesis organized findings into three overarching analytical clusters: conceptual contestation, geopolitical dynamics, and governance implications. Data extraction and coding were conducted iteratively with inter-coder reliability checks applied to a 20% subsample

Table 1. Summary of Selected Studies on Digital Sovereignty in International Relations

Author / Year	Geographic Focus	Core Argument	Theoretical Lens	Journal
Liu (2021)	China / Global	Data politics as China's instrument of domestic control and global influence	Realism / Political Economy	Stud. Comp. Intl. Dev.
Hummel et al. (2021)	Global (review)	Data sovereignty as a multi-dimensional concept spanning legal, political and technical domains	Critical / Constructivist	Big Data & Society
Gu (2023)	China / Global	Big Tech reshapes sovereignty norms; states must reclaim regulatory authority over data	Realism / Regulatory Theory	J. Chinese Pol. Sci.
Glasze et al. (2022)	Global / Comparative	Digital sovereignty is spatially contested; different actors project divergent territorial imaginaries	Critical Geopolitics	Geopolitics
Falkner et al. (2024)	European Union	EU digital sovereignty discourse diverges significantly from policy reality	Liberal Institutionalism	J. European Pub. Policy

Author / Year	Geographic Focus	Core Argument	Theoretical Lens	Journal
Bellanova et al. (2022)	European Union	Digital sovereignty reframes EU security integration but introduces new tensions	Constructivism	European Security
Calderaro & Blumfelde (2022)	European Union / AI	AI-driven digital sovereignty is a false promise; structural dependencies persist	Critical IR	European Security
Broeders et al. (2023)	European Union	Normative Power Europe narrative drives but also limits EU digital sovereignty ambitions	Normative Power Theory	JCMS
Lambach & Oppermann (2022)	Germany	Digital sovereignty discourse in Germany reflects contested national identity narratives	Discourse Analysis	Governance
Farrand & Carrapico (2022)	European Union	EU cybersecurity reflects shift from regulatory capitalism to regulatory mercantilism	Political Economy	European Security
Monsees & Lambach (2022)	European Union	Digital sovereignty reproduces European identity while obscuring its exclusionary dimensions	Poststructuralism	European Security
Roberts et al. (2021)	European Union	EU digital sovereignty policies attempt to operationalize European values in cyberspace	Liberal / Normative	Internet Policy Rev.
Adler-Nissen & Eggeling (2024)	EU / Gaia-X	Gaia-X is a discursive battleground between security, economy and rights framings	Discourse Theory	JCMS
Tan et al. (2023)	Global (technical)	Digital sovereignty requires layered identity frameworks spanning digitization and digitalization	Systems / Technical	ACM Computing Surveys
Heidebrecht (2023)	European Union	EU digital single market has shifted from market liberalism toward public intervention	Regulatory Theory	JCMS
Von Scherenberg et al. (2024)	Global / Technical	Data sovereignty in information systems requires new architectural and governance standards	Information Systems	Electronic Markets

Author / Year	Geographic Focus	Core Argument	Theoretical Lens	Journal
Möller et al. (2024)	Global / Industrial	Industrial data ecosystems and data spaces operationalize sovereignty at sectoral level	Information Systems	Electronic Markets
Nost & Goldstein (2021)	Global	Political ecology framework reveals power relations embedded in data infrastructure	Critical Political Ecology	Env. & Planning E
Edler et al. (2023)	Global / Policy	Technology sovereignty as an emerging innovation policy frame with distinct rationales	Innovation Policy	Research Policy
Mügge (2024)	European Union / AI	EU AI sovereignty serves primarily corporate and regulatory elite interests	Critical Political Economy	J. European Pub. Policy

***Source**: Authors' systematic review of literature (2021–2024)*

RESULTS AND DISCUSSION

The synthesis of 20 peer-reviewed studies reveals a richly contested and rapidly evolving scholarly landscape around digital sovereignty. Three overarching thematic clusters emerged from the analysis: (1) conceptual contestation in the definition and normative framing of digital sovereignty; (2) geopolitical dynamics of the contest for data control; and (3) governance implications and emerging institutional responses. Each cluster is examined in turn below.

A. Conceptual Contestation: Defining Digital Sovereignty

The most fundamental finding of this review is that "digital sovereignty" is not a stable, agreed-upon concept but a contested signifier whose meaning varies substantially across geopolitical contexts, theoretical traditions, and policy arenas. Hummel et al. (2021) provide the most comprehensive conceptual mapping, identifying at least four distinct registers of data/digital sovereignty: legal-jurisdictional (state authority over data within territorial borders), individual-rights (persons' control over their own data), indigenous/collective (community authority over data generated within marginalized communities), and technical-infrastructural (control over the hardware, software, and protocols of digital infrastructure). The diversity of these registers reflects the fact that "digital sovereignty" has been mobilized by actors with fundamentally different interests and ideological commitments.

Glasze et al. (2022) approach this conceptual diversity through the lens of critical geopolitics, arguing that competing claims to digital sovereignty are best understood as contested "spatial imaginaries"—discursive constructions of the proper relationship between political authority and digital space. Their comparative analysis of French, German, and European digital sovereignty discourses finds that each constructs a distinctive spatial imaginary: France emphasizes national technological capability and industrial policy; Germany foregrounds data protection rights and the limits of corporate surveillance; and the EU level constructs a "European digital space" positioned as a third way between US platform capitalism and Chinese state authoritarianism. These diverging imaginaries produce policy tensions within the EU itself, complicating the aspiration to unified European digital sovereignty.

The question of whether digital sovereignty is genuine policy achievement or sophisticated rhetoric is addressed directly by Falkner et al. (2024), who conduct a systematic analysis of the gap

between EU digital sovereignty discourse and actual policy outcomes. Their finding, that digital sovereignty functions primarily as a legitimating frame for diverse and sometimes contradictory policy initiatives rather than as a coherent strategic project, resonates with Lambach and Oppermann's (2022) discourse analysis of German digital sovereignty narratives, which shows how the concept is deployed differentially across partisan and institutional contexts to advance pre-existing policy agendas. These findings caution against taking digital sovereignty claims at face value in international relations analysis.

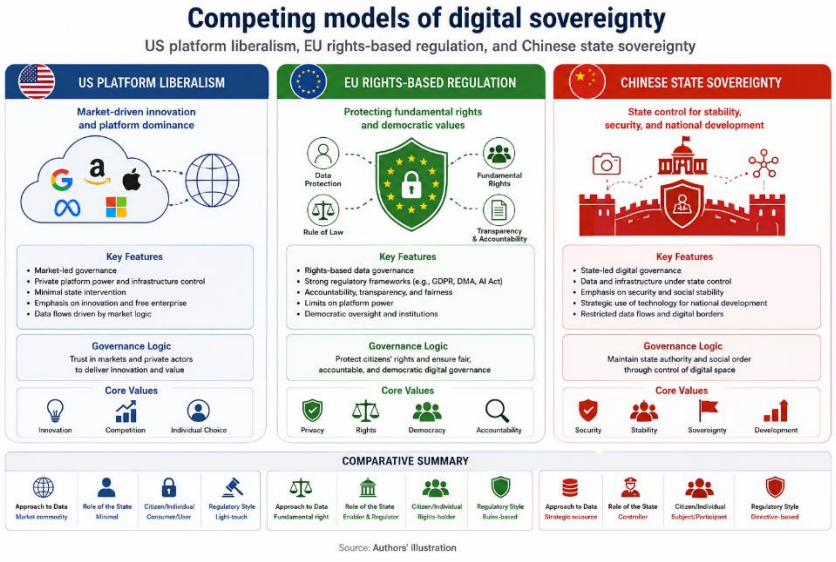

Figure 1. *Competing models of digital sovereignty: US platform liberalism, EU rights-based regulation, and Chinese state sovereignty. Source: Authors' illustration*

B. Geopolitical Dynamics of the Data Control Contest

The geopolitical dimensions of the digital sovereignty contest are analyzed most comprehensively by Liu (2021), whose study of "Digital China" situates Chinese data politics within the framework of authoritarian statecraft and great power competition. Liu argues that the Chinese state has pursued a distinctive three-track strategy: internally, deploying data governance mechanisms, including the Social Credit System, data localization mandates, and algorithmic surveillance infrastructure, to enhance political control and economic planning; externally, promoting an alternative norm of "cyber sovereignty" in multilateral internet governance forums to contest the liberal internet governance model championed by the United States; and transnationally, leveraging the Digital Silk Road to extend Chinese technological infrastructure and data governance norms into partner states, particularly across Central Asia, Southeast Asia, and Sub-Saharan Africa.

The European response to this geopolitical context is theorized through the lens of "Normative Power Europe" by Broeders et al. (2023), who argue that the EU has sought to translate its regulatory power, most visibly the GDPR's extraterritorial data protection standards, into a form of geopolitical influence that positions Europe as a model for rights-based digital governance globally. However, Broeders et al. identify a fundamental tension: the same normative ambition that constitutes the EU's distinctive contribution to global digital governance simultaneously limits its capacity to develop the offensive technological capabilities that geopolitical competition increasingly demands. This tension manifests

most acutely in debates over AI governance, where Calderaro and Blumfelde (2022) argue that the EU's framing of AI as a digital sovereignty issue produces rhetorical empowerment but structural dependency, since European AI development continues to rely on US and Chinese hardware, cloud infrastructure, and foundational model capabilities.

Nost and Goldstein (2021) contribute a distinctive perspective from political ecology, arguing that the power relations embedded in data infrastructure, data centers, undersea cables, satellite networks, and cloud architecture, must be understood not only as instruments of state power but as material configurations that generate their own political dynamics. Their analysis reveals how the geography of digital infrastructure reproduces and intensifies existing patterns of global political-economic inequality, with Global South states subject to data extraction regimes that mirror the extractive dynamics of colonial resource governance. This perspective illuminates why digital sovereignty has resonance well beyond the major power competition between the US, EU, and China, manifesting as demands for "data justice" and "digital colonialism" frameworks among scholars and activists representing developing country interests.

Table 2 Comparative Models of Digital Sovereignty: Key Actors and Approaches

Dimension	United States	European Union	China	Global South
Primary Model	Platform liberalism; minimal state intervention; market-led governance	Rights-based regulatory model; GDPR, DSA, DMA as regulatory exports	State sovereignty model; cyber sovereignty in multilateral forums	Data justice; anti-digital colonialism; localization & capacity building
Key Mechanisms	Export of US platform norms; bilateral data agreements; intelligence surveillance	Regulatory extraterritoriality; Gaia-X cloud initiative; AI Act	Great Firewall; data localization laws; Digital Silk Road	Data localization mandates; multilateral coalitions; UN Internet Governance Forum
Normative Frame	Freedom of information flow; open internet; anti-censorship norms	Fundamental rights; democratic values; technological autonomy	National sovereignty; non-interference; cyber order	Development sovereignty; equitable data governance; digital inclusion
Main Tensions	Contradiction between data freedom rhetoric and NSA surveillance	Gap between normative ambition and structural tech dependency	Tension between internal control and global connectivity needs	Limited bargaining power; fragmentation of demands across 130+ states
Geopolitical Vector	Maintaining platform hegemony; bilateral ally alignment	Third-way positioning; Brussels Effect in regulation	Expanding Digital Silk Road; contesting liberal internet governance	Seeking regulatory space; avoiding becoming arena for US-China competition

***Note**. Adapted from Glasze et al. (2022); Liu (2021); Broeders et al. (2023); Nost & Goldstein (2021)*

C. Governance Implications and Institutional Responses

The governance implications of the digital sovereignty contest are analyzed across multiple institutional levels in the reviewed literature. At the national level, Von Scherenberg et al. (2024) and Möller et al. (2024) examine the technical and organizational

architectures required to operationalize data sovereignty in practice. Von Scherenberg et al. argue that data sovereignty in information systems requires a shift from ownership-centric to control-centric governance frameworks, in which rights over data are specified not merely in terms of legal title but in terms of enforceable technical constraints on data access, processing, and transfer. Möller et al. extend this analysis to industrial data ecosystems, demonstrating how "data spaces", federated technical architectures enabling controlled data sharing between firms within defined governance rules, represent a promising institutional model for operationalizing sovereignty at sectoral level.

The role of technology sovereignty in innovation policy is theorized by Edler et al. (2023), who argue that technology sovereignty has emerged as a new framing for industrial and innovation policy that transcends traditional market-failure rationales for state intervention. Their analysis identifies three distinct rationales for technology sovereignty policy: security rationales (protecting critical infrastructure from foreign control), economic rationales (maintaining industrial competitiveness and avoiding strategic dependencies), and values rationales (ensuring that technological development reflects domestic social and political values). These rationales are not always mutually consistent, and Edler et al. argue that failure to distinguish them generates policy incoherence, a critique that resonates strongly with Falkner et al.'s (2024) finding that EU digital sovereignty policy is internally contradictory.

The governance of artificial intelligence represents a particularly acute site of digital sovereignty contestation. Both Calderaro and Blumfelde (2022) and Mügge (2024) subject the EU's AI sovereignty agenda to critical scrutiny. Calderaro and Blumfelde argue that the EU's framing of AI governance as a digital sovereignty issue systematically overstates European institutional capacity while understating structural dependencies on non-European AI infrastructure. Mügge (2024) offers a sharper political economy critique, arguing that EU AI sovereignty primarily serves the interests of large European corporations and regulatory elites rather than broader European citizenry, reproducing within the European digital space the concentration of technological power that European digital sovereignty ostensibly contests.

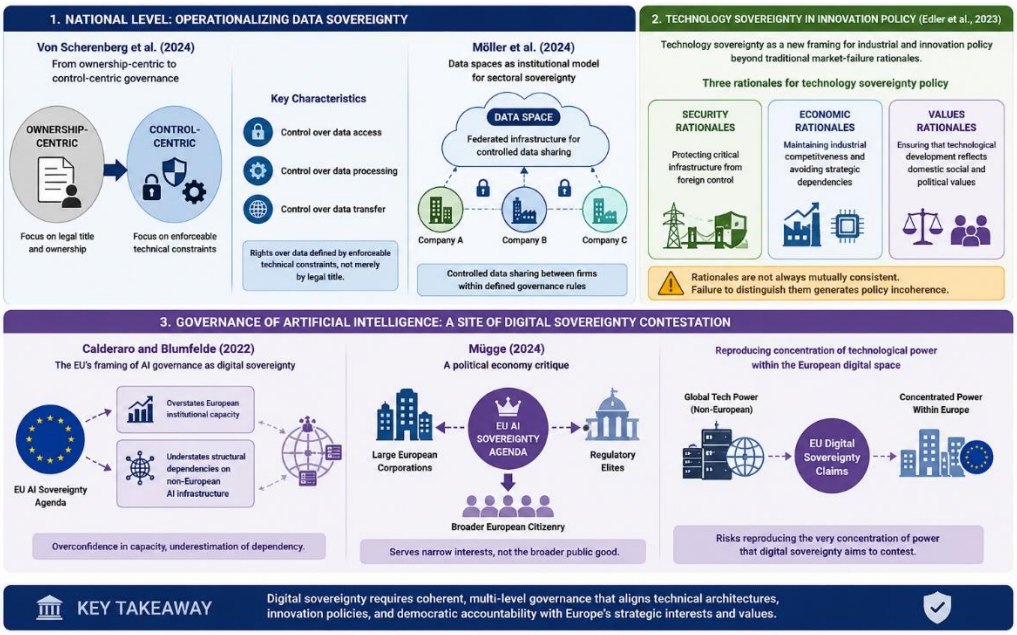

Figure 2. *Governance Implication and Institutional Responses*

The Gaia-X cloud initiative provides perhaps the most instructive case study of the gap between digital sovereignty ambition and governance reality. Adler-Nissen and Eggeling (2024) analyze Gaia-X as a discursive field in which three competing framings, security, economic competitiveness, and rights protection contest the meaning and direction of the initiative, producing what the authors characterize as a "discursive battleground" that simultaneously enables coalition-building across these diverse interests and generates fundamental tensions over Gaia-X's scope, membership, and governance model. The inclusion of Amazon Web Services and Microsoft Azure as Gaia-X participants, a decision driven by pragmatic consideration of existing market dependencies exemplified these tensions, provoking criticism that Gaia-X was reproducing rather than contesting US platform dominance under the cover of European sovereignty rhetoric.

Tan et al. (2023) contribute a technical systems perspective, arguing that effective digital sovereignty requires layered identity frameworks that span the full spectrum from digitization (converting analog information to digital form) to digitalization (embedding digital technologies in social processes) to digital transformation (systemic reorganization of institutions around digital capabilities). Their survey of digital identity architectures finds that existing frameworks are systematically inadequate for supporting genuine data sovereignty, particularly in cross-border contexts, and propose a reference architecture for self-sovereign identity systems that would enable individuals and institutions to manage their own digital identities without dependence on centralized platform intermediaries.

The implications of these governance challenges for international order are considerable. The reviewed literature converges on a diagnosis of increasing fragmentation—what Monsees and Lambach (2022) characterize as the reproduction of geopolitical boundaries within digital space, that threatens the interoperability and universality of the global internet. Whether this fragmentation constitutes a fundamental challenge to international order or is better understood as a functional differentiation within a continuing global information ecosystem remains a matter of scholarly debate. What is clear from the synthesis is that digital sovereignty is not merely a technical governance problem but a fundamental political question about the distribution of power, rights, and responsibilities in the digital age, a question that international relations scholarship is uniquely positioned to address.

CONCLUSION

This systematic review has synthesized 20 peer-reviewed studies to construct a comprehensive analytical framework for understanding digital sovereignty as a contested phenomenon in contemporary international relations. Three principal conclusions emerge. First, digital sovereignty is a fundamentally contested concept whose meaning varies across geopolitical contexts, theoretical traditions, and institutional arenas, and whose analytical utility depends on careful specification of which dimension, legal-jurisdictional, individual-rights, technical-infrastructural, or collective-developmental is at stake. Second, the geopolitical dynamics of the data control contest reflect a triangular competition between US platform liberalism, EU rights-based regulation, and Chinese state sovereignty, within which Global South states occupy a structurally disadvantaged position from which they seek to articulate an alternative "data justice" agenda. Third, the governance implications of this

contest are severe, threatening the fragmentation of the global information environment and demanding institutional innovation at national, regional, and international levels that goes far beyond the rhetorical proclamations of digital sovereignty that characterize current policy discourse.

Future research should prioritize comparative empirical analysis of digital sovereignty policy implementation across diverse national contexts, including systematic examination of Global South sovereignty claims that have been underrepresented in existing scholarship. Interdisciplinary collaboration between international relations, legal studies, information systems, and technical computer science will be essential for developing governance frameworks that are simultaneously politically viable and technically effective. The digital sovereignty contest will shape international order for decades to come; the quality of scholarly analysis available to inform it matters enormously.

LITERATURE

Adler-Nissen, R., & Eggeling, K. (2024). The discursive struggle for digital sovereignty: Security, economy rights and the Cloud Project Gaia-X. JCMS: Journal of Common Market Studies. https://doi.org/10.1111/jcms.13594

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

Broeders, D., Cristiano, F., & Kaminska, M. (2023). In search of digital sovereignty and strategic autonomy: Normative Power Europe to the test of its geopolitical ambitions. JCMS: Journal of Common Market Studies. https://doi.org/10.1111/jcms.13462

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. European Security, 31, 415–434. https://doi.org/10.1080/09662839.2022.2101885

Edler, J., Blind, K., Kroll, H., & Schubert, T. (2023). Technology sovereignty as an emerging frame for innovation policy: Defining rationales, ends and means. Research Policy. https://doi.org/10.1016/j.respol.2023.104765

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty – Rhetoric and reality. Journal of European Public Policy, 31, 2099–2120. https://doi.org/10.1080/13501763.2024.2358984

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

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Desforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2022). Contested spatialities of digital sovereignty. Geopolitics, 28, 919–958. https://doi.org/10.1080/14650045.2022.2050070

Gu, H. (2023). Data, Big Tech, and the new concept of sovereignty. Journal of Chinese Political Science, 1–22. https://doi.org/10.1007/s11366-023-09855-1

Heidebrecht, S. (2023). From market liberalism to public intervention: Digital sovereignty and changing European Union Digital Single Market governance. JCMS: Journal of Common Market Studies. https://doi.org/10.1111/jcms.13488

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

Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. Governance. https://doi.org/10.1111/gove.12690

Liu, L. (2021). The rise of data politics: Digital China and the world. Studies in Comparative International Development, 56, 45–67. https://doi.org/10.1007/s12116-021-09319-8

Möller, F., Jussen, I., Springer, V., Gieß, A., Schweihoff, J., Gelhaar, J., Guggenberger, T., & Otto, B. (2024). Industrial data ecosystems and data spaces. Electronic Markets, 34. https://doi.org/10.1007/s12525-024-00724-0

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

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? Journal of European Public Policy, 31, 2200–2225. https://doi.org/10.1080/13501763.2024.2318475

Nost, E., & Goldstein, J. (2021). A political ecology of data. Environment and Planning E: Nature and Space, 5, 3–17. https://doi.org/10.1177/25148486211043503

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. Internet Policy Review, 10. https://doi.org/10.14763/2021.3.1575

Tan, K.-L., Chi, C.-H., & Lam, K.-Y. (2023). Survey on digital sovereignty and identity: From digitization to digitalization. ACM Computing Surveys, 56, 1–36. https://doi.org/10.1145/3616400

Von Scherenberg, F., Hellmeier, M., & Otto, B. (2024). Data sovereignty in information systems. Electronic Markets, 34. https://doi.org/10.1007/s