cogitatio

POLITICS AND GOVERNANCE

Volume 13

2025

The Geopolitics of Transnational Data Governance

Open Access Journal

ISSN: 2183-2463

Edited by Xinchuchu Gao and Xuechen Chen

Politics and Governance, 2025, Volume 13
The Geopolitics of Transnational Data Governance

Published by Cogitatio Press
Rua Fialho de Almeida 14, 2º Esq.,
1070–129 Lisbon
Portugal

Design by Typografia®
http://www.typografia.pt/en/

Cover image: © Designed by Freepik (www.freepik.com)

Academic Editors
Xinchuchu Gao (University of Lincoln)
Xuechen Chen (Northeastern University London)

Available online at: www.cogitatiopress.com/politicsandgovernance

Table of Contents

Table of Contents

Politics and Governance
2025 • Volume 13 • Article 11428
https://doi.org/10.17645/pag.11428

cogitatio

EDITORIAL

Open Access Journal

Geopolitics and Transnational Data Governance

Xinchuchu Gao [1] and Xuechen Chen [2]

[1] School of Social and Political Sciences, University of Lincoln, UK
[2] Faculty of Social Sciences, Northeastern University London, UK

Correspondence: Xinchuchu Gao (xingao@lincoln.ac.uk)

Submitted: 27 September 2025 **Published:** 23 October 2025

Issue: This editorial is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

This editorial introduces a thematic issue that examines the geopolitics of transnational data governance through interdisciplinary perspectives. It explores how data governance—once a technocratic concern—has become a core domain of geopolitical rivalry and statecraft. Contributions in this issue highlight the tensions between data sovereignty and transnational flows, great power rivalry in transnational data governance, the growing importance of informal and plurilateral governance, and the strategic agency of Global South actors. The issue also foregrounds the critical but often overlooked roles of private sector actors and sector-specific governance in domains such as energy, semiconductors, and development aid. By analysing contested norms, competing governance models, and hybrid institutional arrangements, the articles collectively show how transnational data governance reflects and shapes broader geopolitical dynamics.

Keywords

data governance; geopolitics; normative contestation; power rivalry; technology

1. Introduction

In the contemporary digital era, data has emerged as one of the most valuable and contested resources in the global political economy. Its significance extends far beyond its economic role as a driver of innovation, commerce, and growth. Data also underpins national sovereignty and serves as a key determinant of security. The regulation and governance of data flows are therefore no longer peripheral concerns reserved for technocrats or niche regulators; they have become central issues of geopolitics and international power rivalry (O'Hara & Hall, 2021).

Recent global crises have reinforced this shift. The Covid-19 pandemic underscored the indispensability of data for crisis management, from health surveillance and vaccine distribution to the control of misinformation (Caceres et al., 2022; Li et al., 2022). At the same time, the war in Ukraine highlighted the strategic role of data and information warfare in contemporary conflict (Arner et al., 2022). These events collectively demonstrate the extent to which data infrastructures, standards, and governance frameworks are deeply intertwined with questions of politics, security, and global power dynamics. Crucially, the governance of cross-border data flows has evolved from a technical or regulatory concern into a core field of geopolitical contestation. Competing models—including liberal, market-driven approaches, rights-based frameworks, and sovereignty-centric paradigms—promoted by major international actors, such as the United States, the European Union, and China, are reshaping the global digital order (Arner et al., 2022; Bradford, 2023).

Against this backdrop, this thematic issue brings together 12 contributions from diverse disciplinary perspectives—including political science, communication studies, law, and development studies—to examine the geopolitics of transnational data governance.

The contributions in this issue interrogate how state actors, regional organisations, and private sector stakeholders frame and implement data governance amid intensifying great-power rivalry, technological interdependence, and normative contestation. Together, they illuminate three central dynamics. First, data governance has become a key instrument of geoeconomic and geopolitical statecraft, exercised through both formal and informal mechanisms. Second, the pursuit of digital sovereignty increasingly clashes with the inescapable interdependence of global infrastructures and supply chains. Third, agency in transnational data governance is highly distributed: not only great powers, but also middle powers, private corporations, and international organisations actively shape the emerging order. This editorial outlines the contours of these debates, synthesises the findings of the 12 articles, and proposes a future research agenda for the study of geopolitics and data governance.

2. Key Debates Featured in This Thematic Issue

This thematic issue explores key debates at the intersection of geopolitics and transnational data governance. First, it highlights the persistent tension between data as a sovereign resource and as a transnational flow. Sovereignty claims have proliferated—from China's cyber sovereignty and the EU's digital sovereignty to India's emphasis on developmental data and the US's restrictions on sensitive transfers. Yet, the global nature of data infrastructures renders full autonomy elusive. Contributions reveal how governance frameworks often oscillate between data localisation and conditional openness, seeking to balance security with economic integration.

Second, the issue examines formal versus informal governance mechanisms. While early digital trade efforts centred on formal WTO-led agreements, recent years have seen the rise of informal and plurilateral arrangements. These enable regulatory flexibility and coalition-building, yet raise concerns about accountability and inclusivity. The contributions show that informality is now central—not peripheral—to the practice of data geopolitics.

A third major theme is the evolving role of the Global South and cross-regional actors. While much attention has focused on the US–EU–China regulatory triangle and the EU's "Brussels effect," this issue foregrounds the agency of Global South actors such as India and ASEAN. These actors are not passive recipients of external norms; they strategically leverage data governance to attract investment, build capacity, and negotiate influence. Development data infrastructures like the OECD Creditor Reporting System (CRS) and International Aid Transparency Initiative (IATI) both reflect power asymmetries and offer opportunities for contestation.

Another underexplored yet critical dimension involves the entanglement of state and corporate actors. Private firms—especially big tech and infrastructure providers—act as both rule-takers and rule-makers, wielding infrastructural power comparable to that of states. Controversies around TikTok, Chinese cloud providers in ASEAN, and Starlink's negotiations with European governments illustrate how corporate agency intersects with sovereign agendas in complex and unpredictable ways. Several contributions also stress the importance of sectoral and issue-specific governance. Data politics extend well beyond digital platforms, influencing energy transitions, semiconductor supply chains, and development aid. This sectoralisation underscores how data infrastructures shape a broadening array of geopolitical domains once considered technocratic. Finally, the issue engages with normative and cognitive contestations surrounding data governance. Competing views of data—as a commodity, strategic asset, or fundamental right—shape regulatory frameworks and reflect deeper ideological cleavages. Collectively, the contributions demonstrate that the geopolitics of data is as much about meanings and norms as it is about infrastructure and power.

3. Synthesis of Contributions

In this thematic issue, several articles explore how great powers and major players instrumentalise data governance as part of broader geoeconomic and geopolitical strategies. Specifically, Sukumar and Basu's (2025) contribution traces the US turn towards informality in its withdrawal from WTO negotiations and reliance on plurilateral initiatives such as the Indo-Pacific Economic Framework and G7 statements. Su and Zhang (2025) examine the evolution of China's legislative framework from the 2016 Cybersecurity Law to the Data Security Law and Personal Information Protection Law. They show how China balances sovereignty claims with selective openness, pursuing an "adaptive sovereignty" that seeks both security and global influence. Complementing this, He and Zeng (2025) analyse China and India comparatively, emphasising the role of state–capital relations. They argue that what appears as sovereignty discourse is often deeply rooted in domestic political economy and the interests of technology firms and capital. From a broader perspective, Liu (2025) adopts a constructivist lens, highlighting how data cognition—the cultural values attached to data—shapes governance. By comparing the US, EU, China, and Russia, the article identifies distinct "evaluative cognitions" that underpin policy shifts and international contests over cross-border flows. In addition, Cristiano and Monsees (2025) explore the framing of TikTok bans in Europe and the US—a telling example of geopolitical contestation over data governance. While both invoke security, the EU frames its actions through privacy and fundamental rights, whereas the US foregrounds national security and China-related risks. This illustrates divergent governance cultures within the West. A cluster of contributions investigates the EU's unique position and evolving role in transnational data governance. Carrapico and Farrand (2025) analyse the governance gap between autonomy aspirations and interdependence realities in the EU's data sovereignty agenda. Using semiconductors as a case study, they show how global supply chain dependencies undermine the EU's ability to operationalise full sovereignty. Heidebrecht (2025) highlights

how digital policy has served as a driver of integration and Commission empowerment. In addition, Zhang (2025) examines the diffusion of EU data governance to Japan and Singapore, highlighting both the strength and the limits of the EU's normative power in Asia.

Further contributions show that data governance debates also play out in the context of domestic politics. For example, Griffini's (2025) study of Italy's populist radical right analyses parliamentary debates on digital sovereignty in the context of Giorgia Meloni's engagement with Elon Musk's Starlink project. It shows how party ideology shapes external digital policy, with sovereignist parties prioritising control and security over openness. Yang and Li (2025) introduce the concept of offshore embeddedness to explain how Chinese cloud providers like Alibaba and Tencent secure legitimacy in ASEAN. By decoupling from home-state control and embedding themselves in host-country governance structures, these firms turn suspicion into acceptance, illustrating ASEAN states' agency as regulators, brokers, and orchestrators.

In addition, several contributors look beyond the traditional focus on major power rivalry and conventional regulatory issues in terms of data governance by paying specific attention to an increasing trend of sectoralisation and issue-specific governance of transnational data. Specifically, Yu et al. (2025) extend the debate into the energy sector, comparing EU and ASEAN data governance in the energy transition, showing how centralised EU governance enables cross-border power grids, raw material tracking, and carbon markets, whereas ASEAN's decentralised model offers flexibility but risks fragmentation. Similarly, Park's (2025) contribution examines development data infrastructures as an insightful case study. By analysing OECD's CRS and IATI, it shows how aid data governance reflects power hierarchies, donor priorities, and competing visions of transparency and accountability. Datafication of aid reshapes development practices, with geopolitical implications for how the Global South engages with international donors. Together, these studies highlight that data governance permeates diverse policy fields, each revealing tensions between sovereignty, interdependence, and normative contestation.

Acknowledgments

We would like to express our deepest gratitude to all the contributors to this thematic issue for their insightful and thought-provoking articles. Their work reflects a remarkable breadth of disciplinary perspectives and empirical cases, and together they have significantly advanced scholarly understanding of the geopolitics of transnational data governance. We are also sincerely grateful to the anonymous peer reviewers whose constructive feedback and intellectual generosity greatly enriched the quality of the individual contributions and the coherence of the thematic issue as a whole. Their careful engagement and critical insights were invaluable throughout the editorial process. Finally, we extend our heartfelt thanks to the editorial team at *Politics and Governance* for their unwavering support and professionalism at every stage—from the initial proposal to final production. Their guidance, efficiency, and encouragement made the realisation of this thematic issue possible.

Conflict of Interests

The authors declare no conflict of interests.

References

Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. *Berkeley Technology Law Journal*, 37, 623–699.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Caceres, M. M. F., Sosa, J. P., Lawrence, J. A., Sestacovschi, C., Tidd-Johnson, A., Rasool, M. H. U., Gadamidi, V., Ozair, S., Pandav, K., Cuevas-Lou, C., Parrish, M., Rodriguez, I., & Fernandez, J. P. (2022). The impact of misinformation on the Covid-19 pandemic. *AIMS Public Health*, *9*(2), 262–277.

Carrapico, H., & Farrand, B. (2025). EU data sovereignty: An autonomy–interdependence governance gap? *Politics and Governance*, *13*, Article 10331. https://doi.org/10.17645/pag.10331

Cristiano, F., & Monsees, L. (2025). Beyond the Ban: TikTok and the Politics of Digital Sovereignty in the EU and US. *Politics and Governance*, *13*, Article 10461. https://doi.org/10.17645/pag.10461

Griffini, M. (2025). Digital sovereignism: A comparative analysis of Italian Parties' positioning on transnational data governance. *Politics and Governance*, *13*, Article 10575. https://doi.org/10.17645/pag.10575

He, Y., & Zeng, K. (2025). A geopolitical economy analysis of China and India's approaches to transnational data governance. *Politics and Governance*, *13*, Article 10361. https://doi.org/10.17645/pag.10361

Heidebrecht, S. (2025). Digital policy as a driver of integration: Spillover effects and European Commission empowerment. *Politics and Governance*, *13*, Article 10474. https://doi.org/10.17645/pag.10474

Li, V. Q., Ma, L., & Wu, X. (2022). Covid-19, policy change, and post-pandemic data governance: A case analysis of contact tracing applications in East Asia. *Policy and Society*, *41*(1), 129–142.

Liu, J. (2025). Ruling the data flows: Data cognition in global cross-border data flows governance. *Politics and Governance*, *13*, Article 10460. https://doi.org/10.17645/pag.10460

O'Hara, K., & Hall, W. (2021). *Four internets: Data, geopolitics, and the governance of cyberspace*. Oxford University Press.

Park, K. (2025). Fragmented Data Governance, Shared Norms: Navigating Regime Complexity in Aid Data Governance. *Politics and Governance*, *13*, Article 10508. https://doi.org/10.17645/pag.10508

Su, R., & Zhang, D. (2025). Adaptive sovereignty: China's evolving legislative framework for transnational data governance. *Politics and Governance*, *13*, Article 10413. https://doi.org/10.17645/pag.10413

Sukumar, A., & Basu, A. (2025). The China gambit: Geoeconomics and the US' turn to informal data governance initiatives. *Politics and Governance*, *13*, Article 10512. https://doi.org/10.17645/pag.10512

Yang, B., & Li, M. (2025). Offshore embeddedness beyond the wall: Chinese cloud providers in Southeast Asia's data governance landscape. *Politics and Governance*, *13*, Article 10437. https://doi.org/10.17645/pag.10437

Yu, K., Sung, J., & Zhou, Y. (2025). Data governance in the geopolitics of energy transition: Comparing regional energy cooperation in ASEAN and the EU. *Politics and Governance*, *13*, Article 10429. https://doi.org/10.17645/pag.10429

Zhang, D. (2025). The EU's digital footprint: Shaping data governance in Japan and Singapore. *Politics and Governance*, *13*, Article 10422. https://doi.org/10.17645/pag.10422

About the Authors

Xinchuchu Gao is a lecturer in international relations at the University of Lincoln. Her research interests lie at the intersections between international relations, international political economy, and European studies. Within this broad framework, she is specifically interested in the twin green and digital transitions of the EU and global cyber governance.

Xuechen Chen is an associate professor in politics & international relations at Northeastern University London. Her research expertise lies at the intersection of international relations and area studies. Her research interests include EU external relations with the Asia-Pacific region, China's foreign policy, and norm diffusion in international politics, with a particular focus on digital governance and non-traditional security issues.

Politics and Governance
2025 • Volume 13 • Article 10512
https://doi.org/10.17645/pag.10512

cogitatio

ARTICLE

Open Access Journal

The China Gambit: Geoeconomics and the US' Turn to Informal Data Governance Initiatives

Arun Sukumar [1] and Arindrajit Basu [2]

[1] Department of International Relations, Ashoka University, India
[2] Institute of Security and Global Affairs, Leiden University, The Netherlands

Correspondence: Arindrajit Basu (a.basu@fgga.leidenuniv.nl)

Submitted: 11 April 2025 **Accepted:** 25 June 2025 **Published:** 24 September 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

In October 2023, the US withdrew its proposals on cross-border data flows at the World Trade Organization (WTO), reversing its long-held position on binding commitments against data localization. Concurrently, it has orchestrated the creation of several informal data governance initiatives, including the Indo-Pacific Economic Framework for Prosperity, which are all characterized by fluid commitments on data flows. This article demonstrates that the US' turn toward informal data governance is influenced considerably by geoeconomic statecraft. Confronted with the prospect of China leveraging global data flows to undermine American interests, both in terms of national security and economic competitiveness, the US executive has sought to restrict outbound data flows. In parallel, it has developed informal, like-minded coalitions to promote norms around "trusted data flows," that similarly restrict data collection by Chinese actors globally. Having withdrawn from formal WTO discussions on cross-border data, its informal initiatives give the US ample regulatory space to implement coercive domestic measures against Chinese actors. Informal initiatives simultaneously allow the US to develop norm-setting coalitions with states that may otherwise be wary of binding commitments on restrictive data flows. Drawing on an analysis of seven international data governance initiatives, alongside US domestic policies and official statements, we trace the US' turn toward informality to its geoeconomic considerations. We contribute to theoretical debates on the evolution and shift in geoeconomic statecraft, particularly the shift away from formal sanctions-based regimes to informal agreements, as well as to the empirical literature on international cross-border data governance.

Keywords

cross-border data flows; geoeconomics; informality; United States

1. Introduction

In October 2023, the US Trade Representative (USTR) withdrew US proposals for binding commitments at the World Trade Organization (WTO) on the free flow of data and against the forced disclosure of source code by governments. The withdrawal was abrupt, and marked a reversal in longstanding US trade policy (Global Data Alliance, 2023). The US government justified its decision on the grounds that it was preserving "policy space" to further review the implications of digital trade rules on its digital economy and security (USTR, 2023). Less than a month later, the US also withdrew support for digital trade-related proposals at the Indo-Pacific Economic Framework for Prosperity (IPEF), an economic arrangement with Asia-Pacific countries that the US itself had orchestrated (Lawder, 2023).

These back-to-back announcements signaled not only a consequential shift in how the US approaches cross-border data flows, but also the governance mechanisms it uses to manage them. Even as the US withdrew its support for WTO proposals, the US continued to champion open data flows through informal arrangements such as the G7, the Organisation for Economic Cooperation and Development (OECD), the EU–US Trade and Technology Council (TTC), the Digital Transformation with Africa initiative, and the Americas Partnership for Economic Prosperity. While non-binding agreements are an increasingly prominent part of the US diplomatic toolkit, there appears at the time of writing to be a strong preference for informal mechanisms over formal commitments on cross-border data flows. Indeed, the only binding agreement that currently enshrines the free flow of data across American borders is the US–Mexico–Canada Agreement (USMCA), which may well be revoked when it comes up for review in 2026 ("Making NAFTA worse," 2025).

What explains the US shift on cross-border data governance, both in form and in substance? The rise of informality in global governance is a well-documented phenomenon and an object of inquiry in both international relations and international law scholarship. Studies in both disciplines have examined the drivers of informal "executive agreements" by states, including the US, emphasizing the flexibility of non-binding commitments and their ability to circumvent protracted treaty ratification processes (Bradley et al., 2023; Vabulas & Snidal, 2013). In the context of cross-border data governance, scholars have argued that the US preference for non-binding frameworks is driven by a desire for regulatory autonomy to address antitrust and workers' rights concerns (Mueller, 2025).

This article highlights another important, yet understudied, consideration that has influenced the US' turn towards informal cross-border data governance: geoeconomics. The study of "geoeconomics"—understood as the use of "economic instruments to promote national interests [and] produce beneficial geopolitical results" (Blackwill & Harris, 2016)—has long been a mainstream theme within international relations and international political economy literature. Geoeconomic tools of coercion and deterrence have typically taken the form of sanctions or other binding instruments. That is, however, now beginning to change. In the backdrop of Great Power competition between the US and China, more states (including the main protagonists themselves) have turned towards coercive economic measures against their foreign adversaries. However, for reasons we detail in this article, such tools of statecraft are increasingly informal. States that orchestrate geoeconomic initiatives are concerned that binding multilateral commitments will reduce their own autonomy to craft domestic policies targeting foreign adversaries. Equally, they are mindful that formal agreements may prevent coalition-building with partners and allies who find themselves enmeshed in interdependent supply chains. "The game is not the same," noted then-US National Security Advisor (NSA)

Jake Sullivan in 2023, referencing the inability of the formal "multilateral trading system to…accommodate legitimate national security interests….Our international economic policy has to adapt to the world as it is, so we can build the world that we want" (Sullivan, 2023b). Informal agreements have emerged as key instruments for the US in this world-building endeavor.

We demonstrate that the US' turn to informality in cross-border data governance too is being influenced by the abovementioned domestic and international concerns. Mindful of the collection of American and global data by Chinese entities, and the potential transfer of such data to Chinese state actors, the US has retreated from binding commitments against freer data flows. Both national security and economic security concerns about China (Harrell, 2025) have played a role in the US' decision, as we show. At the same time, the US continues to champion "trusted" data flows globally—understood as data flows that prevent or limit the storage and processing of data by Chinese actors—with allies and partners. To accommodate domestic policies that restrict outward data flows from its territory in certain cases, and simultaneously develop coalitions of states that can implement data transfer policies similar to its own, Washington DC has turned to informal initiatives. In 2024, the US State Department folded its informal digital trade and cross-border data initiatives within the umbrella of "digital solidarity," denoting a diplomatic effort to bring together like-minded partners to create "trusted" digital ecosystems that exclude American adversaries (Fang & Hwang, 2024).

Our findings are based on an empirical analysis of US domestic policies, official statements, and public commentary on digital trade and cross-border data flows. The review period for primary sources spans from January 2020 to December 2024, aligning chronologically with the Biden administration's announcement of informal agreements. Primary data were drawn from press releases issued between January 2020 and January 2024 by key government entities responsible for US trade and security policy, including:

a. The White House;
b. The Office of the USTR;
c. The US Department of Commerce.

From the archives of these government entities, we analyzed the following types of documents:

a. Statements made by nodal policymakers in each government agency (specifically, the USTR, Commerce Secretary, NSA, and the President);
b. Notifications of domestic federal legislation, policy, or executive orders related to data governance.

Sorting for relevance, we further filtered those documents that included one or more of the following criteria:

a. Referred to national security concerns;
b. Addressed any aspect of digital trade or policy on data governance;
c. Highlighted informal governance and coalition-building.

We then developed a timeline of US engagement with informal data governance initiatives, and demonstrate that (a) the US' withdrawal of formal proposals against data localization, (b) the restrictive domestic policies on data flows, and (c) informal coalition building on "trusted data flows," all occurred in lockstep with the articulation by policy-makers of the data security threat posed by China. We consider seven informal initiatives,

namely the Indo-Pacific Economic Framework (IPEF), G7, Quadrilateral Security Dialogue ("the Quad"), EU–US Trade and Technology Council (EU–US TTC), OECD Declaration on Government Access to Personal Data Held by Private Sector Entities, Digital Transformation with Africa initiative (DTAT), and the Americas Partnership for Economic Prosperity (APEP).

By highlighting geoeconomics as a factor shaping US engagement with data governance initiatives, we contribute to both theory and empirical scholarship on the impact of geoeconomic statecraft on contemporary international relations and international law. Section 2 reviews the literature on global governance and economic statecraft. Section 3 outlines the evolution of US diplomacy on cross-border data flows, beginning with its withdrawal from the WTO's Joint Initiative on e-Commerce (JI). Section 4 explores the reasons behind its shift toward informal data governance initiatives. Section 5 concludes by examining the prospects for informal data governance under the Trump administration.

2. Geoeconomic Statecraft, Multilateral Governance, and 21st-Century Concerns

Scholarly analyses of geoeconomic statecraft have traditionally focused on tools of coercion such as sanctions (Mastanduno, 1999), including circumstances under which they are imposed (Pape, 1997), generalizable political attributes of sanctioning states and targeted states (Brooks, 2002; Escribà-Folch & Wright, 2010), the effectiveness of coercive measures in meeting stated policy goals (Baldwin & Pape, 1998; Blanchard & Ripsman, 1999), as well as their subtle impact as tools of signaling or deterrence (Drezner, 2003; Kirshner, 1997). These analyses correspond to a post-Cold War period where coercive measures were mainly deployed by a hegemon, either unilaterally or in concert with like-minded partners, against smaller powers for objectives such as human rights compliance, non-proliferation, or liberal market reforms (Drezner, 2024). That period is now over, and geoeconomics is today characterized by competition and contestation between two Great Powers, the US and China (Aggarwal & Reddie, 2021). Both parties contemplate coercive measures against each other at a point when their economies and supply chains are deeply intertwined in ways that make spillover effects difficult to discern.

Indeed, geoeconomics has acquired renewed interest in academic and policy settings primarily on account of the rise of China (Blackwill & Harris, 2016). China's emergence as an economic and military power has been underpinned by "party-state capitalism," a form of political economy in which the Communist Party of China exerts express or implicit authority over market actors to secure the state's interests (Pearson et al., 2022). The Chinese state has wielded its influence over the domestic market, especially in digital technologies, to shape favorable political outcomes for the Party. At the same time, it has also induced and compelled geopolitical outcomes in Asia, Africa, and Latin America through the use of economic tools like lines of credit, informal sanctions, supply chain controls, and strategic investment initiatives (Norris, 2016; Wong, 2023). The use of such tools, whether as carrots or sticks, is not a novelty (Drezner, 2024). While there may be differences in approaches between the US and China, the use of economic statecraft by the latter as it rises on the world stage should not be a surprise.

Nevertheless, this era of geoeconomic statecraft is likely to be different from previous decades, because it also coincides with a crisis in multilateral governance. Multilateral mechanisms of global governance are going through a period of major transformation. Great Power competition, tensions induced by multipolarity, and the rise of private actors with the infrastructure and resources to shape diplomatic outcomes have all eroded the

ability of existing international organizations to induce compliant behavior (Tallberg et al., 2023). Geoeconomic maneuvering is arguably contributing to this crisis. Attempts by states to restrict commerce with competitors or deny them access to sensitive technologies through sanctions challenge existing rules on international trade and mobility (Malkin & He, 2024). The ongoing US trade war with China is one of the most "frequently cited examples" (Kürzdörfer, 2025, p. 2) of the vulnerability of global supply chains (Zeng et al., 2022). Meanwhile, major technology companies like Microsoft, SpaceX, and ASML have also begun to exert "corporate autonomy" in sectors and scenarios where they can be sometimes singularly influential by dint of their "infrastructural power" (Broeders et al., 2025, p. 1).

This article addresses an important aspect of the transformation in multilateral governance that has been induced by geoeconomics, namely, the turn to informal governance initiatives. Highlighting the US' orchestration of seven informal, non-binding initiatives on cross-border data flows and digital trade, we demonstrate that the US' preference for informal governance has been influenced by its need to constrain Chinese capabilities, both from a national security as well as digital economy perspective.

By examining the geoeconomic roots of the US' turn toward informal data governance agreements, we contribute to contemporary theoretical debates on economic statecraft, and highlight a less explored theme of cross-border data governance.

We contribute in four ways to the burgeoning literature in international relations and international law on geoeconomics. Firstly, by examining a crucial factor shaping informality in major cross-border data governance initiatives, we hope to foreground an important development in economic statecraft, one that is increasingly reflected in contemporary international relations and international law scholarship. The study of coercive economic measures has focused traditionally on formal, multilateral efforts such as sanctions (McLean, 2025), a reflection of their use by Western countries either through formal international commitments or domestic legislation. While scholarship on informal geoeconomic measures is rising, it is skewed toward the use of coercion by China and authoritarian states (Cho, 2021; Lim & Ferguson, 2022). As one scholar notes, "we have no account of the logics of these alternative [informal] approaches or how they affect outcomes" (Ferguson, 2022, p. 3).

Scholarly attention has increasingly turned towards global infrastructures (Bueger et al., 2023), specifically evaluating how ownership or control of critical material resources allows states to shape geoeconomic outcomes (Abels, 2024; Chen & Evers, 2023) through coercive statecraft (Farrell & Newman, 2019; Schindler et al., 2024). Informal governance has played a key role in facilitating the "infrastructural turn" in international relations (Broeders et al., 2025). Diplomatic efforts by states to "derisk" their economies from supply chain-based dependencies and sanction the use of infrastructures have taken the form of informal initiatives (Du, 2024). However, the impact of such initiatives is understudied in the literature.

International law scholarship has also begun to analyse how multilateral rules and regimes are evolving in response to geoeconomic statecraft (Cohen, 2025). Although international law scholarship on informal, non-binding agreements has burgeoned in recent years (Broude & Shereshevsky, 2021; Pauwelyn et al., 2012), the state of the art on geoeconomics and international law has centered on cooperation or competition through formal rules and institutions (Moraes, 2024). As multilateralism becomes more "selective" in times of Great Power competition, it is essential to understand which domains of economic

activity are likely to see rules-based cooperation, and how "like-minded" countries shape those rules (Roberts et al., 2019).

International law scholars have pointed to the emergence of bilateral and plurilateral agreements in international trade as indicative of this shift towards selective multilateralism (Dimitropoulos et al., 2025). These agreements are, however, characterized not only by like-minded coalitions but also reflect a "spectrum of bindingness" (Claussen, 2022). Some plurilateral agreements are altogether informal and non-binding. In recent years, however, it has become difficult to separate non-binding aspects of some plurilateral agreements from their formal commitments and, in other cases, discern their status in international law. The bottom line is that even like-minded countries, especially Western states with an established preference for formal trade arrangements, pursue informal governance mechanisms as a viable tool of economic statecraft.

Secondly, and on a related note, our study of informal data governance initiatives emphasizes the evolving strategy of the US towards geoeconomic measures. As noted previously, the literature on coercive economic statecraft has tended to focus on how the US leverages, through formal channels, its strategic position as a nodal state on global networks and infrastructures (Chen & Evers, 2023; Farrell & Newman, 2023). While its "institutional capacity" (Farrell & Newman, 2019)—generally understood as the regulatory capacity and expertise within a state to execute coercive measures—has been highlighted, less attention has been paid to the form of American diplomacy that sets the stage for economic statecraft.

The reality is that the US has been relying increasingly on informal agreements in global governance. Across domains and notably in sensitive matters of geopolitics and international security, the US has championed the adoption of political, non-binding agreements in recent years (Bradley et al., 2023). The US' turn towards informality is arguably owed partially to domestic political gridlock. It is challenging for any American president to secure treaty ratification in the US Congress today. As we demonstrate in this article, the flexibility that informal initiatives provide to the US and its coalition partners is an equally pertinent consideration for the executive use of statutory power.

Thirdly, our analysis of informal US data governance initiatives also contributes to the literature on how technology is shaping the "geoeconomic order" (Roberts et al., 2019), including through shoring up domestic industrial policy measures (Zhang, 2024). Coercive economic measures often present a major challenge for companies that have business operations around the world and are critically dependent on global supply chains (Gjesvik, 2023; Moraes & Wigell, 2022).

Finally, our article joins growing legal and international relations scholarship on global data governance, which includes literature both on digital trade and cross-border data flows. While recognizing the turn to informality in digital trade agreements (Burri & Polanco, 2020; Claussen, 2022), the literature on digital trade in general and cross-border data flows in particular has mainly focused on formal multilateral and plurilateral trade agreements (Burri, 2021; Dimitropoulos et al., 2025; Sen, 2018). The international relations scholarship on digital trade also looks at the approaches of specific countries or regional blocs on formal trade agreements, and has yet to study drivers of informality (Borgogno & Zangrandi, 2024; He & Zeng, 2024). Analysis of "regulatory autonomy" (Burri & Kugler, 2024) as a national policy priority has largely focused on exceptions to formal trade commitments based on public policy or security interests (Peng,

2023). To be sure, scholars have begun to acknowledge (Bradford, 2023) the possibilities and promise of informal coalitions between like-minded countries. (Goodman & Roberts, 2021; Mishra, 2024; Rasser, 2021).

Our banner finding, that the US has withdrawn from binding commitments and turned to informal data initiatives to enhance its own regulatory flexibility against China and induce greater international support for geoeconomic measures, sits well with the international law and international relations scholarship on informal governance (Abbott & Biersteker, 2024; Westerwinter et al., 2021). A nascent but discernible trend toward ad hoc initiatives is evident in the international security domain, reflecting the difficulties of forging formal cooperation in sensitive areas (Reykers et al., 2023). As we highlight in Section 4, there are admittedly several factors driving the turn towards informality in global governance: Some of them apply to the US case as well. Inequities presented by the Washington Consensus and the global economic order—specifically, the perceived marginalization by the government of consumer and labor rights as well as small business priorities in favor of monopolistic interests—have triggered a backlash among influential political constituencies within the US (Bowen & Broz, 2022). The US' skepticism of the WTO has been further entrenched by a bipartisan understanding that the multilateral trading system has enabled other countries, especially China, to engage in unfair practices that have harmed US economic interests (Chow, 2024). One way of addressing deglobalizing and protectionist impulses that have buffeted the US is arguably through softer international commitments that give the government room to calibrate domestic industrial and consumer policy (Schropp, 2024). Such arrangements may also offer increasing marginal returns or reduced incentives for states to venture into formal cooperation (Fioretos, 2019) or may simply be internalized by states as an established way of advancing global governance (Sukumar et al., 2024).

In any event, it is neither easy nor practical to entirely separate issues such as protectionism or fair trade from the geoeconomic aspects of US' China policy, given that China has been a direct beneficiary of technology, capital, and job outflows from the US. The perceived security threats posed by China "align seamlessly" (Kürzdörfer, 2025, p. 2) with the securitization of trade policy. US geoeconomic rhetoric is often framed in terms of "market-distorting effects" (Kürzdörfer, 2025, p. 3). The country's embrace of "minilateralism" (Richey & Guseinova, 2024; Wuthnow, 2018) suggests that it will continue to pursue many informal initiatives "in parallel" across complex and interlinked domains such as cyber governance, given the need to ensure redundancies (Brosig et al., 2025, p. 18). Cross-border data flows are only one component of broader digital trade and economic initiatives, including those highlighted in this article. Some informal initiatives are likely to prioritize particular issues or agendas over others, depending on their composition, objectives, and historical circumstances. Nonetheless, our finding that geoeconomic considerations have shaped the US' approach to informal data governance initiatives invites attention from international relations and international law scholars to the evolving nature and tools of economic statecraft.

3. About Turn: The US Embrace of Informal Governance for Cross-Border Data Flows

Since the inception of the World Wide Web, and its global adoption in the 1990s, the US has promoted the free flow of data through online networks (Cochetti, 2024). Beginning that decade, the US also became a key proponent of WTO negotiations on e-commerce, defined as the "production, distribution, marketing, sale or delivery of goods and services by electronic means" (WTO, 1998). From the earliest WTO ministerial meetings on this subject, the US emphasized "liberalization, open competition and universal access" through binding trade agreements (Delegation of the USA to the WTO, 1999, p. 2). In the decades that followed,

the protection of unrestricted cross-border flows through WTO agreements remained a policy priority for the US (Delegation of the USA to the WTO, 1999, 2014, 2016, 2019). "Many countries have enacted rules that put a chokehold on the free flow of information," and it was important to develop "appropriately crafted trade rules [that] protected the movement of data," a 2016 US statement noted (Delegation of the USA to the WTO, 2016, p. 2). The weight of evidence from WTO negotiations clearly suggests that the US favored formal, binding commitments against data localization until the latter half of the previous decade. Section 3.1 examines the US' withdrawal of support from existing formal mechanisms on cross-border data governance. Section 3.2 then highlights its growing engagement with informal initiatives, both new and ongoing, with the aim of developing coalitions around "trusted data flows."

3.1. US' Withdrawal From the WTO and the IPEF Agenda on Digital Trade

The US' position on cross-border data flows shifted abruptly in 2023 when it withdrew its proposals prohibiting data localization from the WTO's JI. The JI is an effort by some WTO members to "initiate exploratory work together toward future WTO negotiations" on e-commerce (WTO, 2017). It was incubated by the US and 70 other countries at the 11th WTO Ministerial Conference in 2017, following the failure of the WTO's Work Programme on Electronic Commerce. The WTO's Work Programme had been the sole multilateral negotiating forum on digital trade rules from 1998 to 2017. Any plurilateral agreement (Dimitropoulos et al., 2025) developed by the JI would be binding on the countries involved in the initiative (Basu, 2021). In December 2020, the JI took its first major stride towards a binding agreement by circulating a Consolidated Negotiating Text titled "WTO Electronic Commerce Negotiations." This draft laid out restrictions on states against computing facilities as well as the storage and processing of data (WTO, 2020). The US actively participated in the JI negotiations from 2017 to 2024 and endorsed proposals promoting the free flow of data.

The US continues to participate in the JI along with 88 other WTO members, including China. It is evident that the withdrawal of support for provisions on data localization was not a stopgap maneuver, but rather a broader recalibration of the US' position on cross-border data flows. In July 2024, the JI at the WTO released a "stabilized text" that did not include any references to cross-border data flows or data processing. Nevertheless, the US did not endorse the text, stating that it fell short concerning the "essential security exception" (US Mission Geneva, 2024). The "essential security exception" is a well-known "self-judging" provision in trade and investment law, which, when invoked, enables a member to justify any trade-restrictive domestic measure on the broad ground of security interests (Pinchis-Paulsen, 2020).

The view that the US has retreated from formal arrangements on cross-border data flows is supported by its withdrawal from the IPEF in November 2023. The IPEF announcement marked an even sharper shift in US policy, not least because it was a framework that the US had itself championed since its launch in May 2022 (Forough, 2022). Then-USTR Katherine Tai had previously stated that the trade pillar of the IPEF would "address issues in the digital economy that will help build…standards on cross-border data flows and data localizations" (USTR, 2022). The IPEF was designed as a non-binding framework, and even after its withdrawal, the US continues to participate in it. Yet, as we demonstrate in the next section, evidence indicates that the US' withdrawal was prompted by concerns that IPEF commitments, especially on digital trade, would become binding over time.

3.2. Advancing Informal Data Governance Initiatives

Even as it retreated from binding commitments on cross-border data flows, the US has stepped up its engagement with informal initiatives and framework agreements on data governance. In May 2024, the US Department of State released its International Cyberspace & Digital Policy Strategy, which specifically highlighted seven informal initiatives and notably omitted the WTO on matters relating to digital trade and data flows (US Department of State, 2024). Although the withdrawal of support for data-related provisions at the WTO was led by the USTR, the evident prioritization of informal initiatives by the State Department suggests that US government agencies were in sync. These informal initiatives, as noted previously, were framed by the US State Department as part of its overall attempt to foster "digital solidarity" (US Department of State, 2024, p. 1). Digital solidarity connotes a "willingness to work together on shared goals, to help partners build capacity, and to provide mutual support" (US Department of State, 2024, p. 1). Operationalizing digital solidarity also involves "developing shared mechanisms for…trusted cross-border flows" (US Department of State, 2024, p. 28). There is a strong geopolitical element to this concept, girded as it is by the need to keep digital networks and infrastructure (including subsea cables and cloud services) secure and resilient from adversaries such as China. Equally, it has a critical geoeconomic component. The US is orchestrating agreements that can reduce the world's dependence on Chinese digital technologies, while assuring allies and partners that US networks and infrastructure will remain open to cross-border data flows and technology sharing (Fang & Hwang, 2024).

In the remainder of this section, we introduce and offer an overview of these informal initiatives and explain them in turn. Although the Quad, the DTAT, and APEP do not explicitly address cross-border data flows, these initiatives—alongside the G7, EU–US TTC, and OECD initiatives—are integral to digital trade. There is, however, a risk and potential fallacy in retroactively applying the State Department's formulation of "digital solidarity" to informal data governance and digital trade initiatives that were inked five years ago. While we acknowledge this risk, the timeline we present establishes that these informal international initiatives emerged in lockstep with domestic policies that explicitly addressed geoeconomic considerations. "Digital solidarity" can thus be better understood as a diplomatic effort to coherently address the relationship between seemingly protectionist domestic measures and international coalition-building around data flows. "Legitimate concerns about data privacy can be addressed through protective mechanisms that follow the data while at the same time facilitate cross-border data flows," notes the strategy, specifically highlighting this as a "line of effort" to "reinforce" digital solidarity (US Department of State, 2024, p. 29).

The G7, comprising the world's advanced economies and leading liberal democracies, is arguably among the first informal initiatives to develop an agenda on cross-border data flows. What is notable here is not the fact that the G7 is an informal initiative—it always has been—but that the US has steered the issue of cross-border data flows into the G7 agenda as a geoeconomic concern. G7 ministerial declarations and leaders' statements have increasingly referenced "Data Free Flow with Trust" (DFFT), a concept promoted by Japan that was first introduced at the 2019 Osaka G20 summit. In its original formulation, DFFT emphasized the importance of seamless data flows across the internet while also acknowledging the importance of privacy and security of sensitive information held across countries. DFFT was specifically envisioned as a pillar of future digital trade rules, particularly at the WTO. The premise was that regulatory concerns about cybersecurity and privacy could be addressed fairly and legitimately through formal trade regimes, without risking the global datasphere splintering into multiple domestic jurisdictions (Dale & Aizawa, 2024). In this vein, the 2021

Cornwall G7 summit produced a DFFT Roadmap (G7 Digital and Technology Track, 2021). Among other priorities, this roadmap sought and successfully incubated greater coordination among G7 Data Protection and Privacy Authorities (2022, 2023, 2024) along with alternate policy responses to data localization.

The 2022 G7 summit in Elmau linked DFFT to the objective of "advancing" the WTO JI negotiations on data flows (G7, 2022). However, DFFT soon evolved into a tool of geoeconomic statecraft within the G7 framework. At the 2023 G7 summit in Hiroshima, member states agreed to facilitate "trustworthy cross-border data flows" that preserved governments' ability to "address legitimate public interest" (Ministry of Foreign Affairs, 2023). With its greater emphasis on "trust" rather than "free flows," the 2023 G7 language on cross-border data governance was notably more qualified than its previous iterations. Driving this transformation was the growing US concern that China was leveraging global data flows to gain both economic and national security advantages. "Policymakers admit (behind closed doors) that DFFT (now) is largely defined not by what it is for, but by what it is against: China," noted one commentator following the Hiroshima summit (Cory, 2023). It is crucial to note that the Hiroshima communiqué was released only days before the USTR withdrew data localization provisions from the WTO JI negotiations.

The TTC, established between the US and the EU in June 2021, is another key forum for coordinating digital economy and trade issues. At its first meeting in Pittsburgh, the TTC created a Data Governance and Technology Platforms Working Group to "exchange information and views regarding current and future regulations [with] a goal of effectively addressing shared concerns, while respecting the full regulatory autonomy of the European Union and the United States" (EU–US Trade and Technology Council, 2021). The TTC remains an important coordination mechanism for the US, particularly in light of the divergences between the EU's and the US' approaches to privacy and the legal complications they have posed for cross-border data flows. In both 2016 and 2020, the European Court of Justice invalidated mechanisms enabling the free flow of data from the EU to the US, citing insufficient safeguards under US law for the data of EU citizens (Court of Justice of the European Union, 2020). In response to the 2020 "Schrems II" judgment, President Joe Biden issued an Executive Order titled "Enhancing Safeguards for United States Signal Intelligence Activities" (Executive Office of the President, 2022). The order specified legitimate objectives for data collection and prioritized targeted collection over mass surveillance. These policy measures, alongside additional judicial safeguards, were deemed adequate by the EU, paving the way for the Transatlantic Data Privacy Framework, which restored unencumbered data flows to the US. While the TTC was not directly responsible for developing the Framework, it played an important role in harmonizing "regulatory cultures" in the EU and US (Burwell & Rodríguez, 2023). Both the TTC and the Transatlantic Data Privacy Framework are informal, bilateral frameworks that, at the time of writing, are bilateral in scope and do not focus on China.

The OECD has also emerged as an important forum for informal frameworks and principles on cross-border data flows. The US played a key role in negotiating the OECD's Declaration on Government Access to Personal Data, which affirmed the organization's commitment to DFFT principles. The OECD Declaration identified seven common principles regarding government access to privately held data, such as having a legal basis for collection, prior approvals, targeting personal data for legitimate aims, and proper data handling (OECD, 2022). While it did not name any state in particular, the declaration specifically called on OECD members to "take into account a destination country's effective implementation of the principles as a positive contribution towards facilitating transborder data flows" (OECD, 2022).

The other informal initiatives highlighted in the 2024 US International Cyberspace & Digital Policy Strategy do not, at the time of writing, have a defined program on digital trade or data flows. The Quad is a partnership between the US, Australia, Japan, and India to jointly tackle critical issues impacting the Indo-Pacific, including climate protection, health policy, and maritime security. Originally set up in 2004 to coordinate relief efforts following the Indian Ocean tsunami, the Quad was revived in 2017, arguably aimed at "checking and containing China in Asia" (Papa & Han, 2025). The Quad has recently seen a "growing tech focus" (Rajagopalan, 2022), spurring cooperation on technical standards, 5G deployment, cybersecurity, ICT supply chains, and artificial intelligence. These efforts are driven by informal agreements on technology design, development, and governance (Ministry of External Affairs, 2021). The Digital Transformation with Africa initiative and the Americas Partnership for Economic Prosperity are more recent initiatives aimed at strengthening digital environments through trusted and resilient supply chains across Africa and Latin America.

4. The Geoeconomic Drivers of Informal US-Led Initiatives

From this overview of US diplomacy on data governance and cybersecurity, two conclusions emerge: first, that the US has exhibited a strong preference in recent years towards informal initiatives, eschewing formal commitments on freer cross-border data flows in particular, and second, in at least a few of these initiatives, its diplomatic overtures are animated by concerns around China. In some cases, such as the DFFT concept and the Quad initiative, the economic security threats presented by China to US interests have been spelled out clearly. In other instances, the link is not immediately apparent.

The objective of this section is to trace in greater detail the geoeconomic considerations underlying the US' turn to informal data governance initiatives. This section proceeds in three parts. Section 4.1 highlights the increased recognition among Washington DC policymakers of the threats posed by data collection by Chinese actors and by data flows to mainland China. Section 4.2 examines domestic policy measures undertaken by various US government agencies to mitigate the Chinese threat to data security. Section 4.3 focuses on statements by leading US policymakers acknowledging the need for coalition-building to tackle the China threat.

The informal initiatives reviewed in Section 3 allow the US to develop coalitions of states that share similar economic and national security concerns around China. Indeed, as talk of coalition-building reached a crescendo in 2024, these initiatives were subsumed under the diplomatic umbrella of "digital solidarity" by the US State Department, giving them an explicitly geoeconomic hue.

The timeline illustrated in Table 1 details how coalition-building around informal international initiatives was chronologically advanced in lockstep with high-level statements and key domestic policies by the US. Figure 1 illustrates our banner finding, that the shift away from formality and the incubation of domestic policy measures (right of figure) proceeded in parallel with the articulation and pursuit of informal coalition-building by US policy-makers (left of figure).

Table 1. Chronicling the US shift to informal data governance initiatives.

Date	Event
1998–2023	US backs formal proposals at WTO restricting data localization measures
June 2019	Osaka Track (DFFT) championed by Japan at the Osaka G20
June 2020	USMCA (with firm commitments against data localization) enters into force
2021 onward	G7 "Cornwall Consensus" acknowledges DFFT
June 2021	EU–US TTC set up, Pittsburgh working group acknowledges need to work on data flows
2021	Declassified National Intelligence Council report identifying the misuse of digital tools by authoritarian states
2022	The 2022 National Security Strategy acknowledges the use of technology supply chains to spread authoritarianism
December 2022	The US is a key negotiator in the OECD Government Declaration on Access to Data, affirming its commitment to DFFT
January 2023	Civil society exerts pressure on Katherine Tai to withdraw from IPEF
April 2023	NSA Jake Sullivan's speech at Brookings recognizing the need for new trade tools to counter China
May 2023	G7 Hiroshima Leaders' Communiqué explicitly acknowledges DFFT and "trusted" data flows
October 2023	US withdraws support for provisions on data flows from JI
November 2023	US withdraws support for data-related proposals at IPEF
January 16, 2024	NSA Sullivan at the World Economic Forum (WEF) stresses the need for US to bring together countries and companies to set standards (coalition-building)
January 30, 2024	Gina Raimondo and Margrethe Vestager at the Atlantic Council highlight transatlantic cooperation (coalition-building)
February 2024	US Executive Order on data brokers
February 2024	Katherine Tai remarks at the Council on Foreign Relations explicitly linking trade withdrawals to data brokers
June 2024	Katherine Tai remarks at the Atlantic Council referencing the Executive Order on data brokers
March 2024	Bipartisan legislation compelling ByteDance to sell off TikTok to a US-based company or be banned
September 2024	Notification for Proposed Rule-Making on Electric Vehicles addressing data security threats in Chinese electric vehicles
October 2024	NSA Sullivan at Brookings emphasizes the need to use "modern trade tools" (Sullivan,2024b) including markets based on standards and sector-specific trade agreements
May 2024	US International Cyberspace & Digital Policy Strategy, noting informal mechanisms and digital solidarity released by the State Department, explicitly mentions informal arrangements for furthering digital trade (does not mention WTO)
June 2024	G7 Communiqué acknowledging DFFT and trusted data flows

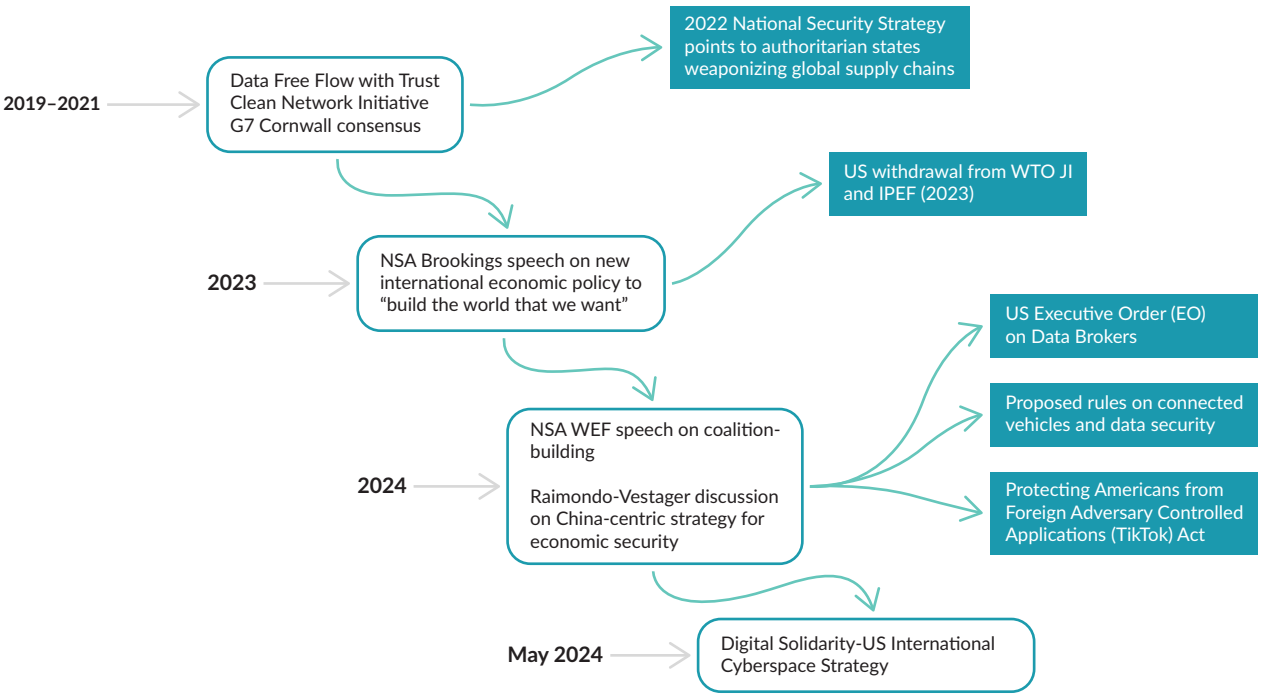


Figure 1. Visualising policy-space and coalition-building.

4.1. The China Threat

Policymakers in the US are increasingly concerned about data flows to China, both from a national security and an economic security perspective (Harrell, 2025; Joel, 2023; Sullivan, 2024a). The broader backdrop to this concern is the rise of China as a competitor and the challenge it poses to US strategic interests and to the liberal international order (President of the United States of America, 2017, 2022; Sullivan, 2023a, 2023b).

The view that Chinese access to US data poses threats to national security is shared by all branches of the US government and across the political spectrum. Former National Security Council member and China expert Rush Doshi has outlined four key objectives of Chinese cyber operations: accessing American personal data for intelligence purposes, commercial espionage, stealing private communications of government officials, and positioning Chinese actors behind US networks in advance of wartime scenarios (Doshi, 2025). The 2022 National Security Strategy explicitly states that "strategic competitors cannot exploit foundational American and allied technologies, know-how, or data to undermine American and allied security" (President of the United States, 2022). A declassified US National Intelligence Council Report dated 2022 that was declassified in 2023 highlighted that "authoritarian states [are] using digital tools to conduct transnational repression against individual critics and diaspora communities to limit their influence over domestic audiences" (National Intelligence Council, 2023, p. 5). Harrell (2025) notes that while there is no evidence that Chinese private companies have helped orchestrate these attacks, the US government fears that they could be exploited in the future, thus necessitating restrictions on data flows. This ties into concerns that Chinese actors may be "pre-positioning" themselves in American networks or infrastructure in anticipation of conflict (Corera & Buchanan, 2025).

From an economic standpoint, the rapid rise and dominance of Chinese companies across emerging technology sectors, such as electric vehicles (EVs), unmanned aerial vehicles, digital platforms, and artificial intelligence, is a growing concern for US policymakers. US policymakers have publicly articulated apprehensions that Chinese dominance in these sensitive sectors and supply chains will not only undermine American competitiveness but also make countries vulnerable to "coercion" from Beijing (Sullivan, 2024a, 2024b).

Official correspondence retrieved via the US Freedom of Information Act reveals that leading civil society groups had cautioned the Office of the USTR, led by Katherine Tai, against binding digital trade commitments for economic security reasons. In a January 2023 email, veteran trade activist Lori Wallach requested Tai not to incorporate open data flows provisions in the IPEF (akin to those in the Comprehensive and Progressive Trans-Pacific Partnership or USMCA) for the following reason:

> IPEF countries have strong economic connections with China and some have agreements with open data flows obligations with China, [and therefore] the inclusion of the USMCA/TPP terms in IPEF would run afoul of national security-related limits on data flows to China. (US Chamber of Commerce, 2023)

Messaging from civil society groups that assail Big Tech's digital trade agenda for its anti-competitive and anti-consumer effects refers increasingly to the national security risks of open data flows, especially to China (Wallach, 2025).

USTR Tai has articulated similar security concerns in a *Financial Times* op-ed (Tai, 2024d): "In digital trade or other sectors, we must be clear-eyed that China is not just a trading partner, but is pursuing global dominance across key economic sectors." Drawing on both national and economic security concerns, Tai defended the US' withdrawal of support for data localization provisions from the WTO JI:

> The PRC's approach is one that is really informed by control, especially by the government, and possession….And what we know is data flows into China, it doesn't flow back out, and that all of that data, eventually, will either be in the possession of or be accessible to the state. (Tai, 2024a)

4.2. Space for Domestic Policy

Following its withdrawal of provisions relating to data localization at the WTO in November 2023, the US articulated domestic policies restricting the potential cross-border flow of American citizens' data. The scope and context of these policies indicate that they sought to specifically address concerns around Chinese access to US citizens' personal and sensitive data.

The first such policy was Executive Order 14117 titled "Preventing Access to Americans' Bulk Sensitive Personal Data and United States Government-Related Data by Countries of Concern," issued by President Biden in February 2024, just five months after the US withdrawal of support for proposals related to cross-border data flows from the WTO JI. The Executive Order directed other agencies of the US government to restrict sales of US persons' data to foreign entities "through data brokerages, third-party vendor agreements, employment agreements, investment agreements, or other such arrangements" (Executive Office of the President, 2024, p. 15422) when it posed a "particular and unacceptable risk" to US

national security (Sherman, 2024). The source of these threats was often "in whole or substantial part outside the United States," namely in the form of, the order noted, "countries of concern" securing access to Americans' bulk sensitive personal data or US government data through such foreign entities (Executive Office of the President, 2024,p.15421) Bulk data were not only used for espionage and cyber operations but also to "fuel the creation and refinement of AI" by competitors (Executive Office of the President, 2024, p. 15421). USTR Tai herself referred to the threat posed by data brokers on at least two separate occasions in 2024 (Tai, 2024a, 2024c).

A second policy measure focused on data security threats posed by Chinese technology in "connected" vehicles, i.e., automobiles equipped with "networked hardware with automotive software systems [designed] to communicate" via a range of wireless media (US Department of Commerce, 2024). This policy, first proposed by the US Department of Commerce nearly a year after the US withdrew its data-related proposals at the WTO in September 2024, mainly targeted Chinese hardware and software not only in EVs but also in internal combustion engine vehicles. Finalized in January 2025, just a week before President Biden left office (Shepardson, 2024), the policy was slated to take effect on March 17, 2025, under the incoming Trump administration ("BIS connected vehicles rule," 2025). US officials have identified both economic and national security concerns over permitting Chinese vendors to test, develop, and deploy technology in commercial vehicles. The potential transfer of customer data and critical infrastructure information, such as positioning and metrics of energy grids, to Chinese manufacturers raised fears of espionage, pre-positioning, and economic competitiveness, officials have said (Shepardson, 2024). Notably, during the rulemaking process, the US Department of Commerce explicitly acknowledged that this policy was driven more by geoeconomic goals than by trade concerns (Shepardson et al., 2024). Once again, the US withdrawal of support for data localization provisions provided executive agencies the flexibility needed to restrict data flows to China and Chinese vendors.

A final policy instrument in this vein is the law titled "Protecting Americans from Foreign Adversary Controlled Applications Act (H.R. 7521)," passed by the US Congress on March 13, 2024. The law requires the Chinese company ByteDance to sell its social media application, TikTok, to a US entity by January 2025 or face a nationwide ban (Lutkevich, 2025). This legislation is the latest in a series of measures the US has contemplated since 2020 to address concerns around the potential transfer of sensitive user data by TikTok to Chinese state agencies for espionage or influence operations (Lutkevich, 2025). In 2020, President Trump invoked emergency powers to block TikTok, and bipartisan consensus around restricting the application reached its peak in March 2023, when both the FBI and the Department of Justice launched investigations into allegations that the application had spied on US journalists (Chander, 2023). The 2024 legislation was upheld by the Supreme Court in January 2025 (*TikTok, Inc. v. Garland*, 2025). In its verdict, the Supreme Court concluded that "TikTok's scale and susceptibility to foreign adversary control, together with the vast swathes of sensitive data the platform collects, justify differential treatment to address the Government's national security concerns" (*TikTok, Inc. v. Garland*, 2025, p. 12).

A TikTok ban, or more specifically, restrictions on data flows from the app to China, may not necessarily have been the only trigger for US withdrawal from the digital trade agenda at the WTO and IPEF. Nevertheless, it is apparent that the withdrawal conferred flexibility not only on US executive agencies but also on the judiciary to set aside considerations of any international obligation that may have rendered domestic policy unlawful. Importantly, it also allowed US private actors, including content delivery networks (CDNs)—the

actual executioners of the TikTok ban—to stop serving TikTok content to American users. When the deadline for its sale had passed in January 2025, US CDNs limited the flow of TikTok data to users. Following "clarity and assurance" (Shepardson, 2025). from then President-elect Trump that US service providers will not face penalties for carrying its content, TikTok worked with CDNs to restore its services. When it came back online, however, TikTok content was served not by its parent company ByteDance's servers in the US, but by other CDNs such as Akamai. While this move may have been an effort by TikTok to guarantee that its data was not flowing out of US territory, it is also possible that US authorities may have sought such a concession as a condition for the platform's reinstatement. Such informal policy maneuvers would have been difficult to seek in the face of formal commitments opposing data localization.

4.3. Coalition-Building Through Informal Arrangements

At the World Economic Forum in Davos in January 2024, Jake Sullivan underscored US efforts to "bring together countries and companies to set high standards for emerging technologies and secure the trusted free flow of data" (Sullivan, 2024a). Months later, in October 2024, at the Brookings Institution, Sullivan suggestively extolled the benefits of informality, highlighting the value of using "modern trade tools to achieve [US] objectives" (Sullivan, 2024b). He specifically referred to "creating markets based on standards" rather than formal agreements, along with "sector-specific trade agreements" (Sullivan, 2024b). Katherine Tai (June 2024) and Gina Raimondo (January 2024) have similarly emphasized the importance of a "community of democracies" in cooperating on digital trade and jointly tackling the China challenge (Tai, 2024b, 2024c).

The US State Department's framing of "digital solidarity" in May 2024, which subsumes informal initiatives that the US had either orchestrated or actively participated in recently, reflects an explicit attempt to build such a coalition of democracies (Kapur, 2024). As we have previously noted, the US seeks "digital solidarity" with like-minded democracies to develop norms around cyber and data governance that can neutralize the economic security threat posed by its adversaries (Kapur, 2024). However, operationalizing "digital solidarity" coalitions—more precisely, the geoeconomic vision behind them—through formal agreements remains difficult for two reasons. First, G7 countries, particularly those in the EU, may be reluctant to sign free trade commitments with the US due to stark differences in domestic regulatory strategies. The US and EU continue to diverge significantly in their approaches to data protection, competition law, and online content moderation, with the US favoring a more laissez-faire model (Bradford, 2023). Second, US partners and allies may be unwilling to commit to binding agreements that restrict the flow of data to "countries of concern." European and Asian economies remain more open to, and dependent on, Chinese technologies, especially in sectors identified by the US as sensitive, such as EVs and unmanned aerial vehicles. Formal commitments could deter American partners from collective action. This is true not only for cross-border data but also for other critical technologies, such as semiconductors (Broeders et al., 2025).

Digital solidarity is arguably feasible only when commitments on cross-border data governance remain soft. This elevates the importance of new and ongoing informal initiatives for the US. Such initiatives can develop global norms around the "trustworthiness" of cross-border data flows, enabling the US and its coalition partners to support open data flows while simultaneously targeting data collection by Chinese private and state actors. Initiatives such as the G7 reflect an acknowledgment that coalition-building is essential to counter the national security threat posed by China, while others, such as the TTC, explore alignment in domestic regulatory strategies to sustain cooperation on data flows. As for spooking US partners with

binding commitments against China, the US has already demonstrated a willingness to orchestrate informal initiatives to assuage such concerns. To limit the export of advanced chips and lithographic equipment to China, the US has turned to informal and even secret export control arrangements with the Netherlands and Japan. If Dutch diplomacy following this deal is any indication (Satariano, 2025), informal agreements on cross-border data flows offer a broad normative template that permits the US and its partners to draw redlines around data transfer to Chinese entities, while acknowledging the benefits of working with Chinese interlocutors on digital technologies.

5. Conclusion: Informality Under Trump and Beyond

This article has highlighted how the US' turn to informal data governance initiatives has been significantly shaped by national security and economic security concerns around data flows to China. Between 2020 and 2024, domestic policies and public statements by high-level officials were articulated in lockstep with US diplomacy at these informal initiatives and withdrawal of support for formal provisions (some of which pertain to broader themes of digital trade and data governance) on cross-border data flows. In parallel, the US championed the concept of "trusted data flows"—i.e., the promotion of freer data flows exclusively between partners who are like-minded in their perception of China as a threat and strategic adversary in cyberspace. That concept was folded in May 2024 into the diplomatic umbrella of "digital solidarity."

Given that the period under review largely corresponds with the tenure of the Biden administration—though the US retreat from formal agreements predates Biden's term—an important question persists: why did the first Trump administration support freer data flow proposals under the JI? Moreover, now that President Trump has returned for a second term, will he continue his predecessor's policies? There are two explanations for the Trump administration's decision not to withdraw from the WTO JI during its first term. First, China only joined the JI in 2019, leaving the Trump administration relatively little time to formulate a comprehensive US response. Second, as Kilic (2025) notes in the context of digital trade, "2018 was a different era," because then "Trump was still new to the White House and Washington politics." By 2020, however, the Trump administration had begun orchestrating the first US-led informal initiatives aimed at dissuading states from relying on Chinese 5G vendors and equipment (US Department of State, n.d.). The "Clean Network" initiative and the Prague Proposals sought, among other objectives, to block Chinese actors from accessing US personal and sensitive data (US Department of State, n.d.). In many ways, the Trump administration's rhetoric around building a "coalition of trusted partners" for "clean" networks (US Department of State, n.d.) is mirrored in the Biden administration's concept of "digital solidarity." Officials instrumental to the Clean Network initiative later acknowledged that the first Trump administration's approach evolved from an initial "confrontational style" against China to support "good old-fashioned diplomacy" in its later years (Coy & Mathieson, 2020).

The second Trump administration too appears determined to check China's rise, and manage the national as well as economic security threats posed by Beijing. Geoeconomic measures, in this regard, are not likely to recede anytime soon. Even if Trump's supporters in Silicon Valley or other major technology companies would want firm commitments for cross-border flows of data, his administration will be wary of such flows being weaponized by Chinese actors. In the interim, therefore, we are likely to see mini-deals between the US and its allies promoting digital trade, with data flows ring-fenced from Chinese market players. In other words, it is reasonable to expect continuity rather than disruption in US policies towards informal data governance

initiatives. Trump's second term has also revealed tensions in transatlantic relations, casting doubt on whether many EU member states will fully endorse American initiatives, even if they share concerns about China. Still, geoeconomic compulsions persist for both the US and China, and informal data governance mechanisms, due to their flexibility and utility for coalition-building, will likely remain a tool of statecraft.

Acknowledgments

We would like to thank the editors of *Politics and Governance* as well as the two academic editors, Xuechen Chen and Xinchuchu Gao, for their support. We would also like to thank Shantanu Salgaonkar for designing Figure 1, and The Clean Copy for editing the draft.

Funding

Publication of this article in open access was made possible through the institutional membership agreement between Leiden University and Cogitatio Press.

Conflict of Interests

The authors declare no conflicts of interests.

LLMs Disclosure

While the text, cadence, and design concept of Figure 1 are entirely the authors' own, we wish to acknowledge the assistance of Notion AI in refining this image.

References

Abbott, K. W., & Biersteker, T. J. (Eds.). (2024). *Informal governance in world politics*. Cambridge University Press. https://doi.org/10.1017/9781009180528

Abels, J. (2024). Private infrastructure in geopolitical conflicts: The case of Starlink and the war in Ukraine. *European Journal of International Relations*, *30*(4), 842–866. https://doi.org/10.1177/13540661241260653

Aggarwal, V. K., & Reddie, A. W. (2021). Economic statecraft in the 21st century: Implications for the future of the global trade regime. *World Trade Review*, *20*(2), 137–151. https://doi.org/10.1017/S1474745620000049X

Baldwin, D. A., & Pape, R. A. (1998). Evaluating economic sanctions. *International Security*, *23*(2), 189–198. https://doi.org/10.2307/2539384

Basu, A. (2021, October 5). Can the WTO build consensus on digital trade? *Hinrich Foundation*. https://www.hinrichfoundation.com/research/article/digital/can-the-wto-build-consensus-on-digital-trade

BIS connected vehicles rule effective as of March 17, 2025. (2025, March 19). *Gibson Dunn*. https://www.gibsondunn.com/bis-connected-vehicles-rule-effective-as-of-march-17-2025

Blackwill, R. D., & Harris, J. M. (2016). *War by other means: Geoeconomics and statecraft*. Harvard University Press.

Blanchard, J.-M. F., & Ripsman, N. M. (1999). Asking the right question: When do economic sanctions work best? *Security Studies*, *9*(1/2), 219–253. https://doi.org/10.1080/09636419908429400

Borgogno, O., & Zangrandi, M. (2024). Chinese data governance and trade policy: From cyber sovereignty to the quest for digital hegemony? *Journal of Contemporary China*, *33*(148), 578–602. https://doi.org/10.1080/10670564.2023.2299961

Bowen, T. R., & Broz, J. L. (2022). The domestic political economy of the WTO crisis: Lessons for preserving multilateralism. *Global Perspectives*, *3*(1), Article 55655. https://doi.org/10.1525/gp.2022.55655

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Bradley, C., Goldsmith, J., & Hathaway, O. (2023). The rise of nonbinding international agreements: An empirical, comparative, and normative analysis. *University of Chicago Law Review*, *90*(5), Article 1. https://chicagounbound.uchicago.edu/uclrev/vol90/iss5/1

Broeders, D., Sukumar, A., Kello, M., & Andersen, L. H. (2025). Digital corporate autonomy: Geo-economics and corporate agency in conflict and competition. *Review of International Political Economy*, *32*(4), 1189–1213. https://doi.org/10.1080/09692290.2025.2468308

Brooks, R. A. (2002). Sanctions and regime type: What works, and when? *Security Studies*, *11*(4), 1–50. https://doi.org/10.1080/714005349

Brosig, M., Karlsrud, J., Maglia, C., & Reykers, Y. (2025). *The end of multilateralism as we know it? Assessing current trends in the international security*. NAVIGATOR. https://eunav.eu/wp-content/uploads/2025/03/D8.1-Working-paper-on-institutional-landscape-of-global-security-governance.pdf

Broude, T., & Shereshevsky, Y. (2021). Explaining the practical purchase of soft law: Competing and complementary behavior hypotheses. In H. G. Cohen & T. Meyer (Eds.), *International law as behavior* (pp. 98–127). Cambridge University Press. https://doi.org/10.1017/9781316979792.005

Bueger, C., Liebetrau, T., & Stockbruegger, J. (2023). Theorizing infrastructures in global politics. *International Studies Quarterly*, *67*(4), Article sqad101. https://doi.org/10.1093/isq/sqad101

Burri, M. (Ed.). (2021). *Big data and global trade law*. Cambridge University Press.

Burri, M., & Kugler, K. (2024). Regulatory autonomy in digital trade agreements. *Journal of International Economic Law*, *27*(3), 397–423. https://doi.org/10.1093/jiel/jgae025

Burri, M., & Polanco, R. (2020). Digital trade provisions in preferential trade agreements: Introducing a new dataset. *Journal of International Economic Law*, *23*(1), 187–220. https://doi.org/10.1093/jiel/jgz044

Burwell, F., & Rodríguez, A. G. (2023, April 20). The US–EU Trade and Technology Council: Assessing the record on data and technology issues. *Atlantic Council*. https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/us-eu-ttc-record-on-data-technology-issues

Chander, A. (2023). Trump v. TikTok. *Vanderbilt Journal of Transnational Law*, *55*(5), 1145–1188. https://scholarship.law.vanderbilt.edu/vjtl/vol55/iss5/2

Chen, L. S., & Evers, M. M. (2023). "Wars without gun smoke": Global supply chains, power transitions, and economic statecraft. *International Security*, *48*(2), 164–204. https://doi.org/10.1162/isec_a_00473

Cho, H. (2021). China's informal economic sanctions. *Analyses & Alternatives*, *5*(1), 25–57.

Chow, D. C. (2024). How the rise of China led the United States to wreck the World Trade Organization: A US perspective from a US scholar. *Manchester Journal of International Economic Law*, *21*(2), 105–121.

Claussen, K. (2022). Trade's mini-deals. *Virginia Journal of International Law*, *62*(2), 315–382.

Cochetti, R. (2024, February 29). For 25 years, the WTO has protected the "free flow of information" online—This year, that could change. *The Hill*. https://thehill.com/opinion/technology/4496916-for-25-years-the-wto-has-protected-the-free-flow-of-information-online-this-year-that-could-change

Cohen, H. G. (2025). *The international order, international law, and the definition of security*. SSRN. https://doi.org/10.2139/ssrn.5167227

Corera, J., & Buchanan, E. (2025, March 5). In case we forgot, Typhoon attacks remind us of China's cyber capability—and intent. *The Strategist*. https://www.aspistrategist.org.au/in-case-we-forgot-typhoon-attacks-remind-us-of-chinas-capability-and-intent

Cory, N. (2023, July 27). How the G7 can use "Data Free Flow with Trust" to build global data governance. *Information Technology & Innovation Foundation*. https://itif.org/publications/2023/07/27/how-g7-can-use-data-free-flow-with-trust-to-build-global-data-governance

Court of Justice of the European Union. (2020). *Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems. Request for a preliminary ruling from the High Court (Ireland)* (Case C-311/18, ECLI:EU:C:2020:559). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:62018CJ0311

Coy, P., & Mathieson, R. (2020, December 9). US policy on China may move "America First" to America & Co. *Bloomberg*. https://www.bloomberg.com/news/articles/2020-12-09/u-s-policy-against-china-america-first-is-becoming-america-and-others

Dale, J. G., & Aizawa, N. (2024). "Data Free Flow with Trust": Japan's struggle to integrate democracy and human rights into digital trade policy. *Frontiers in Sociology*, *9*, Article 1397528. https://doi.org/10.3389/fsoc.2024.1397528

Delegation of the USA to the WTO. (1999). *Submission by the United States* (WT/GC/16 G/C/2 S/C/7 IP/C/16 WT/COMTD/17). World Trade Organization. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=Q:/WT/COMTD/17.pdf&Open=True

Delegation of the USA to the WTO. (2014). *Communication by the United States* (S/C/W/359). World Trade Organization. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W359.pdf&Open=True

Delegation of the USA to the WTO. (2016). *Non-paper from the United States* (JOB/GC/94). World Trade Organization. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/Jobs/GC/94.pdf&Open=True

Delegation of the USA to the WTO. (2019). *The economic benefits of cross-border data flows.* (S/C/W/382). World Trade Organization. https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W382.pdf&Open=True

Dimitropoulos, G., Chen, R. C., & Chaisse, J. (2025). Plurilateralism: A new form of international economic ordering? *The Journal of World Investment & Trade*, *26*(1/2), 1–30. https://doi.org/10.1163/22119000-12340350

Doshi, R. (2025, March 5). Countering threats posed by the Chinese Communist Party to US national security. *Council on Foreign Relations*. https://www.cfr.org/report/countering-threats-posed-chinese-communist-party-us-national-security

Drezner, D. W. (2003). The hidden hand of economic coercion. *International Organization*, *57*(3), 643–659.

Drezner, D. W. (2024). Global economic sanctions. *Annual Review of Political Science*, *27*(1), 9–24. https://doi.org/10.1146/annurev-polisci-041322-032240

Du, M. (2024). International economic law in the era of Great Power rivalry. *Vanderbilt Journal of Transnational Law*, *57*(3), 723–794.

Escribà-Folch, A., & Wright, J. (2010). Dealing with tyranny: International sanctions and the survival of authoritarian rulers. *International Studies Quarterly*, *54*(2), 335–359. https://doi.org/10.1111/j.1468-2478.2010.00590.x

EU–US Trade and Technology Council. (2021, September 29). *Pittsburgh Statement* [Press release]. https://ec.europa.eu/commission/presscorner/api/files/attachment/870149/210929%20Pittsburgh%20Statement.pdf

Executive Office of the President. (2022). *Enhancing safeguards for United States signals intelligence activities* (Executive Order No. 14086). Federal Register. https://www.federalregister.gov/documents/2022/10/14/2022-22531/enhancing-safeguards-for-united-states-signals-intelligence-activities

Executive Office of the President. (2024). *Preventing access to Americans' bulk sensitive personal data and United States government-related data* (Executive Order No. 14117). Federal Register. https://www.federalregister.gov/documents/2024/03/01/2024-04573/preventing-access-to-americans-bulk-sensitive-personal-data-and-united-states-government-related

Fang, T., & Hwang, T. (2024, September 5). Digital solidarity in U.S. foreign policy. *New America*. https://www.newamerica.org/oti/reports/digital-solidarity-in-us-foreign-policy

Farrell, H., & Newman, A. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

Farrell, H., & Newman, A. (2023). *Underground empire: How America weaponized the world economy*. Henry Holt and Co.

Ferguson, V. A. (2022). Economic lawfare: The logic and dynamics of using law to exercise economic power. *International Studies Review*, *24*(3), Article viac032. https://doi.org/10.1093/isr/viac032

Fioretos, O. (2019). Minilateralism and informality in international monetary cooperation. *Review of International Political Economy*, *26*(6), 1136–1159.

Forough, M. (2022, May 26). America's pivot to Asia 2.0: The Indo-Pacific economic framework. *The Diplomat*. https://thediplomat.com/2022/05/americas-pivot-to-asia-2-0-the-indo-pacific-economic-framework

G7. (2022, May 11). *Ministerial declaration of digital ministers meeting* [Press release]. https://g7g20-documents.org/database/document/2022-g7-germany-ministerial-meetings-digital-economy-ministers-ministers-language-ministerial-declaration-digital-ministers-meeting

G7 Data Protection and Privacy Authorities. (2022, September 8). *Promoting Data Free Flow with Trust and knowledge sharing about the prospects for international data spaces* [Press release]. https://www.cnil.fr/sites/cnil/files/atoms/files/g7-communique-2022.pdf

G7 Data Protection and Privacy Authorities. (2023, June 21). *Working toward operationalizing Data Free Flow with Trust and intensifying regulatory cooperation* [Press release]. https://www.edps.europa.eu/system/files/2023-06/23-06-21_g7roundtable_202306_communique_en.pdf

G7 Data Protection and Privacy Authorities. (2024, October 11). *Privacy in the age of data* [Press release]. https://www.priv.gc.ca/en/opc-news/news-and-announcements/2024/communique-g7_241011

G7 Digital and Technology Track. (2021). *G7 roadmap for cooperation on data free flow with trust*: *Annex 2*.

Gjesvik, L. (2023). Private infrastructure in weaponized interdependence. *Review of International Political Economy*, *30*(2), 722–746. https://doi.org/10.1080/09692290.2022.2069145

Global Data Alliance. (2023). *Congressional statements on USTR's digital trade policy reversal*. https://globaldataalliance.org/wp-content/uploads/2023/11/11212023gdaustrcomp.pdf

Goodman, M. P., & Roberts, B. (2021, October 13). Toward T-12: Putting allied technology cooperation into practice. *Center for Strategic and International Studies*. https://www.csis.org/analysis/toward-t12-putting-allied-technology-cooperation-practice

Harrell, P. E. (2025). *Managing the risks of China's access to US data and control of software and connected technology*. Carnegie Endowment for International Peace. https://carnegie-production-assets.s3.amazonaws.com/static/files/Harrell_US-China%20Data%20Regulation.pdf

He, Y., & Zeng, K. (2024). China in global digital trade governance: Towards a development-oriented agenda? *International Affairs*, *100*(5), 2195–2215.

Joel, A. (2023, November 13). Trusted cross-border data flows: A national security priority. *Lawfare*. https://www.lawfaremedia.org/article/trusted-cross-border-data-flows-a-national-security-priority

Kapur, A. (2024, July 31). What is digital solidarity, and why does the US want it? *Foreign Policy*. https://foreignpolicy.com/2024/07/31/digital-solidarity-rsa-conference-blinken-speech

Kilic, B. (2025, January 27). On digital trade: Will Trump 2.0 continue to break from neoliberalism? *Centre for International Governance Innovation*. https://www.cigionline.org/articles/on-digital-trade-will-trump-20-continue-to-break-from-neoliberalism

Kirshner, J. (1997). The microfoundations of economic sanctions. *Security Studies*, *6*(3), 32–64. https://doi.org/10.1080/09636419708429314

Kürzdörfer, N. (2025). The dog that does not bark—Weaponised interdependence and digital trade at the World Trade Organization. *Review of International Political Economy*. Advance online publication. https://doi.org/10.1080/09692290.2025.2483371

Lawder, D. (2023, November 9). US suspends Indo-Pacific talks on key aspects of digital trade—Lawmakers. *Reuters*. https://www.reuters.com/business/finance/us-suspends-indo-pacific-talks-key-aspects-digital-trade-lawmakers-2023-11-08

Lim, D. J., & Ferguson, V. A. (2022). Informal economic sanctions: The political economy of Chinese coercion during the THAAD dispute. *Review of International Political Economy*, *29*(5), 1525–1548. https://doi.org/10.1080/09692290.2021.1918746

Lutkevich, B. (2025, July 11). TikTok bans explained: Everything you need to know. *TechTarget*. https://www.techtarget.com/whatis/feature/TikTok-bans-explained-Everything-you-need-to-know

Making NAFTA worse: Giveaways for Big Tech in the USMCA. (2025, March 9). *Public Citizen*. https://www.citizen.org/article/making-nafta-worse-giveaways-for-big-tech

Malkin, A., & He, T. (2024). The geoeconomics of global semiconductor value chains: Extraterritoriality and the US–China technology rivalry. *Review of International Political Economy*, *31*(2), 674–699. https://doi.org/10.1080/09692290.2023.2245404

Mastanduno, M. (1999). Economic statecraft, interdependence, and national security: Agendas for research. *Security Studies*, *9*(1/2), 288–316. https://doi.org/10.1080/09636419908429402

McLean, E. V. (2025). Economic coercion. In J. C. W. Pevehouse & L. Seabrooke (Eds.), *The Oxford handbook of international political economy* (pp. 254–275). Oxford University Press.

Ministry of External Affairs. (2021, September 24). *Quad principles on technology design, development, governance, and use* [Press release]. https://www.mea.gov.in/bilateral-documents.htm?dtl/34323/Quad_Principles_on_Technology_Design_Development_Governance_and_Use

Ministry of Foreign Affairs. (2023, May 20). *G7 Hiroshima leaders' communiqué* [Press release]. https://www.mofa.go.jp/policy/economy/summit/hiroshima23/documents/pdf/Leaders_Communique_01_en.pdf

Mishra, N. (2024). *International trade law and global data governance: Aligning perspectives and practices*. Hart Publishing.

Moraes, H. C. (2024). The changing logic of international economic law. *UCLA Journal of International Law and Foreign Affairs*, *27*(2). https://escholarship.org/uc/item/11b2525f

Moraes, H. C., & Wigell, M. (2022). Balancing dependence: The quest for autonomy and the rise of corporate geoeconomics. In M. Babić, A. D. Dixon, & I. T. Liu (Eds.), *The political economy of geoeconomics: Europe in a changing world* (pp. 29–55). Palgrave Macmillan. https://doi.org/10.1007/978-3-031-01968-5_2

Mueller, A. (2025). *One step forward, two steps back: The United States' new direction on digital trade*. SSRN. https://doi.org/10.2139/ssrn.5028333

National Intelligence Council. (2023). *Digital repression growing globally, threatening freedoms* (NICA 2022-22810). Office of the Director of National Intelligence. https://www.dni.gov/files/ODNI/documents/assessments/NIC-Declassified-Assessment-Digital-Repression-Growing-April2023.pdf

Norris, W. J. (2016). *Chinese economic statecraft: Commercial actors, grand strategy, and state control*. Cornell University Press.

Organisation for Economic Cooperation and Development. (2022). *Declaration on government access to personal data held by private sector entities*. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0487

Papa, M., & Han, Z. (2025). The evolution of soft balancing in informal institutions: The case of BRICS. *International Affairs*, *101*(1), 73–95. https://doi.org/10.1093/ia/iiae278

Pape, R. A. (1997). Why economic sanctions do not work. *International Security*, *22*(2), 90–136. https://doi.org/10.2307/2539368

Pauwelyn, J., Wessel, R., & Wouters, J. (Eds.). (2012). *Informal international lawmaking*. Oxford University Press.

Pearson, M. M., Rithmire, M., & Tsai, K. S. (2022). China's party-state capitalism and international backlash: From interdependence to insecurity. *International Security*, *47*(2), 135–176. https://doi.org/10.1162/isec_a_00447

Peng, S. (2023). Digital economy and national security: Contextualizing cybersecurity-related exceptions, *AJIL Unbound*, *117*, 122–127. https://doi.org/10.1017/aju.2023.18

Pinchis-Paulsen, M. (2020). Trade multilateralism and U.S. national security: The making of the GATT security exceptions. *Michigan Journal of International Law*, *41*(1), 109–194. https://doi.org/10.36642/mjil.41.1.trade

President of the United States of America. (2017). *National Security Strategy of the United States of America*. The White House. https://trumpwhitehouse.archives.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf

President of the United States of America. (2022). *National Security Strategy of the United States of America*. The White House. https://bidenwhitehouse.archives.gov/wp-content/uploads/2022/11/8-November-Combined-PDF-for-Upload.pdf

Rajagopalan, R. P. (2022, July 9). The growing tech focus of the Quad. *The Diplomat*. https://thediplomat.com/2022/07/the-growing-tech-focus-of-the-quad

Rasser, M. (2021, October 19). The case for an alliance of techno-democracies. *Center for a New American Security*. https://www.cnas.org/publications/commentary/the-case-for-an-alliance-of-techno-democracies

Reykers, Y., Karlsrud, J., Brosig, M., Hofmann, S. C., Maglia, C., & Rieker, P. (2023). Ad hoc coalitions in global governance: Short-notice, task- and time-specific cooperation. *International Affairs*, *99*(2), 727–745. https://doi.org/10.1093/ia/iiac319

Richey, M., & Guseinova, O. (2024). Disputed geometries of great power politics: US–China perspectives on minilateralism. *Australian Journal of International Affairs*, *78*(6), 828–847.

Roberts, A., Moraes, H. C., & Ferguson, V. (2019). Toward a geoeconomic order in international trade and investment. *Journal of International Economic Law*, *22*(4), 655–676. https://doi.org/10.1093/jiel/jgz036

Satariano, A. (2025, June 5). How the maker of the "most complex machine humans ever created" is navigating trade fights. *The New York Times*. https://www.nytimes.com/2025/06/05/technology/asml-chips-tariffs-trade.html

Schindler, S., Alami, I., DiCarlo, J., Jepson, N., Rolf, S., Bayırbağ, M. K., Cyuzuzo, L., DeBoom, M., Farahani, A. F., Liu, I. T., McNicol, H., Miao, J. T., Nock, P., Teri, G., Vila Seoane, M. F., Ward, K., Zajontz, T., & Zhao, Y. (2024). The Second Cold War: US-China competition for centrality in infrastructure, digital, production, and finance networks. *Geopolitics*, *29*(4), 1083–1120. https://doi.org/10.1080/14650045.2023.2253432

Schropp, S. A. (2024). Biden's international trade policy: Déjà vu, again. *Intereconomics*, *59*(3), 183–184.

Sen, N. (2018). Understanding the role of the WTO in international data flows: Taking the liberalization or the regulatory autonomy path? *Journal of International Economic Law*, *21*(2), 323–348. https://doi.org/10.1093/jiel/jgy021

Shepardson, D. (2024, September 23). Biden proposes banning Chinese vehicles, "connected car" technology from US roads. *Reuters*. https://www.reuters.com/business/autos-transportation/biden-proposes-banning-chinese-vehicles-us-roads-with-software-crackdown-2024-09-23

Shepardson, D. (2025, January 20). TikTok restores US service after Trump says 'We have to save it.'. *Reuters*. https://www.reuters.com/technology/tiktok-goes-dark-us-users-trump-says-save-tiktok-2025-01-19

Shepardson, D., Eckert, N., & Roy, R. (2024, September 24). Biden's car-tech ban is a powerful new weapon against Chinese EVs. *Reuters*. https://www.reuters.com/business/autos-transportation/bidens-car-tech-ban-is-powerful-new-weapon-against-chinese-evs-2024-09-24

Sherman, J. (2024, October 22). Data brokers and threats to government employees. *Lawfare*. https://www.lawfaremedia.org/article/data-brokers-and-threats-to-government-employees

Sukumar, A., Broeders, D., & Kello, M. (2024). The pervasive informality of the international cybersecurity regime: Geopolitics, non-state actors and diplomacy. *Contemporary Security Policy*, *45*(1), 7–44. https://doi.org/10.1080/13523260.2023.2296739

Sullivan, J. (2023a). *Remarks by APNSA Jake Sullivan at the Brookings Institution* [Speech transcript]. The White House. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2024/10/23/remarks-by-apnsa-jake-sullivan-at-the-brookings-institution

Sullivan, J. (2023b). *Remarks by National Security Advisor Jake Sullivan on renewing American economic leadership at the Brookings Institution* [Speech transcript]. The White House. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2023/04/27/remarks-by-national-security-advisor-jake-sullivan-on-renewing-american-economic-leadership-at-the-brookings-institution

Sullivan, J. (2024a). *Remarks and Q&A by National Security Advisor Jake Sullivan at the 2024 World Economic Forum, Davos, Switzerland* [Speech transcript]. The White House. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2024/01/16/remarks-and-qa-by-national-security-advisor-jake-sullivan-at-the-2024-world-economic-forum-davos-switzerland/#:~:text=In%20an%20interdependent%20world%2C%20there's,trusted%20free%20flow%20of%20data

Sullivan, J. (2024b). *Remarks by APNSA Jake Sullivan on AI and national security* [Speech transcript]. The White House. https://bidenwhitehouse.archives.gov/briefing-room/speeches-remarks/2024/10/24/remarks-by-apnsa-jake-sullivan-on-ai-and-national-security

Tai, K. (2024a). *C. Peter McColough Series on International Economics with Katherine Tai* [Speech transcript]. Council on Foreign Relations. https://www.cfr.org/event/c-peter-mccolough-series-international-economics-katherine-tai-0

Tai, K. (2024b). *Gina Raimondo and Margrethe Vestager on transatlantic approaches to trade, AI, and China* [Speech transcript]. Atlantic Council. https://www.atlanticcouncil.org/commentary/transcript/gina-raimondo-and-margrethe-vestager-on-transatlantic-approaches-to-trade-ai-and-china

Tai, K. (2024c). *US Trade Representative Katherine Tai on modernizing the transatlantic partnership* [Speech transcript]. Atlantic Council. https://www.atlanticcouncil.org/commentary/transcript/us-trade-representative-katherine-tai-transatlantic-trade

Tai, K. (2024d, May 28). Trade must transform its role in the social contract. *Financial Times*. https://www.ft.com/content/91f22f38-6595-4b08-bebe-948c628fa736

Tallberg, J., Bäckstrand, K., Scholte, J. A., & Sommerer, T. (2023). *SNS Democracy Council 2023. Global governance: Fit for purpose?* SNS Förlag.

TikTok, Inc. v. Garland, No. 24-656 U.S. Supreme Court. (2025).

US Chamber of Commerce. (2023). *Extension of the USMCA/TPP "digital trade" rules that Big Tech Favors would undermine AI justice, privacy, competition, and worker rights policy*. https://www.uschamber.com/assets/documents/USTR-FOIA-Digital-Trade-Redacted-Documents.pdf

US Department of Commerce. (2024). *Securing the information and communications technology and services supply chain*. Federal Register. https://www.federalregister.gov/documents/2024/12/06/2024-28335/securing-the-information-and-communications-technology-and-services-supply-chain

US Department of State. (n.d.). *The Clean Network*. https://2017-2021.state.gov/the-clean-network/#:~:text=The%20Clean%20Network%20program%20is,as%20the%20Chinese%20Communist%20Party

US Department of State. (2024). *United States International Cyberspace & Digital Policy Strategy: Towards an innovative, secure and right-respecting digital future*. https://2021-2025.state.gov/wp-content/uploads/2024/07/United-States-International-Cyberspace-and-Digital-Strategy-FINAL-2024-05-15_508v03-Section-508-Accessible-7.18.2024.pdf

US Mission Geneva. (2024). *Statement by Ambassador María L. Pagán on the WTO E-Commerce Joint Statement Initiative*. https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative

US Trade Representative. (2022, May 23). *On-the-record press call remarks by Ambassador Katherine Tai on the launch of the Indo-Pacific Economic Framework* [Press release]. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2022/may/record-press-call-remarks-ambassador-katherine-tai-launch-indo-pacific-economic-framework

US Trade Representative. (2023, October 24). *USTR Statement on WTO e-commerce negotiations* [Press release]. https://ustr.gov/about-us/policy-offices/press-office/press-releases/2023/october/ustr-statement-wto-e-commerce-negotiations

Vabulas, F., & Snidal, D. (2013). Organization without delegation: Informal intergovernmental organizations (IIGOs) and the spectrum of intergovernmental arrangements. *The Review of International Organizations*, *8*(2), 193–220. https://doi.org/10.1007/s11558-012-9161-x

Wallach, L. (2025, March 17). The "digital trade" trap. *Compact Mag*. https://www.compactmag.com/article/the-digital-trade-trap

Westerwinter, O., Abbott, K. W., & Biersteker, T. (2021). Informal governance in world politics. *The Review of International Organizations*, *16*(1), 1–27. https://doi.org/10.1007/s11558-020-09382-1

Wong, A. (2023). China's economic statecraft: Lessons learned from Ukraine. *The Washington Quarterly*, *46*(1), 121–136. https://doi.org/10.1080/0163660X.2023.2188830

World Trade Organization. (1998). *Work Programme on Electronic Commerce* (WT/L/274). https://docs.wto.org/dol2fe/Pages/FE_Search/DDFDocuments/31348/T/WT/L/274.DOC

World Trade Organization. (2017). *Joint Statement on Electronic Commerce* (WT/MIN(17)/60). https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/WT/MIN17/60.pdf&Open=True

World Trade Organization. (2020). *WTO electronic commerce negotiations: Consolidated negotiating text—December 2020—Revision* (INF/ECOM/62/Rev.1). https://www.bilaterals.org/IMG/pdf/wto_plurilateral_ecommerce_draft_consolidated_text.pdf

Wuthnow, J. (2018). U.S. 'minilateralism' in Asia and China's responses: A new security dilemma? *Journal of Contemporary China*, *28*(115), 133–150. https://doi.org/10.1080/10670564.2018.1497916

Zeng, K., Wells, R., Gu, J., & Wilkins, A. (2022). Bilateral tensions, the trade war, and US–China trade relations. *Business and Politics*, *24*(4), 399–429.

Zhang, K. H. (2024). Geoeconomics of US–China tech rivalry and industrial policy. *Asia and the Global Economy*, *4*(2), Article 100098. https://doi.org/10.1016/j.aglobe.2024.100098

About the Authors

Arun Sukumar is an assistant professor of international relations at Ashoka University. He was previously an assistant professor (on permanent contract) at Leiden University, where he was also affiliated as a researcher with the Hague Program on International Cybersecurity.

Arindrajit Basu is a PHD candidate at the Institute of Security and Global Affairs, Leiden University and a non-resident fellow (Planetary Politics) in New America.

Politics and Governance
2025 • Volume 13 • Article 10413
https://doi.org/10.17645/pag.10413

cogitatio

ARTICLE

Open Access Journal

Adaptive Sovereignty: China's Evolving Legislative Framework for Transnational Data Governance

Ruoxin Su [1] and Dechun Zhang [2]

[1] Faculty of Law and Criminology, Vrije Universiteit Brussel, Belgium
[2] Department of Communication, University of Copenhagen, Denmark

Correspondence: Ruoxin Su (ruoxin.su@vub.be)

Submitted: 26 March 2025 **Accepted:** 20 May 2025 **Published:** 16 July 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

The exponential growth of data has turned transnational data governance into a strategic priority for global data hubs. While the concept of "data as the new oil" highlights big data's economic value, the dominance of large technology firms and increasing geopolitical tensions have prompted states, particularly China, to assert stronger control over cross-border data flows. Since the 2016 Cybersecurity Law, China's legislative approach has evolved significantly, culminating in comprehensive frameworks such as the Personal Information Protection Law and the Data Security Law. While prior research has focused on China's legal infrastructure and data localization mandates, this study examines the adaptive and geopolitical dimensions of its transnational data governance strategy—an area that remains underexplored. Drawing on a content analysis of central-level legislation from 2016 to 2024, this study identifies shifting legislative priorities, governance mechanisms, and legal rationales. The findings show that China has developed a multi-layered and increasingly flexible legal regime that balances sovereignty claims with selective openness, reflecting a pragmatic response to domestic needs and international pressures. This study expands the original scope of the "Beijing effect" by showing that China's influence on global data governance extends beyond the export of digital infrastructure to include dynamic legal adaptation and strategic regulatory innovation.

Keywords

China; Cybersecurity Law; data governance; data localization; Data Security Law; data sovereignty; Personal Information Law; transnational data governance

1. Introduction

The contemporary models of international trade and digital services inevitably involve significant cross-border data flows, a concept first introduced by the Organisation for Economic Co-operation and Development (OECD) in its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data in 1980. These guidelines recognized that national privacy protection laws could impede these data flows, despite their role in promoting the economic and social development of member countries (OECD, 2002). In Europe, the notion of transborder data flows was reiterated in the Convention for the Protection of Individuals with Regard to the Processing of Personal Data (Convention 108+). Over time, frameworks like the EU's General Data Protection Regulation (GDPR; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016) refined the tension between data privacy protection and the economic benefits of international data mobility, establishing criteria to regulate cross-border data transfers through the criterion of "adequate" level of data protection (Vosst, 2020). Nevertheless, as an OECD taxonomy suggests, approaches to regulating data flows differ widely, ranging from fully free flow to strict authorization (Casalini & González, 2019), indicating that the EU's framework does not reflect the practices of all nations.

Against this backdrop, China has pursued its own path toward transnational data governance since the Cybersecurity Law (CSL) in 2016, which diverges markedly. Driven by data localization policies and a state-centric philosophy of cyber sovereignty, China's framework has evolved into a more comprehensive system that prioritizes national security while seeking to navigate international pressures. Alongside these developments, scholars have proposed the "Beijing effect" (Erie & Streinz, 2021) to describe how China exports its digital governance model, although the role of legislative innovation and geopolitics in that process is still unfolding.

This article examines China's legislative innovations in transnational data governance, focusing on how these laws balance domestic regulation with international pressures while shaping global data flows since 2016. It finds that China's legislative framework has progressed from a regulatory gap prior to 2016 to a sophisticated and comprehensive system post-2021, with the introduction of laws like the Personal Information Protection Law (PIPL) and the Data Security Law (DSL), which provide detailed governance mechanisms. These changes reflect China's strategic approach to reconciling national security concerns, data protection, and international cooperation. In this context, China's data governance laws are not merely domestic measures, but strategic tools designed to enhance the country's position in the global data landscape. The article begins by reviewing existing literature on transnational data governance in Chinese law and the "Beijing effect" theory. It then outlines the qualitative content analysis methodology used to examine key Chinese legislative texts on transnational data governance. Finally, the findings are discussed, demonstrating the dynamic and adaptive nature of China's legal framework and its broader geopolitical implications.

2. Transnational Data Governance in Chinese Law, Data Sovereignty, and "Beijing Effect"

2.1. China's Emerging Legislative Framework for Data

China's legal framework for data governance has undergone significant transformation since 2021, with the enactment of two key legislative pillars: the PIPL and the DSL. These laws have established a more

structured and systematic data governance regime, reshaping China's regulatory landscape (Creemers, 2022). Some scholars further consider the CSL, introduced in 2016, as the third foundational pillar of China's data governance system (Peng et al., 2023; Y. Zhang, 2024). This legislative evolution has been largely driven by China's rapid and expansive datafication over the past decade, which has outpaced many other nations (Jia, 2024). Beyond addressing domestic regulatory needs, these laws also position China as a major actor in shaping global data governance norms—a phenomenon increasingly conceptualized as the "Beijing effect" (Erie & Streinz, 2021).

China's data protection laws are widely recognized as drawing inspiration from the EU's GDPR (W. Li & Chen, 2024; Pernot-Leplay, 2020). For example, the extraterritorial provisions embedded in the DSL and PIPL, similar to the EU's GDPR, suggest that Chinese cyber regulators may seek to extend their jurisdiction to foreign organizations and activities (M. Chen, 2024). However, while the EU emphasizes privacy as a fundamental right and enforces transnational governance principles, China's approach remains state-centric. Regarding cross-border data governance, unlike the EU, China does not require external jurisdictions to align with its standards, nor does it adopt the GDPR's foundational commitment to privacy as an inalienable right (Creemers, 2022; Peng et al., 2023). Beyond personal information protection, M. Chen (2024) points out that national security is also at the core of China's regulatory approach to cross-border data transfers.

At the operational level, the CSL, DSL, and PIPL collectively establish a multi-layered regulatory framework, supplemented by an expanding body of administrative regulations and guidelines issued by bodies such as the Cyberspace Administration of China (CAC). While these laws profess to safeguard personal information, they coexist with broad surveillance powers retained by state actors who present themselves as a guardian of citizens' privacy, raising questions about the genuine strength of individual privacy protections (Ollier-Malaterre, 2023; R. Wang et al., 2024). Jia (2024) argues that authoritarian regimes, including China, increasingly employ privacy protection rhetoric to enhance their legitimacy, even as they engage in extensive digital surveillance—practices traditionally associated with democratic deficits. R. Wang et al. (2024) further highlight how Chinese legislative bodies strategically frame data governance through legal ambiguity, selective censorship of major data breaches, and the reinterpretation of policy papers on data security threats.

2.2. Legislative Arrangements for Transnational Data Governance

The concept of transnational data governance has gained prominence in recent scholarship, evolving from earlier discussions of cross-border data regulation to address a wider array of challenges. Erie and Streinz (2021) define transnational data governance as the process through which domestic regimes shape and influence data governance beyond their own borders, extending beyond the regulation of data flows alone. A prominent example is the EU's GDPR, which since 2018 has restricted personal data transfers to non-EU countries unless they meet the EU's adequacy standards (Lin, 2024). As Safari (2017) and Ryngaert and Taylor (2020) observe, this has compelled other jurisdictions to align with EU privacy norms. Scholars such as Aaronson (2021) and Marchant (2020) emphasize that transnational data governance must also account for domestic policy priorities, technological advancements, geopolitical dynamics, and economic interests. These factors have led to divergent governance approaches among major economies: China enforces state control and stringent data localization, the EU centres individual data privacy rights, and the US favours self-regulation and corporate responsibility (Arner et al., 2022; Boyne, 2018; C. Zhang, 2024).

In China, a key mechanism of transnational data governance is the data export security assessment, first introduced in the 2016 CSL. While Hong (2020) regards it as a milestone toward comprehensive data governance, Y. Li (2021) questions its credibility due to its reliance on expert judgment over empirical evidence in the implementation. In response to both regulatory gaps and international scrutiny—particularly from the US through the World Trade Organization—China initiated efforts to refine this mechanism after the CSL (Guo & Li, 2025). These efforts culminated in the issuance of detailed measures in 2022 to operationalize the CAC assessment procedures (Tan, 2024). Nevertheless, concerns persist regarding the mechanism's vagueness and unpredictability. Y. Li (2021) and Tan (2024) identify three core issues: the vague definition of "important data" (which triggers mandatory assessments), the discretionary and uncertain review process, and the lack of an internationally recognized mechanism to facilitate cross-border data flows. Additionally, Y. Li (2021) and R. Wang et al. (2024) warn that China's national security-based governance model limits the autonomy of individuals and businesses, as authorities retain the power to terminate data transfers under the pretext of data security.

Beyond security assessments, China's 2021 PIPL introduced alternative governance tools, notably the standard contract mechanism and personal data protection certification. While China's standard contract resembles the GDPR's model clauses, it uniquely requires formal notification to the CAC upon execution (Xie et al., 2023; Y. Zhang, 2024). This notification requirement, as Patterson (2010) notes, undermines the principle of voluntary adoption and may create unnecessary regulatory hurdles (Tan, 2024). Paradoxically, Tan (2024) and Zhao (2023) observe that many firms still favour the more rigid security assessment route, as it provides clearer and more direct compliance legitimacy. This trend subtly incentivizes firms to self-restrict transnational data transfers, effectively reinforcing China's data localization policies (Chander, 2020; Tan, 2024). Meanwhile, personal data protection certification—conceptually similar to the EU's Binding Corporate Rules—has been proposed as a more flexible alternative for multinational corporations (Stalla-Bourdillon, 2024; Xie et al., 2023). However, its practical uptake and academic discussions on effectiveness still remain limited.

Recognizing the evolving demands of the digital economy and the challenges of global data governance, Chinese regulators have recently signalled a shift toward regulatory relaxation. Scholars such as A. H. Zhang (2024), M. Chen (2024), and Guo and Li (2025) identify a series of regulatory updates under the Provisions on Promoting and Regulating Cross-border Data Flows (Cross-Border Data Flows Provisions), aimed at easing restrictions. Guo and Li (2025) identify three primary motivations behind this shift: promoting trade-driven growth, aligning with global standards, and advancing China's influence over international data governance norms. Key reforms, including the narrowing of security assessment requirements and the clarification of "important data" classifications, seek to reduce compliance burdens and mitigate the uncertainty that has deterred foreign investment (M. Chen, 2024; Y. Zhang, 2024). Moreover, alongside these sovereignty and security concerns, economic drivers—such as support for national champions, the need to curb market concentration, and active lobbying by major platforms like Didi—have also shaped the CAC's recalibrated stance (A. H. Zhang, 2024). The rapid rollout of these changes reflects the CAC's recognition that overly stringent measures were counterproductive and signals a growing willingness to adopt a more flexible regulatory stance (Samm Sacks et al., 2024).

2.3. Emphasis on Data Sovereignty and National Security

Despite the evolving legislative landscape of China's data governance, scholars widely identify data sovereignty and national security as two central pillars shaping both its legal and political frameworks. Many researchers argue that data sovereignty underpins China's approach to data governance, establishing a framework that asserts the nation's exclusive jurisdiction over data collection and cross-border data flows (Hummel et al., 2021; Kokas, 2022; C. Zhang, 2024). This concept highlights the necessity of maintaining physical control over inherently mobile and fragmented data to ensure effective regulation (C. Zhang, 2024). Creemers (2023) and C. Zhang (2024) further connect data sovereignty to the broader notion of cyber sovereignty, which China employs to regulate its citizens' interactions with the global internet. While cyber sovereignty encompasses broader digital governance strategies, data sovereignty is more narrowly focused on controlling data flows (Creemers, 2023; C. Zhang, 2024). However, despite its conceptual significance, Gu (2023) underscores the challenges of enforcing data sovereignty in a digital environment characterized by data mobility, fragmentation, and decentralization, as well as a longstanding tradition of self-regulation in cyberspace.

National security similarly plays a pivotal role in shaping China's transnational data governance framework. Rooted in a political philosophy that prioritizes collective security over individual rights, China's approach reflects a national security-centric paradigm (Tan, 2024). C. Zhang (2024) explains that the Chinese government conceptualizes "safety" as a public good, justifying extensive state intervention and a strong preference for regulatory oversight. This emphasis on national security is closely intertwined with data sovereignty, leading to the implementation of stringent data localization policies. Lee (2021) and Erie and Streinz (2021) find that China's regulatory framework mandates not only that data be stored and processed within its borders but also that it be managed by domestic entities, forming a twofold data localization strategy. While Tan (2024) observes a recent softening of these policies, foreign companies operating in China continue to face significant regulatory constraints.

China's national security-driven approach has drawn widespread criticism. Jiang (2023) warns that the broad application of national security exceptions imposes excessive procedural and substantive requirements on transnational data transfers, potentially hindering international trade and investment. C. Zhang (2024) critiques the CAC reliance on quantitative methods to determine when privacy concerns become national security matters, arguing that this approach assumes privacy can only be safeguarded through a strong, sovereign state. Additionally, Y. Wang (2022) points out that the vague definition of national security grants administrative authorities excessive discretion in conducting security assessments, leading to unnecessary compliance burdens and reduced regulatory efficiency.

Importantly, China is not alone in emphasizing data sovereignty and national security within its governance framework. Governments worldwide are increasingly prioritizing state control over data as a means of ensuring social order and national security, a trend not exclusive to non-democratic regimes (Erie & Streinz, 2021). Gao (2022) identifies a growing convergence between China's sovereignty-oriented approach and those of Western countries, cautioning against oversimplifying their differences. Scholars suggest that the global emphasis on data sovereignty reflects shared challenges posed by rapid technological advancements and the expanding capabilities of data utilization (Gao, 2022; C. Zhang, 2024). However, despite these commonalities, national data sovereignty ambitions risk undermining the internet's role in fostering global interconnectedness and the free exchange of information (Erie & Streinz, 2021).

2.4. "Beijing Effect" in China's Transnational Data Governance

The EU's GDPR is widely recognized as one of the most influential legal instruments in transnational data governance. Bradford (2020) conceptualizes it as a key example of the Brussels effect, a theory that describes the EU's unilateral ability to shape global regulatory and business environments through its legislation. Building on this idea, Erie and Streinz (2021) introduce the concept of the Beijing effect to explain how China exerts influence over transnational data governance beyond its borders. This framework highlights China's assertion of digital sovereignty through mechanisms such as data localization mandates, the export of digital infrastructure, and the promotion of Chinese technical standards. According to Erie and Streinz (2021), the Beijing effect operates through three primary channels: (a) the adoption of China's data sovereignty model by foreign governments, (b) China's growing role in digital technology standard-setting, and (c) the external deployment of Chinese digital infrastructure and platforms, particularly via the Digital Silk Road.

While Erie and Streinz (2021) focus on China's use of digital infrastructure to shape external data governance regimes, they may overlook the equally transformative role of China's evolving legal frameworks. Recent legislative developments—such as the PIPL, the DSL, and regulations governing cross-border data flows—demonstrate China's increasing precision in regulating transnational data governance. These legal instruments not only reinforce China's data sovereignty but also reflect the broader securitization of data governance, shaped by both domestic needs and international geopolitical pressures. As C. Zhang (2024) argues, the continued evolution of China's legislative framework could escalate geopolitical tensions with other major regulatory powers while simultaneously offering a governance model for states seeking greater control over data.

This study addresses this gap by extending the Beijing effect framework to incorporate the strategic role of legislative evolution in China's transnational data governance. Through qualitative content analysis of central-level legal instruments, it explores how China's legislative innovations navigate transnational data flows amidst domestic regulatory needs and international pressures. The authors argue that a comprehensive understanding of the Beijing effect must move beyond China's export of digital infrastructure to consider the dynamic and adaptive nature of its legislative landscape. This integrated perspective enriches both legal and international relations scholarship by shedding light on the complex interplay between regulatory reform and geopolitical strategy in the digital age.

3. Methodology

This study investigates the legal evolution of China's transnational data governance and its geopolitical dimensions through a qualitative content analysis. This method provides a structured framework to identify legislative trends, governance patterns, and geopolitical implications embedded within China's data governance framework. To ensure a focused and in-depth examination, the analysis is limited to Chinese legal instruments directly relevant to transnational data governance, excluding government policies, notices, and propaganda. This distinction clarifies the boundary between binding legal frameworks and advisory or promotional documents, aligning with the legal definition of laws as formal, enforceable rules established by governing authorities. Following the Legislation Law of the People's Republic of China, the study examines formal legal categories, including the Constitution (宪法), laws (法律), administrative regulations (行政法规),

regional regulations (地方性法规), departmental rules (部门规章), and regional rules (地方政府规章). Afterwards, this study narrows its focus to laws enacted by the central government, reflecting the hierarchical nature of China's legal system, where regional legislation must comply with central-level laws. Analyzing central laws ensures a coherent understanding of the overarching legal framework governing transnational data issues while avoiding the impracticality of reviewing the extensive body of regional legislation across China's provinces, autonomous regions, and municipalities.

Within this central legal framework, this study first identifies laws that explicitly or implicitly address transnational data governance. This selection includes legal instruments where transnational data governance is either a primary focus or an integrated component of broader legislative objectives. Given the rapid legislative activity in China over the past decade, particularly in cyberspace and data governance, the analysis employs a keyword-based screening process. Keywords such as "cybersecurity" (网络安全), "personal information" (个人信息), "data security" (数据安全), "personal information protection" (个人信息保护), "cross-border data flow" (数据跨境流动), and "data export" (数据出境) guide the identification of relevant legal texts. Each text is reviewed for relevance based on its legislative purpose, scope, and governance objectives.

The study also considers legislative proposals related to transnational data governance that, while not yet officially adopted, indicate evolving regulatory trends (categorized as "legislative proposal" in Figure 1). Including these proposals captures the dynamic and forward-looking nature of China's legislative process, where draft laws often transition rapidly into formal statutes (categorized as "formal legislation" in Figure 1). To avoid double-counting, any draft that subsequently becomes formal legislation is excluded from the "legislative proposal" count. The selected legal instruments include foundational texts such as the CSL (网络安全法), DSL (数据安全法), and PIPL (个人信息保护法), alongside various legally binding measures, regulations, and rules addressing cross-border data flows and mechanisms, such as the Measures on Security Assessment for Data Export (数据出境安全评估办法) and Cross-Border Data Flows Provisions (促进和规范跨境数据流动规定).

This study employs qualitative content analysis with a thematic analytical approach to examine the substantive provisions of selected legal texts. The analysis was conducted in several steps. First, key legislative documents related to transnational data governance were collected and chronologically organized. The analysis begins by mapping the legislative evolution of key legal instruments to identify distinct phases of regulatory activity, highlighting patterns of acceleration, shifts in focus, and the interplay between domestic and global factors influencing China's data governance framework. Second, an initial coding scheme was developed based on recurring themes such as legislative themes and purposes, governance models, governance tools, special legislative designs, and legal liabilities.

Third, the documents were subjected to iterative and systematic coding to identify both manifest and latent themes. This involved multiple rounds of close reading: open coding was used to tag relevant textual segments, followed by axial coding to link related codes and identify overarching categories. Selective coding was then applied to refine and consolidate the most salient themes that capture regulatory priorities and shifts. The coding scheme was continuously adjusted as new patterns emerged, particularly in relation to evolving concepts such as "data sovereignty," "data localization," "security assessment," "exterritorial jurisdiction," and "discriminatory reciprocal measures." These themes were tracked across the legislative timeline to assess changes in emphasis, legal framing, and policy intent. This approach enabled the

identification of structural shifts in the legal discourse around transnational data governance. While government policies, administrative notices, and propaganda materials were not the primary focus, they were referenced when necessary to contextualize legal instruments and clarify their geopolitical implications. Overall, this methodology supports a comprehensive and nuanced analysis of China's regulatory approach, situating it within broader geopolitical dynamics and global governance trends.

4. Results

4.1. Legislative Evolvement in Transnational Data Governance

The review of China's evolving legislative landscape in transnational data governance reveals a significant shift over time. Prior to 2016, China lacked formal legislation dedicated to cross-border data transfers, leaving this digital frontier open and largely unregulated. The 2016 CSL inaugurated a formal data localization requirement (Article 37), obliging critical information infrastructure operators (CIIOs)—initially defined in narrow sectors such as finance, telecommunications, and energy—to store personal information and important data domestically and to submit to security assessments for any outbound transfer. While limited in scope, this marked the first legislative assertion of China's sovereignty over data generated within its territory.

Between 2017 and 2020, China issued several legislative drafts that signalled a gradual broadening of the localization principle beyond CIIOs to other significant data controllers through the security assessment mechanism. These included the Measures on Security Assessment for Exporting Personal Information and Important Data (2017), the Measures on Data Security Management (2019), and the Measures on Security Assessment for Exporting Personal Information (2019). Although not crystalizing into legally binding instruments, these drafts reinforced China's declarative positioning: cross-border data transfers are a matter of national security and must be governed by state-defined mechanisms. However, the lack of finalized legislation during this period reflected a cautious and experimental approach.

A watershed came in 2021 with the enactment of the PIPL and the DSL. The PIPL's Article 40 extended data localization and security assessment requirements to any processor handling significant volumes of data and Article 36 imposed domestic-storage mandates on national authorities processing citizens' data. Otherwise, they must undergo a government-conducted security assessment before exporting personal data. The DSL's Article 31 replicated and deepened these localization and risk-assessment requirements for "important data," aligning them with previous CSL provisions but applying them to a wider universe of data-holding actors. These laws together shift China's strategy from reactive rule-making to proactive sovereignty assertion: Data produced in China is an asset under the state's exclusive jurisdiction, and legislative iteration becomes the vehicle for articulating and defending that claim.

Since 2022, implementation has been reinforced by a series of detailed regulatory instruments, including the Measures on Security Assessment for Data Export (2022), the Implementation Rules for Personal Information Protection Certification (2022), the Standard Contract Measures for Personal Information Export (2023), and the Cross-Border Data Flows Provisions (2024). While these emerging instruments occupy a lower position in China's legal hierarchy, they play a crucial role in clarifying the ambiguities left by the three cornerstone laws—CSL (2016), PIPL (2021), and DSL (2021)—thereby shaping a multi-layered legislative framework for China's

transnational data governance. Notably, the Cross-Border Data Flows Provisions (2024) relaxes restrictions on transnational data flows by carving out industry-specific exemptions and delegating "negative-list" authority to provincial regulators, suggesting a calibrated shift to strategic flexibility of governance. Together, these developments represent a transition from an exploratory legislative phase to more mature and strategically flexible governance. Yet even in these relaxations, China's sovereignty strategy remains evident: the state retains ultimate control over what data may exit its borders, and under what conditions.

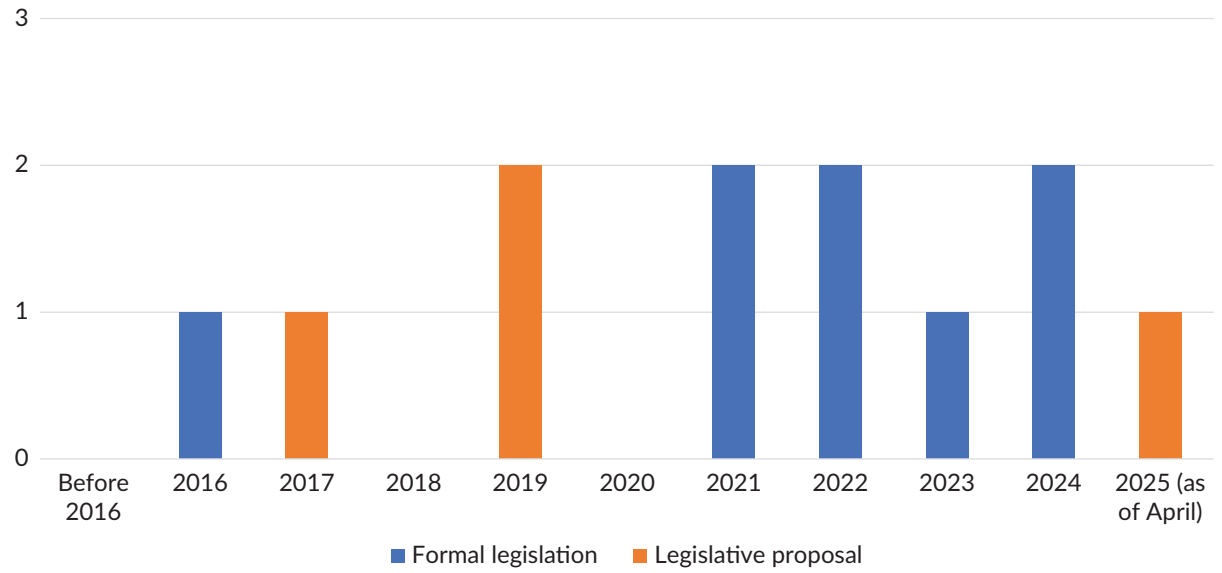


Figure 1. China's legislative activities for transnational data governance.

Accordingly, the evolution of China's legislative landscape can be categorized into four distinct phases. The first phase, prior to 2016, was marked by a legislative vacuum with no specific legal framework governing cross-border data flows. The second phase, from 2016 to 2020, introduced key concepts such as data localization through the CSL and began to establish mechanisms for assessing the security of cross-border data transfers. The third phase, from 2021 to 2023, saw a surge in legislative refinement, characterized by systematic and detailed legal requirements for data protection and cross-border data governance. The fourth phase, beginning in 2023, reflects a shift toward a more flexible approach to regulating cross-border data transfers, signalling potential relaxation in oversight.

The focus of these laws can be broadly classified into three themes: safeguarding national data sovereignty and security, protecting personal data and privacy, and facilitating international data transfers. At the national level, laws such as the CSL (2016) and DSL (2021) emphasize cyberspace sovereignty and national security. At the individual level, legislation such as the PIPL (2021) and the Measures on Standard Contract for Personal Information Export (2022) focuses on protecting personal data rights in cross-border contexts. At the societal level, the legislation seeks to balance secure and lawful data use with promoting economic and social growth, including facilitating international data flows.

Legal liabilities for breaches of China's cross-border data rules have also escalated sharply alongside the burgeoning regulatory framework. Under the 2016 CSL, offending entities face fines up to 500,000 yuan; by 2021, the DSL raised this cap to 10 million yuan for unlawful international data transfers, and the PIPL

further augmented penalties to as much as 50 million yuan or 5% of the previous year's turnover, while introducing additional measures such as blacklisting, business-activity restrictions, and formal recording of infractions within China's social credit system. At the same time, the CAC has consolidated its authority as the principal architect and enforcer of transnational data governance. Although the Standing Committee of the National People's Congress enacts the CSL, DSL, and PIPL, these high-level laws vest sweeping rule-making and implementation powers in the CAC, underscoring its central rule-making role in shaping China's transnational data governance.

4.2. China's Legal Designs and Tools for Transnational Data Governance and Sovereignty

An analysis of the screened laws reveals that since 2021, China's legislative architecture of transnational data governance architecture has manifested an explicit sovereignty strategy, embedding extraterritorial jurisdiction and novel countermeasures in the DSL and the PIPL. Before 2021, the CSL (2016) and three legislative drafts proposed by the CAC were only focused on regulating networks and data within China's territorial boundaries, without extraterritorial applicability. However, the DSL and PIPL introduced a significant oversight expansion to data processing activities outside of China: Article 2 of the DSL asserts to govern overseas data processing that threatens China's national security, public interests, or the rights of Chinese citizens and organizations; similarly, Article 3 of the PIPL applies to any foreign data processing targeting individuals in China, such as providing products or services or analyzing their behaviour. These jurisdictional extensions are not simply technical rules but deliberate assertions of China's claim to exclusive authority over data once generated within or concerning its citizenry.

To operationalize this claim in transnational data governance, China has developed three primary governance tools: (a) security assessments for data export, requiring government approval for certain data transfers; (b) standard contracts for personal information export, which companies adopt voluntarily but must report to regulators; and (c) personal information protection certification, demonstrating a company's compliance with data protection standards during international transfers. Security assessments, first introduced in 2016, initially targeted CIIOs to prevent cross-border data transfers that could risk national security or public interest. The CAC explored this tool through legislative drafts between 2017 and 2019 but did not clarify it until the 2022 Security Assessment Measures, such as the thresholds, criteria, procedural details, and legal liabilities related to security assessments. In 2024, the CAC further eased the thresholds with the Cross-Border Data Flows Provisions, indicating a more relaxed regulatory attitude towards trade-oriented data flows. Companies must now undergo security assessments if they act as a CIIO, i.e., transfer important data abroad or exceed data-transfer volume thresholds (i.e., more than 1 million individuals or sensitive personal data of over 10,000 individuals). Notably, Article 6 of the 2024 Cross-Border Data Flows Provision allows regional regulators to further lower these thresholds in pilot free trade zones via "negative lists" of cross-border data transfer, which determine which types of data should be subject to the government's scrutiny (by the time of writing, for example, Beijing, Shanghai, the Hainan Province, and the Zhejiang Province have respectively issued their "negative list" tailored to local trade needs).

The standard contract and certification tools, introduced later in 2021, complement the security assessment mechanism by addressing scenarios where companies do not meet the thresholds for mandatory security assessments. In November 2022, the CAC, in collaboration with the State Administration for Market Regulation, introduced the personal information protection certification. This voluntary certification allows

companies to demonstrate their capacity to protect personal data during international transfers. In February 2023, the CAC released a standard contract template for companies to use when transferring personal data abroad. In the subsequent year, the CAC issued two parallel standard contract templates tailored to cross-border data flows occurring in the Greater Bay Area, i.e., from the mainland to Hong Kong/Macau. These contracts include clauses outlining data protection obligations, individual rights, liabilities, and remedies, ensuring compliance with China's data security standards. Companies must also complete a filing process for signed contracts, which strengthens regulatory oversight without involving substantive reviews. Overall, these findings underscore the systematic evolution of China's legal framework for transnational data governance, marked by its extraterritorial reach, distinct governance tools, and nuanced legal terminology. Together, these developments illustrate China's strategic approach to regulating cross-border data flows while safeguarding national security and public interests.

Complementing these tools, the DSL and PIPL introduced two distinctive mechanisms for transnational data governance. The first mechanism is established by the PIPL's reciprocal countermeasure provision (Article 43), which empowers China to retaliate against countries or regions that impose discriminatory data protection restrictions. Their principal effect is to signal China's readiness to defend its digital jurisdiction selectively, rather than establish a universally applied mechanism, while they have not been invoked substantively. The second mechanism, established by Article 41 of the PIPL and Article 36 of the DSL, restricts foreign judicial or law enforcement agencies from accessing personal data stored in China without government approval. This prohibition can only be waived through international agreements or based on principles of equality and mutual benefit.

Even the terminology used in China's data governance laws reinforces China's sovereignty narrative. For example, the term "cross-border" (跨境) is preferred over "transnational" (跨国) to describe data flows between jurisdictions. This distinction emphasizes China's legal view of itself as a singular jurisdiction, separate from regions like Hong Kong and Macau. Moreover, the 2021 draft of the Regulations on the Security Management of Network Data used the term "outside of the border" (境外) 32 times, whereas "outside of the nation" (国外) appeared only once. These delineate a single and indivisible jurisdiction whose external data flows are subject to sovereign will.

5. Discussion

The results of this study reveal a significant transformation in China's legislative approach to transnational data governance, marking a shift from early experimental regulation (2017–2020) to a more institutionalized and adaptive legal framework since 2021. This shift is not merely a chronological progression but reflects a deeper reconfiguration of regulatory priorities and state rationalities. While the CSL (2016) initially introduced the idea of data control through the regulation of CIIOs, it lacked broader applicability. The subsequent legal developments, particularly the enactment of the DSL and the PIPL in 2021, have institutionalized a more expansive and sophisticated governance system.

These findings extend the arguments made by Creemers (2022) and A. H. Zhang (2024), who view these legislative milestones as signalling a structural consolidation of China's digital governance regime. However, this study contributes further by showing how China's approach has evolved not only in scope but also in legal strategy—through the gradual layering of enforcement tools and the fine-tuning of regulatory instruments.

This supports the theoretical claim that authoritarian legalism in China is increasingly operationalized through "rule-by-law" rather than merely symbolic legal expression (Hurst, 2016; Whiting, 2017)

Moreover, the emphasis on data sovereignty—consistently articulated from the CSL's reference to "cyberspace sovereignty" (Article 1) to the DSL's opening declaration on "safeguarding national sovereignty"—confirms a central tenet in the literature on China's techno-nationalism (Hummel et al., 2021; Kokas, 2022). Yet this study nuances the prevailing assumption that China's approach is uniformly rigid and security-centric. The recent Cross-Border Data Flows Provisions (2024) introduce selective regulatory relaxations, suggesting a recalibration of state priorities. This dual logic—assertive sovereignty combined with conditional flexibility—complicates earlier portrayals of China's regime as singularly defensive (Erie & Streinz, 2021; Lee, 2021). Instead, our findings align with a growing body of scholarship (e.g., M. Chen, 2024; Guo & Li, 2025; Sacks et al., 2024) that interprets China's evolving data regime as balancing geopolitical anxieties with pragmatic economic considerations.

Theoretically, this study contributes to ongoing debates on authoritarian resilience and regulatory hybridization. The Chinese case demonstrates how legal infrastructures can function dually as instruments of exclusionary state control and strategic international engagement. This reflects what T. Chen et al. (2023) describe as "adaptive governance," whereby authoritarian states adjust regulatory tools to navigate both domestic political imperatives and external economic pressures. By tracing the evolution of legal instruments and regulatory rationales, this study offers an empirically grounded account of how a techno-authoritarian regime manages tensions between sovereignty, market openness, and global interoperability. In doing so, the findings not only reaffirm but also refine existing theories of digital sovereignty, legal authoritarianism, and policy adaptation in the context of intensifying global data governance.

5.1. Legislative Designs in Response to Dynamic Geopolitics

This study also identifies an increasing prevalence of specialized legislative designs within China's transnational data governance framework, which can be interpreted as a strategic response to external geopolitical pressures. For instance, the extraterritorial provisions in the DSL and the PIPL extend regulatory oversight to data processing activities occurring outside of China, particularly when these activities threaten national security or public interests. This extraterritorial reach is unsurprising, considering the broader shift from exploratory drafts (2017–2020) to the establishment of more robust and detailed legal rules post-2021. This legislative evolution partially aligns with C. Zhang's (2024) description of China's national security-centric model, but it also signifies a more assertive stance in the global regulatory competition than was previously evident in earlier drafts of these laws.

The introduction of extraterritorial reach is not unique to China but rather echoes broader global trends, such as those established by the EU's GDPR. This development can be situated within the framework of the "Brussels effect" (Bradford, 2020), wherein non-EU jurisdictions, including China, are influenced by the EU's regulatory standards. Scholars such as Creemers (2022) and W. Li and Chen (2024) have observed this phenomenon, noting that China's evolving data governance laws reflect similar regulatory assertiveness. The findings of this study further demonstrate that China has incorporated reciprocal or adversarial clauses in its legal texts that directly address perceived external threats, signalling China's intent to challenge Western regulatory dominance. For example, Article 43 of the PIPL introduces reciprocal measures against

"discriminatory" foreign data practices, while Article 36 of the DSL (2021) prohibits data sharing with foreign judicial or law enforcement agencies without the approval of the Chinese government. These provisions are considered a direct response to the extraterritorial reach of foreign laws such as the US CLOUD Act (Zheng, 2021). These legal clauses corroborate M. Chen's (2024) argument that China's data governance approach extends beyond domestic concerns, actively countering the imposition of cross-border data restrictions by foreign jurisdictions on Chinese entities.

This study further argues that rather than being solely defensive, these legal provisions function as proactive tools designed to recalibrate global power dynamics in transnational data governance, an area traditionally dominated by Western democracies. Such legislative innovations underscore the interaction between domestic legal refinement and external geopolitical pressures, highlighting that China's approach to data governance is not merely reactive or driven by technological considerations. On the international stage, China's legislative actions represent both a response to perceived foreign extraterritoriality—exemplified by US and EU data laws—and an attempt to assert a significant role in shaping global data governance standards. The emphasis on extraterritorial oversight and reciprocal clauses against foreign intrusion reflects China's broader geopolitical strategy, signalling its intention to maintain strong state control over its digital and data governance frameworks.

Domestically, Chinese regulators are balancing the need to foster economic digitalization and facilitate international data flows within the digital economy while maintaining the broader objective of cyber sovereignty. For example, the PIPL introduced the tool of personal information protection certification, which offers conditional exemptions from government assessments for routine cross-border data transfers (for example, Alibaba's cross-border e-commerce platform was among the first beneficiaries). This measure reflects a more flexible stance towards multinational enterprises that comply with domestic security guidelines, signalling a pragmatic approach that accommodates global trade and economic realities. The partial relaxation of data localization requirements may represent an emerging convergence with the global trade landscape, as observed by Gao (2022), who notes that China's traditionally sovereignty-oriented approach to data governance is increasingly tempered by pragmatic considerations in the context of global data flows and economic interdependence. Overall, China's evolving legal framework for transnational data governance represents a complex balancing act between asserting national sovereignty, responding to external geopolitical pressures, and strategically positioning itself within the global digital economy. The shift toward more flexible and adaptive legal provisions, while retaining a strong emphasis on state control, reflects China's growing ambition to shape the future of global data governance.

5.2. Expanding the "Beijing Effect" in China's Data Governance

The "Beijing effect" theory, initially conceptualized by Erie and Streinz (2021), offers a compelling account of how China seeks to influence global data governance through the strategic export of digital infrastructure, particularly via initiatives like the Digital Silk Road. According to this framework, China promotes a sovereignty-centric model of data governance, underpinned by territorial data localization requirements that are appealing to developing nations seeking strong state control over digital flows. While this interpretation remains valid in explaining China's technical and infrastructural outreach, our findings suggest that an equally important vector of influence lies in China's evolving legal architecture—what can be understood as a legislative dimension of the "Beijing effect."

China's legal framework for transnational data governance has undergone significant transformation since 2016. Initially, Article 37 of the CSL introduced data localization for CIIOs, laying the groundwork for domestic data control. The scope and strategic intent of this law were explicitly framed in Article 1, which declares the safeguarding of "cyber sovereignty" as a primary legislative goal—an early legal articulation of digital sovereignty that transcends traditional territorial concepts. In 2021, the enactment of the PIPL and the DSL further extended China's data sovereignty claims. For instance, Article 3 of the PIPL introduces extraterritorial jurisdiction over foreign entities that process the personal data of individuals within China, mirroring the EU's GDPR and also adapting to China's geopolitical imperatives. Simultaneously, Article 40 of the PIPL reinforces data localization for CIIOs and major data processors, while Article 36 of the DSL empowers Chinese authorities to block foreign access to data on grounds of national security and public interest, signalling a legal mechanism for data sovereignty in transnational contexts.

Beyond these foundational laws, China has built a layered system of enforcement through regulatory instruments such as the Measures on Security Assessment for Data Export (2022), which operationalize security reviews for cross-border transfers involving sensitive data. The Standard Contract Measures for Personal Information Export (2023) and the Cross-Border Data Flows Provisions (2024) further illustrate how China seeks to institutionalize data transfer governance while retaining discretionary control. The 2024 Provisions, in particular, mark a notable shift: they introduce exemptions for certain categories of data processors, such as those handling small-scale transfers or engaging in trade-related activities with minimal privacy risks. This pragmatic adjustment suggests that China is not pursuing data sovereignty in absolutist terms but is instead fine-tuning its legal regime to balance control with economic openness.

These developments indicate that China's approach to data sovereignty is no longer characterized solely by rigid data localization and top-down control. Rather, the emerging model involves dynamic regulatory adaptation, combining hard sovereignty with selective flexibility. For instance, while extraterritorial provisions in the PIPL and DSL assert China's regulatory power beyond its borders, the recent streamlining of security assessments and increased reliance on standardized contracts indicate a willingness to accommodate international stakeholders. This dual approach enables China to project influence globally while reducing friction with foreign firms and governments—a recalibration that reflects both internal deliberations and external pressures.

This evolving strategy revises the initial premises of the "Beijing effect." While Erie and Streinz (2021) correctly highlight the geopolitical logic behind China's digital infrastructure exports and strict sovereignty norms, their emphasis on infrastructure overlooks how China's legal frameworks themselves act as vehicles of influence. Our findings suggest that legal instruments—ranging from localization mandates to extraterritorial rules and reciprocal access clauses—serve as tools of geopolitical signalling and regulatory modelling. Importantly, the recent trend toward conditional openness, reflected in the 2024 Provisions, suggests that China is not simply exporting a rigid model of authoritarian control but is instead experimenting with a hybrid regulatory approach that combines sovereignty discourse with economic pragmatism.

Thus, the "Beijing effect" should not be viewed as a static projection of China's early digital exportation. It must be understood as a dynamic and evolving framework that reflects China's efforts to adapt its legal governance to shifting global conditions. China's strategy now involves embedding sovereignty claims within a more sophisticated regulatory architecture that is capable of adjusting to international norms when

advantageous, while still preserving mechanisms for control when strategic interests are at stake. This hybridization marks a departure from earlier, more confrontational models and suggests that China's influence on global data governance is increasingly exerted not only through infrastructure but also through law.

5.3. China's Dynamic Legislative Strategy in Transnational Data Governance

Taken as a whole, this study reveals that China's legislative framework for transnational data governance—within the broader context of the "Beijing effect"—is characterized by both strategic intentionality and adaptive responsiveness. Rather than representing a monolithic or rigid model, China's approach reflects a dynamic negotiation between competing imperatives: the assertion of national sovereignty, the safeguarding of data security, the promotion of indigenous innovation, and the pragmatic need to remain integrated within global digital markets.

Building on scholarship that emphasizes the centrality of sovereignty and national security in Chinese data governance (Hummel et al., 2021; Kokas, 2022; C. Zhang, 2024), our findings reaffirm that these principles are deeply embedded in China's legal infrastructure through instruments such as extraterritoriality clauses (PIPL, Article 3), data localization requirements (PIPL, Article 40 and CSL, Article 37), and defensive provisions against foreign legal requests (DSL, Article 36). These mechanisms reinforce China's efforts to exert both internal and transnational control over data flows. However, our analysis also reveals important signs of regulatory recalibration. The relaxation of data transfer mandates in low-risk contexts such as cross-border e-commerce, travel services, human resource management, and scientific collaboration—introduced most notably in the 2024 Cross-Border Data Flows Provisions—suggests a growing recognition that overly rigid controls can inhibit economic growth, international trade, and technological innovation. The delegation of exemption authority to regional regulators by means of negative lists of data categories subject to assessment, within pilot free-trade zones such as Shanghai, Hainan, and Zhejiang, exemplifies the same logic: asserting sovereignty where strategic interests demand while accommodating global trade and technological cooperation when advantageous.

This evolving governance pattern resonates with and extends recent theoretical work on adaptive governance under authoritarianism (T. Chen et al., 2023; Lee, 2021). Our findings support the notion that China is not only building coercive legal tools to centralize data control but is also engaging in regulatory experimentation to balance economic interests and global pressures. In this regard, the Chinese model reflects a form of "authoritarian legal pragmatism"—where legal instruments are both vehicles of state control and strategic flexibility. Contrary to earlier portrayals of China's approach as uncompromising or anti-global (Erie & Streinz, 2021; Lee, 2021), this study suggests a more nuanced trajectory: one in which sovereignty claims are asserted, but selectively moderated in response to shifting geopolitical and market conditions.

From a comparative perspective, our findings also contribute to the growing literature on regulatory competition in global data governance (Arner et al., 2022). China's model can be seen as a third pathway that contrasts with the privacy-oriented EU framework (anchored in the GDPR) and the sector-specific, industry-driven US approach. China's hybrid model combines sovereignty-driven legal mechanisms with selective openness, enabling the state to shape international data norms while preserving discretionary

control. This dual strategy has implications for global norm diffusion: it may prompt other jurisdictions—particularly in the Global South—to adopt similar frameworks that prioritize state oversight while maintaining space for international economic cooperation. For instance, at the recent ASEAN Digital Ministers' Meeting, participants endorsed China's 2025 work plan to facilitate aligning ASEAN Model Contractual Clauses with China's standard contract for cross-border data flows, thereby institutionalizing China's legal templates within regional governance.

At the same time, China's evolving approach may exacerbate global regulatory fragmentation. As our findings suggest, foreign companies operating in China now face an increasingly complex landscape of compliance, where domestic legal requirements (e.g., security assessments, standard contracts, and localization mandates) interact with external regulations such as the GDPR and US laws on foreign data transfers. This growing complexity could deepen what some scholars term "regulatory friction" (Bradford, 2020), intensifying the costs of compliance and operational uncertainty for multinational enterprises.

In sum, this study refines the theoretical understanding of the "Beijing effect" by illustrating how China's influence is not limited to infrastructure exports or normative assertions of digital sovereignty. Rather, it extends through a sophisticated and evolving legal regime that blends coercive control with regulatory adaptation. The Chinese state's use of legal instruments to shape global data flows should thus be understood not only as an authoritarian assertion but also as an ongoing process of legal adaptation—responsive to both domestic imperatives and international strategic considerations. This dynamic suggests a new phase in China's role within global digital governance: not just as a norm challenger, but increasingly, as a norm shaper.

6. Conclusion

In conclusion, this study highlights the significant evolution of China's transnational data governance framework, which has progressed from fragmented early drafts to a sophisticated, multi-layered legal system that balances sovereignty, national security, and economic interests. Through key legal instruments such as the PIPL and DSL, China has strategically integrated extraterritorial provisions and sovereignty discourses, positioning its regulatory framework as a tool for asserting influence on the global data governance landscape. However, recent trends indicate a shift towards greater flexibility, with partial relaxations of data localization requirements aimed at promoting economic growth and global integration. This evolving approach reflects a dynamic interplay between internal imperatives and external geopolitical pressures.

Moreover, this study extends the "Beijing effect" framework beyond digital infrastructure export, incorporating legislative innovation and adaptation as crucial components of China's influence on global data governance. While China's model continues to emphasize state-led data sovereignty, its recent legislative adjustments suggest a more adaptive strategy that accommodates global trade and technological collaboration. As such, the "Beijing effect" should be viewed as a dynamic, evolving framework, with China's legislative approach serving as both a response to international regulatory competition and a proactive tool for shaping global data governance norms.

Acknowledgments

This study would like to thank the two academic editors, Xuechen Chen and Xinchuchu Gao, for their valuable support and comments.

Funding

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. Publication of this article in open access was made possible through the institutional membership agreement between the Vrije Universiteit Brussel and Cogitatio Press.

Conflict of Interests

The authors declare no conflict of interests.

References

Aaronson, S. A. (2021). *Could trade agreements help address the wicked problem of cross-border disinformation?* (No. No. 255). Centre for International Governance Innovation. https://www.cigionline.org/publications/could-trade-agreements-help-address-the-wicked-problem-of-cross-border-disinformation

Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. *Berkeley Technology Law Journal*, *37*(2), 623–700. https://doi.org/10.15779/Z38GF0MX5G

Boyne, S. M. (2018). Data protection in the United States. *The American Journal of Comparative Law*, *66*(Suppl. 1), 299–343. https://doi.org/10.1093/ajcl/avy016

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press. https://doi.org/10.1093/oso/9780190088583.001.0001

Casalini, F., & González, J. L. (2019). *Trade and cross-border data flows* (Trade Policy Papers No. 220). Organisation for Economic Co-operation and Development. https://doi.org/10.1787/b2023a47-en

Chander, A. (2020). Is data localization a solution for Schrems II? *Journal of International Economic Law*, *23*(3), 771–784. https://doi.org/10.1093/jiel/jgaa024

Chen, M. (2024). Developing China's approaches to regulate cross-border data transfer: Relaxation and integration. *Computer Law & Security Review*, *54*, Article 105997. https://doi.org/10.1016/j.clsr.2024.105997

Chen, T., Liang, Z., Yi, H., & Chen, S. (2023). Responsive e-government in China: A way of gaining public support. *Government Information Quarterly*, *40*(3), Article 101809. https://doi.org/10.1016/j.giq.2023.101809

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1). https://doi.org/10.1093/cybsec/tyac011

Creemers, R. (2023). The Chinese conception of cybersecurity: A conceptual, institutional, and regulatory genealogy. *Journal of Contemporary China*, *33*(146), 173–188. https://doi.org/10.1080/10670564.2023.2196508

Erie, M. S., & Streinz, T. (2021). The Beijing effect: China's Digital Silk Road as transnational data governance. *New York University Journal of International Law and Politics*, *54*(1), 1–92.

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, *57*(3), 15–30. https://doi.org/10.1080/03932729.2022.2074710

Gu, H. (2023). Data, big tech, and the new concept of sovereignty. *Journal of Chinese Political Science*, *29*, 591–612. https://doi.org/10.1007/s11366-023-09855-1

Guo, S., & Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation? *Computer Law & Security Review*, *56*, Article 106079. https://doi.org/10.1016/j.clsr.2024.106079

Hong, Y. (2020). The institutional logic of security assessment of cross-border data transfers in China: Context and progress. *International Cybersecurity Law Review*, *1*(1/2), 93–102. https://doi.org/10.1365/s43439-020-00007-2

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 1–17. https://doi.org/10.1177/2053951720982012

Hurst, W. (2016). Chinese law and governance: Moving beyond responsive authoritarianism and the rule of law. *Journal of Chinese Governance*, *1*(3), 457–469. https://doi.org/10.1080/23812346.2016.1212549

Jia, M. (2024). Authoritarian privacy. *University of Chicago Law Review*, *91*, 733–809. http://doi.org/10.2139/ssrn.4362527

Jiang, F. (2023). China's legal efforts to facilitate cross-border data transfers: A comprehensive reality check. *Asia Pacific Law Review*, *32*(1), 81–101. https://doi.org/10.1080/10192557.2023.2232613

Kokas, A. (2022). *Trafficking data: How China is winning the battle for digital sovereignty*. Oxford University Press. https://doi.org/10.1093/oso/9780197620502.001.0001

Lee, A. (2021). *Personal data, global effects: China's draft privacy law in the international context*. DigiChina. https://digichina.stanford.edu/work/personal-data-global-effects-chinas-draft-privacy-law-in-the-international-context

Li, W., & Chen, J. (2024). From Brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China. *Computer Law & Security Review*, *54*, Article 105994. https://doi.org/10.1016/j.clsr.2024.105994

Li, Y. (2021). La disciplina cinese del trasferimento transfrontaliero dei dati. *Rivista Italiana Di Informatica e Diritto*, *3*(1), 67–78. https://doi.org/10.32091/RIID0028

Lin, Y. (2024). More than an enforcement problem: The general data protection regulation, legal fragmentation, and transnational data governance. *Columbia Journal of Transnational Law*, *62*(1), 1–39.

Marchant, G. E. (2020). Governance of emerging technologies as a wicked problem. *Vanderbilt Law Review*, *73*(6), 1861–1878.

Ollier-Malaterre, A. (2023). *Living with digital surveillance in China: Citizens' narratives on technology, privacy, and governance*. Routledge.

Organisation for Economic Co-operation and Development. (2002). *OECD guidelines on the protection of privacy and transborder flows of personal data*. https://doi.org/10.1787/9789264196391-en

Patterson, M. R. (2010). Standardization of standard-form contracts: Competition and contract implications. *William and Mary Law Review*, *52*(2), Article 327. https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=1201&context=faculty_scholarship

Peng, C., Shao, G., & Zheng, W. (2023). China's emerging legal regime for privacy and personal information protection. *Tsinghua China Law Review*, *15*. https://www.tsinghuachinalawreview.law.tsinghua.edu.cn/issues/info/10300

Pernot-Leplay, E. (2020). China's approach on data privacy law: A third way between the U.S. and the E.U.? *Penn State Journal of Law and International Affairs*, *8*(1), 49–117. https://elibrary.law.psu.edu/cgi/viewcontent.cgi?article=1244&context=jlia

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 (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L119/1. https://eur-lex.europa.eu/eli/reg/2016/679/oj/eng

Ryngaert, C., & Taylor, M. (2020). The GDPR as *Global* data protection regulation? *AJIL Unbound*, *114*, 5–9. https://doi.org/10.1017/aju.2019.80

Sacks, S., Zeng, K. C., & Webster, G. (2024). *Moving data, moving target: Uncertainties remain in China's overhauled cross-border data transfer regime*. DigiChina. https://digichina.stanford.edu/work/moving-data-moving-target

Safari, B. A. (2017). How Europe's GDPR will set a new global standard for personal data protection. *Seton Hall Law Review*, *47*(3), 809–848.

Stalla-Bourdillon, S. (2024). *Global governance of cross-border data flows*. Centre on Regulation in Europe. https://cerre.eu/wp-content/uploads/2024/09/CBDT_FullBook_FINAL.pdf

Tan, W. (2024). National security as the trump card: Assessing China's legal regime on cross-border data transfer. *Information & Communications Technology Law*, *33*(3), 368–383. https://doi.org/10.1080/13600834.2024.2375125

Vosst, W. G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*(3), 485–532.

Wang, R., Zhang, C., & Lei, Y. (2024). Justifying a privacy guardian in discourse and behaviour: The People's Republic of China's strategic framing in data governance. *The International Spectator*, *59*(2), 58–76. https://doi.org/10.1080/03932729.2024.2315064

Wang, Y. (2022). National model and reflection on cross-border data flow governance. *International Economic and Trade Exploration*, *1*, 99–112. http://qikan.cqvip.com/Qikan/Article/Detail?id=7106644020

Whiting, S. H. (2017). Authoritarian "rule of law" and regime legitimacy. *Comparative Political Studies*, *50*(14), 1907–1940. https://doi.org/10.1177/0010414016688008

Xie, T., Liu, J., Sengstschmid, U., & Ge, Y. (2023). *Navigating cross-border data transfer policies: The case of China*. Asia Competitiveness Institute Research. https://doi.org/10.2139/ssrn.4408947

Zhang, A. H. (2024). *High wire: How China regulates big tech and governs its economy* (1st ed.). Oxford University Press. https://doi.org/10.1093/oso/9780197682258.001.0001

Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, *3*, Article 6. https://doi.org/10.1007/s44216-024-00028-2

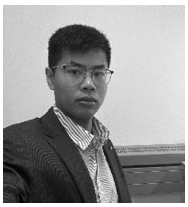
Zhang, Y. (2024). *Personal data protection and data transfer regulation in China*. Vrije Universtiteit Brussel. https://brusselsprivacyhub.com/wp-content/uploads/2024/04/Personal-Data-Protection-in-China.pdf

Zhao, J. (2023). On the systematization of data cross-border assessment, contracts and authentication rules. *Administrative Law Review*, *1*, Article 78.

Zheng, G. (2021). Trilemma and tripartition: The regulatory paradigms of cross-border personal data transfer in the EU, the U.S. and China. *Computer Law & Security Review*, *43*, Article 105610. https://doi.org/10.1016/j.clsr.2021.105610

About the Authors

Ruoxin Su is a doctoral researcher at the Vrije Universiteit Brussel. Her PhD research focuses on the use of genetic data in scientific research from a comparative perspective through EU and Chinese law. Her research areas also include Chinese digital laws and policies and medical device cybersecurity.



Dechun Zhang is a postdoctoral researcher at the Center for Tracking and Society in the Department of Communication, University of Copenhagen. His research focuses on political communication, digital politics, propaganda, and online participation. His work has appeared in several journals, book chapters, and international conferences, including *Journalism Practice*, among others.

Politics and Governance
2025 • Volume 13 • Article 10361
https://doi.org/10.17645/pag.10361

cogitatio

ARTICLE

Open Access Journal

A Geopolitical Economy Analysis of China and India's Approaches to Transnational Data Governance

Yujia He [1] and Ka Zeng [2]

[1] Patterson School of Diplomacy and International Commerce, University of Kentucky, USA
[2] Department of Political Science, University of Massachusetts Amherst, USA

Correspondence: Yujia He (yujia.he@uky.edu)

Submitted: 18 March 2025 **Accepted:** 10 July 2025 **Published:** 10 September 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

Recent literature on the behavior of rising powers in digital trade and data governance highlights their discourses of data sovereignty and desire to preserve domestic policy autonomy. This article contributes to the literature by employing a political economy lens that shifts the focus from the nation-state/inter-state framework towards the dynamics of state–capital relations, allowing for a more historical and contextual understanding of the geopolitics of data governance in emerging economies. Using China and India—two of the largest emerging economies—as comparative cases, and drawing on secondary data from government documents and other sources, the article argues that the interplay between the state's interests in promoting security and development objectives and the commercial interests of domestic firms, global Big Tech companies, and transnational capital in data commercialization and market expansion has shaped the two countries' respective trajectory of data governance over the past three decades. These developments are deeply embedded in each country's distinctive political economic and geopolitical contexts. As a result, key policy developments in digital governance that might appear to be driven primarily by geopolitics may instead have deeper roots in evolving state–business relations.

Keywords

China; data governance; economic interests; geopolitics; India; rising powers

1. Introduction

With the rapid pace of digital transformation across the Global South, an increasing number of emerging economies, especially the BRICS (Brazil, Russia, India, China, and South Africa), have developed their distinct

approaches to transnational data governance based on the notion of "data sovereignty" (Belli et al., 2024). As the cyberspace becomes less Western-centric, rising powers also call for more representation in global digital trade and data governance (He & Zeng, 2024). Policymakers and academics have contested the existing US-centric multistakeholder governance model, arguing that it privileges the interests of the private sector and reinforces the dominance of the incumbent powers (Arsène, 2016). There is considerable speculation about whether the ascendence of these emerging digital economies may generate further tensions in this "post-liberal order" (Barrinha & Renard, 2020, p.749), and whether transnational data governance as an emerging arena of geopolitical tensions may threaten "international coordination in the global data economy" (Arner et al., 2022, p.623).

Much of the recent international relations literature discussing the behavior of rising powers in transnational data governance highlights their discourses of sovereignty and desire to preserve domestic policy autonomy (Adonis, 2019). It is certainly useful, and should be commended, to "bring the state back in" to the discussion of global internet governance (Drezner, 2004, p. 477), an approach that could mitigate the epistemological focus on technical design negotiations in earlier literature (DeNardis, 2009). However, by contrasting the positions of emerging powers with those of the US, this framing risks overlooking the historical contexts of domestic tech industry development and the dialectical relationship between the state and transnational capital and tech companies.

This article adds to the literature by employing a (geo)political economy lens that shifts from either the dominant state-centric/inter-state framework or the earlier focus on technical design and administration of networked technologies, towards the local dynamics of state–firm relations. While not seeking to minimize the importance of inter-state power competition, this study contends that political economic forces, specifically the dynamic relations between the state and capital (both domestic and international), are important in shaping emerging economies' evolving approaches to data governance, behind the often-used buzzword of data sovereignty. The study seeks to answer the following research question: How have the interactions between state interests and the interests of domestic and international capital influenced the rising powers' approach to transnational data governance under evolving global geopolitics?

The study argues that for large emerging economies such as China and India, the interests of the state in promoting security and development objectives, along with the commercial interests of platform companies and transnational capital in data commercialization and market expansion, conditioned by their respective geopolitical as well as domestic political economic contexts, have shaped their evolving approaches to data governance. As digital platforms become infrastructuralized and transnational while amassing vast amounts of citizen data, both states have also considered data as assets with economic and strategic value and developed regulations against the background of shifting global geopolitical dynamics. Regulations concerning cross-border data remain in flux, with nuances, flexibilities, and even scale-backs in policy formation and implementation.

2. The Geopolitical Economy of Data Governance

2.1. Understanding Transnational Data Governance in Emerging Economies: The Limitations of a State-Centric Approach

Extant literature on data governance tends to focus on technical design and network administration, distinct national or supranational approaches to data governance, and patterns of global governance. One strand of the literature focuses on data standards, architecture, infrastructure, interoperability, privacy protection, and anonymization techniques and how they may affect compliance with data governance rules such as the European Union's (EU's) General Data Protection Regulation (GDPR; Khatri & Brown, 2010; Mishra, 2021; Purtova, 2018). As Tang (2022b) pointed out, the earlier mainstream internet governance scholarship focused on technical architectures and protocols, concerns which were in part driven by the dominant multistakeholder governance approach (DeNardis, 2009).

Another stream of the literature highlights distinct national approaches to data governance, showing a broad contrast between the emerging economies' data governance approaches and those of the incumbent Western powers. Large emerging economies, especially the BRICS, have pursued "digital sovereignty" or, specifically regarding data governance, "data sovereignty," as fundamental elements of their digital transformation (Belli et al., 2024). The concept of "digital sovereignty" has emerged as a political buzzword invoked in diverse narratives, policy discourses, and governance practices across multiple countries and regions (Pohle et al., 2024). Generally, it refers to "calls for a stronger role for the state, for strategic autonomy and digital borders," shown in national initiatives "aimed to regain control over strategic data, such as policies of data localization or reshaping of the architecture of connectivity," and its various discourses and practices represent a "condensation and materialization of these new geopolitics of data flows" (Glasze et al., 2023, p. 920). In contrast, the US government has long pursued a market-driven approach to data governance, protecting cross-border data flow, preventing data localization and web blocking, ensuring digital security, and facilitating internet services (Fefer, 2020). While the EU similarly encourages cross-border data flows, its emphasis on the protection of personal data and privacy, and increasing concerns about economic competitiveness, strategic autonomy, and technological sovereignty, have contributed to a rising EU digital sovereignty discourse that allows limited exceptions to free flows (Falkner et al., 2024; Farrand & Carrapico, 2022; Floridi, 2020). Barrinha and Renard (2020, p.758) noted that there is a fundamental divide between countries that "defend the principle of cyber sovereignty and the need to maintain public order in the cyberspace" and those that champion "an open and free internet," reflecting broader tensions within a contested and shifting "post-liberal order." O'Hara and Hall (2018, pp. 6–9) similarly argued that the geopolitics of internet governance should be understood as an uneasy coexistence and competition between the "European bourgeois internet," the "Chinese and Russian authoritarian internet," and the "American commercial internet."

This division can also be found in discussions of global internet governance. Scholars have emphasized that the US, as the center of global digital capitalism and economic networks, holds structural power, which in turn solidifies the power asymmetry of the global communications networks. This allows the US to weaponize such "interdependence" for extraterritorial surveillance and sanctions as coercive tools at times of confrontation (Farrell & Newman, 2019). Nonetheless, the US dominance in global communications and the US-centric multistakeholder governance model have generated many grievances and contestations, on

the ground that the resultant global governance institutions prioritize the interests of the private sector, allow limited inclusion in participation, threaten the domestic policy autonomy of developing states, and sustain the dominance of the Western powers (Arsène, 2016; Jongen & Scholte, 2022). Research on the EU often highlights the so-called "Brussels effect," through which the EU leverages firms' desire to access its internal market to exert regulatory influence, resulting in the potential de jure or de facto harmonization of regulatory standards globally (Bradford, 2020). However, some question the long-term feasibility of the EU's regulatory influence and its ability to maintain digital sovereignty (Calderaro & Blumfelde, 2022). As geopolitical tensions rise among major powers, some scholars bemoan that data governance has become a "wicked problem" and that differing approaches among countries may threaten "international coordination in the global data economy" (Arner et al., 2022, p. 623) or even fragment the internet (Polatin-Reuben & Wright, 2014).

Recent international relations literature discussing data governance in relation to geopolitics often adopts a realist perspective, portraying states as engaged in a power struggle for status and influence within a competitive inter-state system. While some scholars also explore alternative dimensions of digital sovereignty such as citizens' empowerment against the tech sector (e.g., Mügge, 2024), or contest the state boundary-based thinking (Chander & Sun, 2023), the external dimension, characterized by a "state-centered and security-politics narrative" (Adonis, 2019), has gained prominence in discussions of the BRICS economies' approaches (O'Hara & Hall, 2018; Rosenbach & Mansted, 2019; Zinovieva & Shitkov, 2023). This state-centric focus mitigated the earlier tech-deterministic epistemological approaches that had rendered "the issue of state and sovereignty obsolete and irrelevant" (Tang, 2022b, p. 2399), calling attention to how internet governance rules are made and the power dynamics among nation states amidst geopolitical tensions.

However, perhaps unintentionally, by contrasting the data governance approaches of rising powers with those of the incumbent powers (notably the US) and emphasizing the latter's liberalization stance, this state-centric framing implicitly reinforces the earlier imagination of the internet as an open commons guided by market incentives with minimal government intervention (Lessig, 1998). As critical scholars of communications have argued, such an imagination overlooks the reality of the internet's Cold War origins, Washington's historically active role in shaping information and communication technology policies and practices in the developing world, and its long-armed control over American information and communication technology firms' international operations (Aouragh & Chakravartty, 2016; Cartwright, 2020).

Moreover, the state-centric and security-politics focus, while avoiding technical determinism, risks swinging the pendulum too far, giving inadequate attention to the roles of firms and their engagement with various players in policymaking and implementation, and the practices of data governance arising from these interactions. Major digital platform companies may assume the role of "ambassadors" of their home countries (Carr, 2016). However, for homegrown platforms in emerging economies like China and India, their relationships with domestic and foreign government entities, international tech firms, and transnational capital often involve a complex mix of collaboration and contestation (Shen, 2016; Thomas, 2019).

Notably, how data governance in emerging economies is influenced by the dialectical relations between the state and businesses remains largely underexplored. As Belli et al. (2024) argue, the simple division of liberal and non-liberal states can overlook the multi-faceted concerns for data sovereignty and the "complex 'datafied' global value chains dominated by financialized transnational companies headquartered in central

economies." Data regulations in emerging economies are often shaped by a combination of security, regulatory, economic, and technical considerations. These include safeguarding national security against emerging threats, protecting citizen rights, shielding public and private services from cybersecurity and privacy risks, ensuring domestic regulatory or legal compliance, promoting local industry and innovation development with global linkages, and fostering strategic autonomy to build digital capabilities independent of external actors (Belli et al., 2024; X. Chen & Gao, 2024; Foster & Azmeh, 2020; He & Zeng, 2024; Jiang, 2024). Our study extends the literature by emphasizing how the dynamic and evolving transnational data governance approaches of emerging economies are shaped not only by national security concerns driven by geopolitics but also by domestic political economy considerations.

2.2. Towards a Historical, Contextualized (Geo)Political Economy Lens

To overcome the limitations of the state-centric/inter-state framework dominant in recent literature, this study adopts an approach frequently utilized by political economy scholars of information that treats the cyberspace as "layered, varied and evolving" and as "a socio-technical and ultimately geopolitical environment" (Hong & Goodnight, 2020). This perspective "highlights the need to understand the historical contexts and dialectical relations" involved in "the enabling and conditioning of actors in policy processes" (Tang, 2022b). Instead of treating the internet as a boundless, frictionless open commons, critical political economy scholars view it as a space fraught with tensions and contradictions. Therefore, the subjectivity of various actors within and beyond the state and the power dynamics among them in rule-making are important considerations (Mosco, 2009).

As this study illustrates, the development of data governance approaches in both China and India is influenced by the dynamic interplay between the governing authority, the domestic tech platforms, private capital, and international tech firms and transnational capital. This relationship is deeply rooted in the unique historical development of digital industries and local socioeconomic contexts. In both cases, we are interested in key turning points in each country's data governance regime as our dependent variable, with business–state interactions serving as the main independent variable. While the specific pathways linking the two diverged somewhat in the two countries, our analysis underscores the similarities in how external pressures were filtered through the domestic political economic landscape as interest groups in each country navigate the respective institutional setting to mold the policy outcome.

In this vein, this study contributes to the emerging political economy literature on the evolving digital landscape in emerging economies against the backdrop of geopolitical tensions (W. Chen, 2022; Grover et al., 2024; Kumar & Thussu, 2023; Lei, 2023; Schroeder, 2022; Shen & He, 2022; Tang, 2022b). As Qiu et al. (2022, p. 2335) proposed:

> A novel geopolitical approach analyzes 'Chinese internets' as internally diverse and externally border-crossing; as both public (governmental and non-governmental) and private (e.g., corporate); as discursive and policy entanglements beyond the dichotomy of multistakeholderism and multilateralism; and as global, regional, and local formations that are connected to, but not entirely constrained by, their national counterparts.

Similarly, this study treats the geopolitics of data regulations in emerging economies as an evolving and dynamic process that involves public and private players both internally and externally, with the state's key

policy responses to heightened external risks underpinned by such two-way interactions. Analytically, this historical, contextualized approach to explaining changes in transnational data governance based on the dialectical relations between state institutions, private platforms, and capital resonates with L. Zhang and Chen's (2022, p.1454) call for a "regional and historical approach" that helps to "deprovincialize platform studies and extend its analytical relevance beyond the Euro-American focus or the disciplinary boundaries."

This study additionally echoes the call for a "geopolitical economy" research agenda in international relations, moving beyond "geopolitical fetishism" and the narrow strategic or security-centric focus common in policy analysis (Jayasuriya, 2021). As Wijaya and Jayasuriya (2024, p. 2139) argue, one of the most significant developments in international political economy in the past few years has been "the emergence of a new business class in emerging markets with international connections." These emerging market multinationals "seek to shape new projects of globalization which are often, confusingly, seen as new forms of statism" (Wijaya & Jayasuriya, 2024, pp. 2139–2140). This study's analysis similarly highlights how emerging economies' regulatory approaches to data governance have in part been influenced by the logic of capitalist accumulation by private companies. Domestic private digital platforms have grown with both the help of international capital and technology partners in a domestic policy environment that enables market expansion and the gathering of user-generated data. Having built "ecosystems" that straddle domestic public and private services, these homegrown platform companies are also internationalizing (J. Y. Chen & Qiu, 2019; Shen & He, 2022). In response, emerging economies' governments, through digital policy and data regulations, seek to facilitate the firms' capitalist accumulation, while also guarding against possible risks to political stability, including those brought by their international linkages. Meanwhile, the interplay among various domestic and international players, and the realignment of actors in the accumulation process are deeply influenced by each country's domestic political, socioeconomic, and geopolitical circumstances, leading to varied data governance approaches. Consequently, key policy developments in both countries' approaches to data governance that may, at first glance, be attributed to geopolitical tensions may instead need to be placed in the context of evolving state–business relations in their domestic political economy.

3. Methodology

This study employs a qualitative and comparative case study approach that enables an in-depth exploration of emerging economies' evolving approaches to data governance (Ragin & Becker, 1992). Specifically, it addresses the question of how the state's interests in national development agendas and the domestic and transnational private capital's business interests interact to shape government regulations concerning data governance amidst changing global information geopolitics. Such an approach provides valuable insights into not only broad patterns but also variations across cases, therefore contributing to more nuanced explanations of how data governance regimes have evolved in different national contexts. China and India were chosen as the case studies as they are the two largest emerging economies in terms of both the size of their economy and the number of internet users (World Bank, 2024). Qualitative data were collected through a systematic review of scholarly literature, news articles, official documents and government policies, and speeches by government officials and business leaders, to allow for in-depth analysis and systematic comparison of regulatory developments over the past three decades. Data analysis was performed concurrently with data collection to compare the findings against the initial propositions derived from the literature review.

4. The Case of China

This section traces the geopolitical economy of China's data governance development, emphasizing the mediating role of the dialectical relationships between the Chinese state and capital.

4.1. Early Developments in State–Business Relations in Digital Governance: 1990s–Early 2010s

In the early years of its digital economy development from the 1990s until the late 2000s, the Chinese state's approach to internet governance simultaneously emphasized the potential of digital connectivity to facilitate knowledge transfer, trade and economic development, domestic capacity development through joint ventures, and the preservation of national sovereignty and political stability through information control but pluralization of online discourses (Han, 2018; Shen, 2016; Tang, 2022b). Such a permissive policy environment enabled the expansion of Western technology companies such as IBM, Microsoft, Dell, Cisco, Amazon, and Google in the Chinese market, often in partnership with Chinese businesses in the form of joint ventures. China was a latecomer to data governance, with only three domestic regulations over data concerning ID card data, information security protection, and medical data confidentiality by 2010 (Sacks et al., 2019). Moreover, coordination among ministries, even at the central level, was limited (Shen, 2016).

With the rise of new technologies such as cloud computing and the government's shift towards high-tech development in economic planning in the late 2000s and early 2010s, the Chinese government sought to provide a favorable policy environment to promote the development of the digital sector as one of the pillars of the national economy. The State Council named next-generation computing as one of the "strategic emerging industries" in 2010, with significant implications for economic growth and the structural upgrading of the economy, followed by a series of official documents and policies from the relevant government ministries (State Council of the People's Republic of China, 2010). Meanwhile, domestic tech companies such as Baidu, Alibaba, and Tencent (collectively known as BAT) had sprung up as strong rivals to global tech firms in the Chinese market, bolstered by the financial backing of transnational venture capital and the expertise of senior executives with prior experience in Western tech firms (Shen, 2019).

4.2. The Snowden Revelation as a Catalyst for Change: Rising Data Regulations in the 2010s

Notably, China's data governance regulations took a sharp upturn in 2013 (Sacks et al., 2019) in response to Edward Snowden's revelation of the US government's global surveillance networks which, by reinforcing concerns about data security and information geopolitics, provided renewed impetus for the Chinese government to reform internet governance and emphasize data localization. Chinese official media expressed concerns that the operation of eight US technology companies—Apple, Cisco, Google, IBM, Intel, Oracle, Qualcomm, and Microsoft—in the Chinese market may enhance the ability of the US National Security Agency to influence the Chinese government, military, businesses, and academic institutions (Tang, 2022b). The central government subsequently created the Central Leading Group for Cyberspace Affairs and the Cyberspace Administration of China (CAC) in February 2014 to strengthen oversight of China's internet security and the implementation of its internet governance strategy. The CAC took over the responsibilities of the joint task forces under the State Council for safeguarding the strategic importance of China's information industry. A flurry of policies was created in the next few years, including the Internet Plus policy, which systemically planned the development of digital infrastructure and industrial ecosystem, and the

National Cyber Security Strategy, both in 2016, and numerous legal amendments and administrative regulations covering various aspects of internet governance. Market entry was tightened: For example, the Ministry of Industry and Information Technology revised the telecom business catalog in 2015 and identified cloud computing as a value-added service for which a pre-operation license would be required. The most notable legal development was the passage of the 2017 National Cybersecurity Law. Building on previous regulations, this law tightened data localization policies by requiring "critical information service providers" to store personal information or important data within the national border (Creemers et al., 2017).

4.3. Changing Power Dynamics in Chinese Tech Industry Development in the 2010s

The above policy changes contributed to shifting power dynamics and actor realignment in the capitalist accumulation of the Chinese tech industry. Transnational capital and Western tech firms were still important business partners in financing and joint projects with domestic platforms and venture capital (Tang, 2022a), and institutes such as Microsoft Research Asia were instrumental in producing talents who went on to work in Chinese tech firms and found startups. Yet with the industrial planning and localization policies, domestic platforms grew much more rapidly and became influential "ecosystem builders." Some local governments, eager to show alignment with the central government's agenda and willingness to support the local economy, also facilitated the market expansion of domestic tech firms through government contracts or public–private partnerships like Alibaba's Taobao Villages pilots in Zhejiang Province. The liberal and enabling environment for investment in the tech sector allowed Chinese homegrown platforms such as BAT and newcomers like ByteDance to acquire an enormous amount of economic power by expanding services beyond their core business to encompass almost all of Chinese users' online and offline activities, essentially achieving an infrastructural role in the Chinese society (Plantin & De Seta, 2019; Shen, 2021; Tang, 2019). This newly emerged platform capitalism, however, elevated the platforms' power and position vis-à-vis government officials (Su & Flew, 2020) and, in some cases, left regulators relatively powerless vis-à-vis corporate giants (Qiu, 2023). As Qiu (2023) argues, because of the rising power of China's tech giants, Beijing increasingly faced the dilemma of further liberalizing the domestic economy and promoting China's integration into the liberal international economic system on the one hand and maintaining the party-state's continued autonomy and leadership on the other.

Meanwhile, Chinese platforms started expanding internationally, resulting in record-high overseas investments by 2016 (He, 2024a). Some followed a deliberate "parallel platformization" approach to fit the divergent policy frameworks and platform ecosystems in China and abroad, such as ByteDance's video-sharing apps Douyin in China and TikTok overseas (Kaye et al., 2021). Nonetheless, similar to American platforms like Facebook and Google that came under increasing regulatory oversight both domestically and overseas, these Chinese infrastructuralized platforms' expansion in the global internet soon faced not just concerns about their dominating socioeconomic power and potential political leverage within China, but also their international operations and cross-border data flows. This was evidenced by new legal developments overseas that echoed the concerns of Chinese regulators (Wang & Gray, 2022). For example, the EU's GDPR, adopted in 2016, was a milestone legislation mandating data privacy of EU citizens for firms seeking access to the EU market, amplifying calls for the development of similar data protection laws in China. Rising geopolitical tensions further subjected these Chinese platforms to closer scrutiny from overseas regulators, notably the US.

4.4. Shifting State–Business Relations and Data Regulations Amidst Rising US–China Tensions and Internal Challenges

Once again, geopolitical tensions following the US–China trade war starting in 2017 provided the pretext for Beijing to engage in stricter regulations and to eventually crack down on domestic platforms since 2020. The US Trump administration used "national security" as justification to address China's trade practices, trade surplus with the US, and competitive challenges in high-technology development (Sun, 2019). In addition to imposing sanctions on Chinese telecom equipment providers Huawei and ZTE, Washington took a series of actions against Chinese platforms, including the proposed ban of TikTok, opposition to Ant Financial's acquisition of Moneygram, and the Clean Network Initiative, which sought to prohibit Chinese cloud providers from operating in the US and allied countries (He, 2024b; Shen & He, 2022; Steinbower, 2020).

Domestically, the heydays of neoliberal platform capitalism gradually came to an end in 2020, giving way to a new era of tighter control under "state platform capitalism" (Rolf & Schindler, 2023), whereby the state began to exert growing influence over platform development. Notably, rising inequality and poverty in the Chinese society prompted the central leadership under Xi Jinping to consolidate power and to counter threats to political stability and the legitimacy of China's techno-nationalist agenda by, among other measures, introducing reforms to digital governance to reassert government control and promote more balanced socioeconomic development (Au, 2023; A. H. Zhang, 2024; Zhao, 2022). Official discourse emphasized "common prosperity" and the "virtual economy serving substantive economy," justifying the tech crackdown as a policy experiment to combat rising inequality (Qiu, 2023).

Heightened geopolitical contestations provided further impetus for the government to strengthen data protection and enhance data security frameworks, especially as they relate to personal data. Beijing introduced a series of regulatory and legal measures, including the imposition of export controls on algorithms used in social media platforms in August 2020, a move that is widely perceived to influence the overseas operations of TikTok and other Chinese firms. In October 2020, Chinese officials halted the 34 billion USD initial public offering (IPO) of Ant Group, the financial services arm of Alibaba, on the Shanghai and Hong Kong stock exchanges, presumably in a move to reassert the government's authority over domestic commerce and society and to enforce the party's will (Zhong, 2020). This was followed by the levying of a record 18 billion RMB (2.75 billion USD) fine on Alibaba for allegedly abusing its dominant market position according to an anti-monopoly probe (Murdoch & Stanway, 2021). In 2021, two major new legal developments significantly reshaped China's data governance landscape. The Data Security Law introduced requirements for government approval for the transfer of data stored in China to protect national security and public interest (Creemers, 2022), including more stringent requirements for processing "important," "core state," or "sensitive" data (Belli, 2021). Another legislation, the Personal Information Protection Law, regulated the collection and processing of personal data, further expanding the scope of application of the earlier National Cybersecurity Law and broadening data localization requirements (Creemers, 2022). While the Personal Information Protection Law bears resemblance to the GDPR in its scope, key principles, and concepts, and in the provision of some important safeguards to protect individuals, it also diverges in certain areas. These include the lack of meaningful constraints on the state's access to and use of personal data, the institutional arrangements to enforce the law, and the imposition of ex ante state oversight on data localization (Creemers, 2022; W. Li & Chen, 2024).

The case of Didi further illustrates the evolving power dynamics between platform companies and the state. In June 2021, the CAC initiated antitrust investigations against the ride-hailing giant Didi Chuxing, shortly after its successful IPO on the New York Stock Exchange caught the regulators by surprise. The CAC stated that the firm had breached data protection rules and issued an order to remove Didi's app from local app stores (Eamon & Lau, 2021). Didi was fined 8 billion RMB (1.2 billion USD) for violating data privacy, data security, and cybersecurity laws, and was subsequently delisted from the New York Stock Exchange in June 2022 (Warren & Zhu, 2022). Although initially viewed as a partner in digital development, Didi gradually came under increased government scrutiny as concerns grew over the national security risks posed by foreign entities potentially accessing vast amounts of sensitive data (C. Zhang, 2024). The listing of companies such as Didi in the US may have further heightened concerns that such firms might be compelled to comply with foreign regulations and even cede their data to foreign governments, thereby compromising Beijing's oversight. A new version of the Cybersecurity Review Measures took effect in 2022, requiring businesses holding more than one million Chinese individuals' data to apply to the CAC for authorization and pass a cybersecurity review before being listed overseas (Warren & Zhu, 2022).

However, amid the economic downturn compounded by the Big Tech slump and the pandemic, the Chinese government has come under increasing pressure to strike a balance between regulation and business facilitation, prompting the relaxation of certain cross-border data transfer requirements and introducing flexibilities in actual policy implementation. For example, in 2024, one year after implementing the Measures of Security Assessment for Data Export, the CAC narrowed the scope of the security assessment mandate, clarified alternative compliance mechanisms (such as standard contracts and certification), and expanded the range of business scenarios that qualify for exemption from compliance requirements, in an effort to reduce firms' compliance burdens (CAC, 2024; Tencent Research Institute, 2024). Numerous Free Trade Zones in China worked with firms and local cyberspace administrations to implement "negative lists" of cross-border data transfer, essentially exempting some businesses from strict compliance requirements ("Shuju kuajing liudong de zhongguo fangan," 2024). Businesses in the Guangdong–Hong Kong–Macao Greater Bay Area were allowed to coordinate data transfer between the mainland and Hong Kong/Macao through the Greater Bay Area Standard Contract (Au & Witzleb, 2024). In its effort to revive foreign investment, Beijing also faced the imperative to address foreign firms' concerns over regulatory constraints on data transfers. For example, European industry lobbying was among the factors leading the CAC to significantly relax its data export rules in 2024 (Arcesati, 2024). The Regulations on Network Data Security Management, active in 2025 following three years of discussions with stakeholders, further eased restrictions on cross-border data transfer, while clarifying firms' compliance obligations (including special requirements for large platforms), liabilities for violations, and measures for strict enforcement (B. Li, 2024).

Consequently, instead of approaching the Chinese data governance regime merely from the perspective of great power competition between two major internet powers, recent policy development should be viewed in the context of the historical trajectory of the Chinese tech industry and the evolving, dialectical relationships between the Chinese government, domestic firms, and global capital. While the state undertook major initiatives in response to rising external and internal pressures, firms were not completely passive receivers of regulatory shifts; instead, they actively influenced the implementation or interpretation of high-level laws by leveraging their economic significance.

5. The Case of India

This section examines the geopolitical economy of India's evolving data governance approach, focusing on the historical development of India's tech industry and its evolving relationships with the Indian state, foreign platforms, and transnational capital.

5.1. Historical Path of State–Business Relations in Digital Development

With the transition from Soviet-style central planning and self-sufficiency towards more open trade and investment promotion in the 1980s and 1990s, India emerged as an important global player in software and IT services, hosting numerous major companies such as Tata Consulting Services and Infosys and subsidiaries of international firms such as Motorola. However, in comparison to China, internet services such as e-commerce grew much more slowly in India, due to relatively low internet penetration, slow network speeds, diminished spending power of citizens, poor supporting infrastructure, and limited policy support (Singh, 2016; Subramanian, 2020; Thomas, 2009).

Nonetheless, a major wave of growth started in the late 2000s with the rise of homegrown companies like Flipkart, which was established in 2007 and became a leading e-commerce platform in India before its acquisition by Walmart in 2016. The entry of global platforms (eBay in 2004, Facebook in 2006, Amazon in 2013) led to the expansion of transnational tech capital within India's nascent internet industry. Meanwhile, until the early 2010s, the Indian government had implemented only a few regulations on data governance, mainly the IT Act and its amendments and regulations. These regulations focused on expanding the government's power of information monitoring and developing security practices and procedures for dealing with sensitive personal information (Chaudhuri & Joseph, 2024). Enhanced government surveillance drew criticisms from civil society, yet the government justified the legislation on the grounds of fighting terrorism and cybercrime (Subramanian, 2020).

5.2. Changing State–Business Relations Under Modi's "Digital India" Campaign

Prime Minister Narendra Modi's tenure as the country's leader starting in 2015 saw seismic changes in India's digital policy and state–business relations. Digital India, his flagship policy project, seeks to "transform India into a digitally empowered society and knowledge economy," envisioning "infrastructure as a utility to every citizen," "governance & services on demand," and "digital empowerment of citizens" (Ministry of Electronics and Information Technology of India, n.d., p. 14). The passage of the Aadhaar Act in 2016 launched a nationwide digital identity platform and created the world's largest biometric and personal information database containing Indian citizens' pictures, iris scans, and fingerprints, and the assignment of a unique identification number overseen by the Unique Identification Authority of India. A collection of associated software platforms and applications, called the "India Stack," was developed based on the state-generated Aadhaar database, and was promoted as a unique digital infrastructure to help India's digital transformation (Parsheera, 2024). For example, the United Payments Interface (UPI), a real-time instant payment system, was developed by the government for online payments. The 2016 demonetization initiative, by demonetizing certain banknotes (albeit with a haphazard rollout), facilitated the rapid rise of digital payments. As Hicks (2020, p. 331) has argued, the India Stack represents India's move towards "hybrid state–business digital capitalism." Mishra (2023, p. 255) critically characterized the government's close ties

with certain private companies as a relationship in which "the government depend[s] on the private sector for intimate surveillance of citizens, and the private sector depend[s] on the public digital infrastructure."

The datafication of the Indian society and the resultant market expansion of its tech industry led to rising interest from global tech capital and broadened India's integration in global digital capitalist networks. Global Big Tech and capital played major roles as shareholders and partners of domestic players. For example, Jio Platforms, the digital business arm of India's largest family-owned conglomerate and telecom provider Reliance Industries, raised billions of dollars from Google, Facebook, and private-equity firms like Silver Lake (Otto & Bellman, 2020). Chinese platforms and capital were also active: Before India tightened investment by Chinese firms in 2020, Chinese investors such as Alibaba, Tencent, and ByteDance held stakes in 18 of India's 30 unicorns (startups valued at over 1 billion USD), often alongside other major global investors like SoftBank, Sequoia Capital, and eBay (Bhandari et al., 2020).

5.3. Evolving Relations Between State and Non-State Actors Shaping India's Data Regulations Development

India's evolving data governance approach mirrored the government's intent to capitalize on the economic value of data and to promote platform capitalism by shaping market expansion, along with its quest for sovereignty and political stability. Rhetorically, "Data is the new gold (or oil)" was the catchphrase used in Modi's public speeches (Vila Seoane, 2021) and in documents such as the Draft E-Commerce Policy (Mishra, 2023) to justify data localization proposals. Sector-specific regulations mandating data storage on servers located in India were introduced in the telecom, banking, and health sectors. These included the 2018 Reserve Bank of India (India's central bank) regulation to require all system providers to store payment transactions data in India, and a subsequent decision in 2021 to bar new customer onboarding for payment services like Mastercard until successful compliance (Basu & Swaminathan, 2023). However, given India's limited state capacity, some argue that these regulations were not strongly enforced (Mishra, 2023).

Meanwhile, the desire to attract international capital investment and technology partnerships seemed strong enough to prompt the government to make some compromises. During the negotiations over the Regional Comprehensive Economic Partnership (RCEP), a mega free-trade agreement in the Asia Pacific region, India relaxed its foreign direct investment restrictions on e-commerce to allow for 100% foreign ownership. India also reversed early objections to RCEP's e-commerce draft chapter, which contained a prohibition of data localization but provided broad carve-outs for domestic security and public policy exemptions, to allow the chapter to go through. However, India ultimately withdrew from the RCEP negotiations in 2019 due to other concerns (He & Zeng, 2024).

The evolving relationships between the government, domestic businesses, and foreign Big Tech, grounded in India's political economic context, were apparent in the debates shaping India's key data legislation. The first draft of the Personal Data Protection Bill in 2018, along with its 2019 revised version, shared many high-level principles and specific provisions with the EU's GDPR. However, crucial divergences remained, including in international data transfer (Sen, 2021; Wimmer et al., 2020). The Bill advised prohibiting the transfer of "critical personal data" beyond Indian borders, and the processing of such data exclusively within India to avoid foreign surveillance, apparently alluding to the Snowden revelations of US intelligence operations (Vila Seoane, 2021). Geopolitical framing was employed to push for data localization. Prominent

politicians of Modi's ruling Bharatiya Janata Party, which has a history of nationalist ideology, framed Western platforms' dominance in the Indian market as "digital colonialism," and data localization requirements as necessary countermeasures (Vila Seoane, 2021). Domestic firms that stood to benefit from exclusive data access and localization, including platforms like Paytm, and conglomerates like Reliance, which owns Jio Platforms, similarly touted localization requirements (Basu & Nachiappan, 2020). Chinese tech firms like Alibaba, having invested in physical data centers in India, also supported data localization. Meanwhile, US firms fiercely opposed data localization, enlisting lobbyist groups to engage US officials and Indian lawmakers to express concerns (Kalra, 2019). The US Trump administration subsequently made data localization a crucial talking point in US–India trade negotiations and threatened retaliation. Industry associations such as the Internet and Mobile Association of India also opposed data localization, citing the cost to start-ups and hurdles to innovation (Sinha & Basu, 2019). After several revisions and the withdrawal of the initial bill, the final Digital Personal Data Protection Act was passed in 2023. Compared to the initial draft, the final Act was significantly watered down in data localization requirements, permitting data transfer outside India to countries other than those blacklisted by the central government, while allowing sector-specific regulations. Nevertheless, it expanded the government's power over data usage and commercialization, granting broad exemptions for government agencies and providing the government with discretion to exempt certain companies from compliance while subjecting others to increased scrutiny (Grover et al., 2024).

5.4. Rising State Scrutiny of Platforms' International Capital Linkages and Data Practices

Another case of evolving relationships between the state, domestic platforms, and transnational capital concerns the UPI payments, which involved three major platform players, including the Walmart-owned PhonePe (part of Flipkart), Google Pay, and the homegrown Paytm. Following the 2020 Sino-Indian border clash, the Modi government banned scores of Chinese apps out of security concerns, and tightened investment rules in India for Chinese companies (Kharpal, 2020). At the time, Paytm was 30% owned by Ant Group and had received capital and technology support, as noted in Ant Group's IPO prospectus. The imposed restrictions subsequently prohibited any further investments. In 2022, the Reserve Bank of India punished Paytm for data flows overseas to Chinese entities that indirectly held stakes in the firm, while Paytm denied the allegations (Roy & Rai, 2022). In the same year, the Reserve Bank of India rejected Paytm's payment aggregator licensing application, granting the company an extension to reapply by March 2023. To alleviate concerns over Chinese investment, Ant Group reduced its stake to 9.88%, so that by August 2023, Paytm's CEO became the single-largest shareholder (Cornish, 2023). In early 2024, regulators closed part of Paytm's payment business for numerous compliance issues. Regulatory restrictions led to Paytm's market share shrinking to 8%, in comparison to PhonePe and Google Pay which processed 87% of UPI transactions. Meanwhile, a parliamentary panel report raised concerns of the foreign duopoly dominating the payments market, urging the government to support domestic fintech growth. By October 2024, regulators approved Paytm's onboarding of new users, while delaying actions on capping market share for PhonePe and Google Pay (Shetty, 2025). This suggests that while the government is still prioritizing the growth of the digital economy in view of the "emerging" stage of India's development, the platforms' expansion may continue to be subject to the state's scrutiny of their international capital linkages and data practices amidst geopolitical tensions.

6. Conclusion

This study seeks to unpack the dynamics of transnational data governance in large emerging economies, namely China and India, by examining the historical contexts of tech industry development and highlighting the mediating role of state–capital relations against the background of evolving global geopolitics. It contributes to the growing political economy scholarship on how geopolitical tensions shape internet governance and digital platforms development in emerging economies (Qiu et al., 2022; Shen & He, 2022; Tang, 2022b). Analytically, it advances the literature by employing a regional and historical approach to study platform capitalism (L. Zhang & Chen, 2022). More broadly, this study echoes the call for a geopolitical economy approach in international relations research that goes beyond "geopolitical fetishism" to understand geopolitical contestations within the broader context of capitalist transformation (Wijaya & Jayasuriya, 2024). Because of space constraints, this study does not discuss in-depth the institutional transformations within various state agencies or the role of civil society in influencing policymaking. Nevertheless, it serves as an exploratory endeavor to move the analysis beyond the narrow focus on inter-state security politics, towards a broader consideration of the interactions among various state and non-state actors.

Several conclusions and implications for research can be drawn from the above comparative case studies. First, both cases show that the geopolitics of transnational data governance in emerging economies should be approached not simply from the realist perspective of inter-state security politics seen in much of the digital sovereignty literature, but also from a political economy lens that gives more attention to the interactions among state and non-state actors rooted in the domestic socioeconomic contexts of technology industry development. In both the cases of China and India, the government's interests in shaping the domestic digital economy and promoting market expansion to serve the overall national development agenda, along with interests in maintaining national security and political stability, have been an essential focus of data governance regulations. Various private-sector entities are also important players in tech industry development and, in turn, data policy formulation in both countries. They include homegrown platforms that are increasingly infrastructuralized and internationalizing, other forms of domestic private capital, and global firms and transnational capital (such as global venture capital, private equity firms, and international stock markets) that seek to expand capitalist accumulation in emerging markets. The relationships amongst these non-state players and the government involve both collaboration and competition and, indeed, realignment under global information geopolitics (e.g., concerns over surveillance following the Snowden revelations and US–China tensions over trade and high-tech development). Yet these state–capital dynamics are also more complex than what some pundits may call "digital protectionism" or "digital authoritarianism" when critiquing localization rules, or "digital colonialism" when arguing for localization. Inter-state rivalries or alignments that appear on newspaper headlines should not blind us from viewing these internal and external state–capital interactions in the context of the processes of capitalist accumulation and transformation that influence the evolution of transnational data regulations in emerging economies.

Second, while our study has highlighted the common pressure exerted by geopolitical tensions on internet governance in both countries, there are also some differences between the two cases. These differences are rooted in each country's distinct historical trajectories of digital development, the dynamics of state–business relations, and the country's positioning within broader geopolitical shifts. The internet industry in China took

off in the 1990s, almost a decade earlier than in India. Beijing's push for techno-nationalist development since the late 2000s also predated Modi's Digital India project starting in 2015. While global Big Tech and transnational capital were indispensable players in the early development of the Chinese tech industry and still play viable roles as partners to Chinese firms, major Chinese tech platforms have dominated the Chinese market and society and become important players in global digital capitalist networks. This resulted in growing tensions with the Chinese state's leadership and policy autonomy, and an increasingly competitive relationship with US Big Tech, despite ongoing collaboration in areas where profit-seeking interests align, such as the financing of startups. Amidst broader US–China trade and tech wars, the Chinese state has sought to reassert its control and developed a comprehensive set of laws and regulations governing platforms and data flows. In comparison, India's homegrown tech industry is still relatively "emerging" and relies on global Big Tech and transnational capital for the technology, infrastructure, and financing needed for its development. This has led the government to adopt a more ambiguous and flexible approach towards regulating data flows in key data legislation, with watered-down mandates for data localization and yet broad executive power to scrutinize firms. As India's partnerships with US Big Tech and capital have strengthened after the forced exit of Chinese players following Sino-India tensions, one might expect the Modi government to continue to be somewhat amenable to the economic interests of US firms in follow-up regulations. While China's vision for digital sovereignty seems to be more clearly articulated through its data regulations, India currently leans toward more cautious rule-making and less concrete mandates to preserve the state's executive power in shaping domestic market development without seriously alienating US Big Tech and transnational capital that remain crucial to its high-tech ambitions.

The differences between China and India's political systems may at least partly account for the above variation. China's one-party system placed Beijing in a better position to exert strong controls over data flows, as seen in its ability to pass a series of legislations that increased the state's oversight over private firms. Despite the rising clout of domestic tech giants, the party-state's dominance in the domestic political economy enabled wide-reaching regulatory measures vis-à-vis domestic firms, though regulatory implementation showed some flexibility in response to business concerns. In contrast, India's multi-party democratic system provided greater room for domestic stakeholders and international businesses to shape and contest narratives and policies in data governance through lobbying and negotiation, leading to more open debates and challenges in policy rollout.

Finally, our study has broader implications for understanding data governance in emerging economies. Complementing existing scholarship's focus on the emerging economies' push for digital sovereignty, this study shows that regulations concerning cross-border data in both countries are still evolving, with nuances, flexibilities, and even scale-backs in policy formation and implementation. One may argue that this reflects the pragmatic interest of emerging economy governments in juggling internal political and economic considerations, external security concerns, and global standards in developing data regulations to deal with the challenges of changing global geopolitics. While the US's liberalization approach towards digital trade and the EU's privacy-focused GDPR frameworks certainly influence policy formulation in emerging markets, this study demonstrates that the distinct historical paths of national development and local socioeconomic realities continue to shape the government's vision for the internet economy and governance of digital platforms that handle massive amounts of data and expand internationally. Moreover, instead of a one-way street of the government imposing its will, data governance in emerging economies involves a dynamic process where various domestic and international non-state players influence state policymaking. This

means that, instead of trying to force analysis of data governance in emerging economies into frameworks aligned with the "US," "EU," or increasingly the "China" model, or a mix of them, a contextualized approach can unveil on-the-ground forces that mediate geopolitical considerations and shape policy development. While acknowledging the influence of major powers in data governance in emerging economies, such an approach gives due consideration to how the distinct dynamics of the local political economy have shaped the trajectory of data governance.

Funding

This project was partially supported by the University of Kentucky's OPVR CURATE Grant and UKinSPIRE (Seeding Partnerships for International Research Engagement) Grant.

Conflict of Interests

The authors declare no conflict of interests.

References

Adonis, A. A. (2019). Critical engagement on digital sovereignty in international relations: Actor transformation and global hierarchy. *Global: Jurnal Politik Internasional*, *21*(2), 262–282.

Aouragh, M., & Chakravartty, P. (2016). Infrastructures of empire: Towards a critical geopolitics of media and information studies. *Media, Culture & Society*, *38*(4), 559–575.

Arcesati, R. (2024, May 6). The data quagmire for German carmakers in China. *The Diplomat*. https://thediplomat.com/2024/05/the-data-quagmire-for-german-carmakers-in-china

Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. *Berkeley Technology Law Journal*, *37*(2), 623–700.

Arsène, S. (2016). Global internet governance in Chinese academic literature. *China Perspectives*, *2016*(2), 25–35.

Au, A. (2023). China's internet sector reforms and the rise of ESG in the state techno-nationalist agenda. *Policy & Internet*, *15*(4), 646–664.

Au, A., & Witzleb, N. (2024). Data flows and data protection in the Greater Bay Area: The need for a coordinated legal framework. *The Chinese Journal of Comparative Law*, *12*, Article cxae013.

Barrinha, A., & Renard, T. (2020). Power and diplomacy in the post-liberal cyberspace. *International Affairs*, *96*(3), 749–766.

Basu, A., & Nachiappan, K. (2020, July 31). India and the global battle for data governance. *Seminar*. https://www.india-seminar.com/2020/731/731_arindrajit_and_karthik.htm

Basu, A., & Swaminathan, M. (2023, August 4). Will the India–US tech handshake foster digital trade and policy convergence? *The Diplomat*. https://thediplomat.com/2023/08/will-the-india-us-tech-handshake-foster-digital-trade-and-policy-convergence

Belli, L. (2021). Cybersecurity policymaking in the BRICS countries: From addressing national priorities to seeking international cooperation. *The African Journal of Information and Communication*, *28*, 1–14.

Belli, L., Gaspar, W. B., & Singh Jaswant, S. (2024). Data sovereignty and data transfers as fundamental elements of digital transformation: Lessons from the BRICS countries. *Computer Law & Security Review*, *54*, Article 106017.

Bhandari, A., Fernandes, B., & Agarwal, A. (2020). *Chinese investment in India*. Gateway House. https://www.gatewayhouse.in/wp-content/uploads/2020/07/Chinese-Investments_2020-Final.pdf

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415–434.

Carr, M. (2016). *US power and the internet in international relations: The irony of the information age*. Springer.

Cartwright, M. (2020). Internationalising state power through the internet: Google, Huawei and geopolitical struggle. *Internet Policy Review*, *9*(3). https://doi.org/10.14763/2020.3.1494

Chander, A., & Sun, H. (2023). Introduction: Sovereignty 2.0. In A. Chander & H. Sun (Eds.), *Data sovereignty: From the Digital Silk Road to the return of the state* (pp. 1–32). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0001

Chaudhuri, R., & Joseph, A. K. (2024). Living in a fragmented world: India's data way. *India Review*, *23*(2), 154–176.

Chen, J. Y., & Qiu, J. L. (2019). Digital utility: Datafication, regulation, labor, and DiDi's platformization of urban transport in China. *Chinese Journal of Communication*, *12*(3), 274–289.

Chen, W. (2022). Zoom in and zoom out the glocalized network: When transnationalism meets geopolitics and technopolitics. *Information, Communication and Society*, *25*(16), 2381–2396.

Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, *100*(6), 2419–2440.

Cornish, C. (2023, August 7). China's Ant Group swaps stake in India's Paytm for debt. *Financial Times*. https://www.ft.com/content/1bd35c18-867d-48de-9c83-16ecd885d44b

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), Article tyac011.

Creemers, R., Webster, G., & Triolo, P. (2017). *Translation: Cybersecurity Law of the People's Republic of China (effective June 1, 2017)*. DigiChina. https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017

Cyberspace Administration of China. (2024). *Cujing he guifan shuju liudong guiding da jizhe wen*. https://www.cac.gov.cn/2024-03/22/c_1712776611649184.htm

DeNardis, L. (2009). *Protocol politics: The globalization of internet governance*. MIT Press.

Drezner, D. W. (2004). The global governance of the internet: Bringing the state back in. *Political Science Quarterly*, *119*(3), 477–498.

Eamon, B., & Lau, Y. (2021, July 6). Not just Didi: China's internet watchdog targets more U.S.-listed firms for 'national security' review. *Fortune*. https://fortune.com/2021/07/05/didi-chuxing-stock-app-cybersecurity-full-truck-alliance-boss-zhipin

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty—Rhetoric and reality. *Journal of European Public Policy*, *31*(8), 2099–2120.

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453.

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79.

Fefer, R. F. (2020). *Internet regimes and WTO e-commerce negotiations*. Congressional Research Service.

Floridi, L. (2020). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*(3), 369–378.

Foster, C., & Azmeh, S. (2020). Latecomer economies and national digital policy: An industrial policy perspective. *The Journal of Development Studies*, *56*(7), 1247–1262.

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M.-G., Bômont, C., Braun, M., Danet, D., Disforges, A., Géry, A., Grumbach, S., Hummel, P., Limonier, K., Münßinger, M., Nicolai, F., Pétiniaud, L., Winkler, J., & Zanin, C. (2023). Contested Spatialities of Digital Sovereignty. *Geopolitics*, *28*(2), 919–958.

Grover, R., Jang, K., & Su, L. W. (2024). Beyond digital protection(ism): Comparing data governance frameworks in Asia. *Journal of Information Policy*, *14*, 161–193. https://doi.org/10.5325/jinfopoli.14.2024.0005

Han, R. (2018). *Contesting cyberspace in China: Online expression and authoritarian resilience*. Columbia University Press.

He, Y. (2024a). Chinese digital platform companies' expansion in the Belt and Road countries. *The Information Society*, *40*(2), 96–119.

He, Y. (2024b). Chinese fintech goes global: Political challenges and business strategies. *Asia Policy*, *19*(1), 35–50.

He, Y., & Zeng, K. (2024). China in global digital trade governance: Towards a development-oriented agenda? *International Affairs*, *100*(5), 2195–2215.

Hicks, J. (2020). Digital ID capitalism: How emerging economies are re-inventing digital capitalism. *Contemporary Politics*, *26*(3), 330–350.

Hong, Y., & Goodnight, G. T. (2020). How to think about cyber sovereignty: The case of China. *Chinese Journal of Communication*, *13*(1), 8–26.

Jayasuriya, K. (2021). Beyond geopolitical fetishism: A geopolitical economy research agenda. *Australian Journal of International Affairs*, *75*(6), 665–677.

Jiang, M. (2024). Models of state digital sovereignty from the global south: Diverging experiences from China, India and South Africa. *Policy & Internet*,*16*(4), 727–738. https://doi.org/10.1002/poi3.427

Jongen, H., & Scholte, J. A. (2022). Inequality and legitimacy in global governance: An empirical study. *European Journal of International Relations*, *28*(3), 667–695.

Kalra, A. (2019, December 18). U.S.–India business groups plan to lobby for dilution of India's privacy bill—Sources. *Reuters*. https://www.reuters.com/article/world/us-india-business-groups-plan-to-lobby-for-dilution-of-indias-privacy-bill--idUSKBN1YM0H3

Kaye, D. B. V., Chen, X., & Zeng, J. (2021). The co-evolution of two Chinese mobile short video apps: Parallel platformization of Douyin and TikTok. *Mobile Media & Communication*, *9*(2), 229–253.

Kharpal, A. (2020, September 4). 'Chinese firms are learning a painful lesson': India's app crackdown opens doors for U.S. tech giants. *CNBC*. https://www.cnbc.com/2020/09/04/india-crackdown-on-chinese-tech-opens-doors-for-us-giants.html

Khatri, V., & Brown, C. V. (2010). Designing data governance. *Communications of the ACM*, *53*(1), 148–152.

Kumar, A., & Thussu, D. (2023). Media, digital sovereignty and geopolitics: The case of the TikTok ban in India. *Media, Culture & Society*, *45*(8), 1583–1599.

Lei, Y. W. (2023). *The gilded cage: Technology, development, and state capitalism in China*. Princeton University Press.

Lessig, L. (1998). Open code and open societies: Values of internet governance. The Charles Green lecture in law and technology. *Chicago-Kent Law Review*, *74*(3), 1405–1422.

Li, B. (2024). China issues the Regulations on Network Data Security Management: What's important to know. *IAPP*. https://iapp.org/news/a/china-issues-the-regulations-on-network-data-security-management-what-s-important-to-know

Li, W., & Chen, J. (2024). From Brussels effect to gravity assists: Understanding the evolution of the GDPR-inspired personal information protection law in China. *Computer Law & Security Review*, *54*, Article 105994.

Ministry of Electronics and Information Technology of India. (n.d.). *Digital India*. https://www.meity.gov.in/static/uploads/2024/03/Running-single-file.pdf

Mishra, N. (2021). Building bridges: International trade law, internet governance, and the regulation of data flows. *Vanderbilt Journal of Transnational Law*, *52*(2), 463–510.

Mishra, N. (2023). Data governance and digital trade in India: Losing sight of the forest for the trees? In A. Chander & H. Sun (Eds.), *Data sovereignty: From the Digital Silk Road to the return of the state* (pp. 240–263). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0011

Mügge, D. (2024). EU AI sovereignty: For whom, to what end, and to whose benefit? *Journal of European Public Policy*, *31*(8), 2200–2225.

Murdoch, S., & Stanway, D. (2021, April 10). China fines Alibaba record $2.75 bln for anti-monopoly violations. *Reuters*. https://www.reuters.com/business/retail-consumer/china-regulators-fine-alibaba-275-bln-anti-monopoly-violations-2021-04-10

Mosco, V. (2009). *The political economy of communication*. Sage.

O'Hara, K., & Hall, W. (2018). *Four internets: The geopolitics of digital governance*. Centre for International Governance Innovation. https://eprints.soton.ac.uk/427838/1/Paper_20no.206web.pdf

Otto, B., & Bellman, E. (2020, July 15). Google to invest $4.5 billion in India's Jio Platforms. *The Wall Street Journal*. https://www.wsj.com/articles/google-to-invest-4-5-billion-in-indias-jio-platforms-11594815351

Parsheera, S. (2024). Stack is the new black? Evolution and outcomes of the 'India-Stackification' process. *Computer Law & Security Review*, *52*, Article 105947.

Plantin, J. C., & De Seta, G. (2019). WeChat as infrastructure: The techno-nationalist shaping of Chinese digital platforms. *Chinese Journal of Communication*, *12*(3), 257–273.

Pohle, J., Nanni, R., & Santaniello, M. (2024). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy & Internet*, *16*(4), 666–671. https://doi.org/10.1002/poi3.437

Polatin-Reuben, D., & Wright, J. (2014, August 18). *An internet with BRICS characteristics: Data sovereignty and the balkanisation of the internet* [Conference paper]. 4th USENIX Workshop on Free and Open Communications on the Internet, San Diego, USA. https://www.usenix.org/system/files/conference/foci14/foci14-polatin-reuben.pdf

Purtova, N. (2018). The law of everything: Broad concept of personal data and future of EU data protection law. *Law, Innovation, and Technology*, *10*(1), 40–81.

Qiu, J. L. (2023). The return of billiard balls? US–China tech war and China's state-directed digital capitalism. *Javnost – The Public*, *30*(2), 197–217.

Qiu, J. L., Yu, P. K., & Oreglia, E. (2022). A new approach to the geopolitics of Chinese internets. *Information, Communication & Society*, *25*(16), 2335–2341.

Ragin, C. C., & Becker, H. S. (Eds.). (1992). *What is a case? Exploring the foundations of social inquiry*. Cambridge University Press.

Rolf, S., & Schindler, S. (2023). The US–China rivalry and the emergence of state platform capitalism. *Environment and Planning A: Economy and Space*, *55*(5), 1255–1280.

Rosenbach, E., & Mansted, K. (2019). *The geopolitics of information*. Belfer Center for Science and International Affairs.

Roy, A., & Rai, S. (2022, March 14). Paytm Bank punished for sharing data abroad, verification lapses. *Bloomberg*. https://www.bloomberg.com/news/articles/2022-03-14/india-said-to-punish-paytm-bank-for-data-leaks-to-chinese-firms

Sacks, S., Shi, M., & Webster, G. (2019, February 8). The evolution of China's data governance regime: A timeline. *New America*. https://www.newamerica.org/cybersecurity-initiative/digichina/blog/china-data-governance-regime-timeline

Schroeder, R. (2022). Aadhaar and the social credit system: Personal data governance in India and China. *International Journal of Communication*, *16*, 2370–2386. https://ijoc.org/index.php/ijoc/article/view/19059

Sen, P. (2021). *EU GDPR and Indian Data Protection Bill: A comparative study*. SSRN. https://doi.org/10.2139/ssrn.3834112

Shen, H. (2016). China and global internet governance: Toward an alternative analytical framework. *Chinese Journal of Communication*, *9*(3), 304–324.

Shen, H. (2019). *China's tech giants: Baidu, Alibaba, Tencent*. Konrad-Adenauer-Stiftung. https://www.kas.de/documents/288143/4843367/panorama_digital_asia_v3b_HongShen.pdf

Shen, H. (2021). *Alibaba: Infrastructuring global China*. Routledge.

Shen, H., & He, Y. (2022). The geopolitics of infrastructuralized platforms: The case of Alibaba. *Information, Communication & Society*, *25*(16), 2363–2380.

Shetty, M. (2025, January 1). PhonePe, GPay get 2 years more to cut UPI market share. *The Times of India*. https://timesofindia.indiatimes.com/business/india-business/phonepe-gpay-get-2-years-more-to-cut-upi-market-share/articleshow/116843059.cms

Singh, N. (2016). Information technology and its role in India's economic development: A review. In S. Dev & P. Babu (Eds.), *Development in India: Micro and macro perspectives* (pp. 283–312). Springer. https://doi.org/10.1007/978-81-322-2541-6_14

Sinha, A., & Basu, A. (2019). The politics of India's data protection ecosystem. *Economic and Political Weekly*, *54*(49). https://www.epw.in/engage/article/politics-indias-data-protection-ecosystem

State Council of the People's Republic of China. (2010). *Guowuyuan guanyu jiakuai he fazhan zhanluexing xinxing chanye de jueding*. https://www.gov.cn/zwgk/2010-10/18/content_1724848.htm

Steinbower, C. (2020, August 18). President Trump accepts CFIUS's recommendation—Orders TikTok's Chinese owner to divest. *Winston & Strawn LLP Blog*. https://www.winston.com/en/blogs-and-podcasts/global-trade-and-foreign-policy-insights/president-trump-accepts-cfiuss-recommendation-orders-tiktoks-chinese-owner-to-divest

Su, C., & Flew, T. (2020). The rise of Baidu, Alibaba and Tencent (BAT) and their role in China's Belt and Road Initiative (BRI). *Global Media & Communication*, *17*(1), 67–86.

Subramanian, R. (2020). Historical consciousness of cyber security in India. *IEEE Annals of the History of Computing*, *42*(4), 71–93.

Shuju kuajing liudong de zhongguo fangan: Woguo tuidong shuju kuajing anquan youxu ziyou liudong shuping. (2024, June 1). *The Paper*. https://www.thepaper.cn/newsDetail_forward_27593350

Sun, H. (2019). U.S.–China tech war. *China Quarterly of International Strategic Studies*, *5*(2), 197–212.

Tang, M. (2019). *Tencent: The political economy of China's surging internet giant*. Routledge.

Tang, M. (2022a). Not yet the end of transnational digital capitalism: A communication perspective of the US–China decoupling rhetoric. *International Journal of Communication*, *16*, 1506–1531.

Tang, M. (2022b). The challenge of the cloud: Between transnational capitalism and data sovereignty. *Information, Communication and Society*, *25*(16), 2397–2411.

Tencent Research Institute. (2024, November 28). Yinshi zhiyi, mianxiang weilai: Woguo shuju kuajing liudong jizhi de chuangxin tansuo. *36kr*. https://36kr.com/p/3055821212488067

Thomas, P. (2009). Bhoomi, Gyan Ganga, e-governance and the right to information: ICTs and development in India. *Telematics and Informatics*, *26*(1), 20–31.

Thomas, P. (2019). *The politics of digital India: Between local compulsions and transnational pressures*. Oxford University Press.

Vila Seoane, M. F. (2021). Data securitisation: The challenges of data sovereignty in India. *Third World Quarterly*, *42*(8), 1733–1750.

Wang, Y., & Gray, J. E. (2022). China's evolving stance against tech monopolies: A moment of international alignment in an era of digital sovereignty. *Media International Australia*, *185*(1), 79–92.

Warren, S., & Zhu, L. (2022). *China's Didi fined over US$1 billion by Chinese data regulators*. Squire Patton Boggs. https://www.squirepattonboggs.com/-/media/files/insights/publications/2022/07/chinas-didi-fined-over-us-1-billion-dollars-by-chinese-data-regulators/chinas-didi-fined-over-1-billion-us-dollars-by-chinese-data-regulators.pdf

Wijaya, T., & Jayasuriya, K. (2024). A new multipolar order: Combined development, state forms and new business classes. *International Affairs*, *100*(5), 2133–2152.

Wimmer, K., Maldoff, G., & Lee, D. (2020). *Comparison: Indian Personal Data Protection Bill 2019 vs. GDPR*. IAPP. https://iapp.org/media/pdf/resource_center/india_pdpb2019_vs_gdpr_iapp_chart.pdf

World Bank. (2024). *Global digitalization in 10 charts*. https://www.worldbank.org/en/news/immersive-story/2024/03/05/global-digitalization-in-10-charts

Zhang, A. H. (2024). *High wire: How China regulates Big Tech and governs its economy*. Oxford University Press.

Zhang, C. (2024). China's privacy protection strategy and its geopolitical implications. *Asian Review of Political Economy*, *3*(1), Article 6.

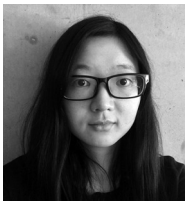
Zhang, L., & Chen, J. Y. (2022). A regional and historical approach to platform capitalism: The cases of Alibaba and Tencent. *Media, Culture & Society*, *44*(8), 1454–1472.

Zhao, S. (2022). *The dragon roars back: Transformational leaders and dynamics of Chinese foreign policy*. Stanford University Press.

Zhong, R. (2020, November 6). In halting Ant's I.P.O., China sends a warning to business. *The New York Times*. https://www.nytimes.com/2020/11/06/technology/china-ant-group-ipo.html

Zinovieva, E., & Shitkov, S. (2023). Sovereignty as practice in digital age. In A. Baykov & E. Zinovieva (Eds.), *Digital international relations* (pp. 75–90). Springer. https://doi.org/10.1007/978-981-99-3467-6_5

About the Authors



Yujia He is an assistant professor at the Patterson School of Diplomacy and International Commerce, University of Kentucky. Her research interests span science and technology policy, international political economy, development studies, and Asian studies.

Ka Zeng is professor of political science at the University of Massachusetts Amherst. Her research focuses on China's role in the global economy. She is the author or co-author of *Trade Threats*, *Trade Wars*, *Greening China*, and *Fragmenting Globalization*, all published by the University of Michigan Press.

Politics and Governance
2025 • Volume 13 • Article 10460
https://doi.org/10.17645/pag.10460

cogitatio

ARTICLE

Open Access Journal

Ruling the Data Flows: Data Cognition in Global Cross-Border Data Flows Governance

Jinhe Liu

School of Journalism & Communication, Peking University, China

Correspondence: Jinhe Liu (liujinhe@pku.edu.cn)

Submitted: 31 March 2025 **Accepted:** 10 July 2025 **Published:** 27 August 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

Noting the "awakening" of data cognition in the governance of global cross-border data flows over the past half-century, this article calls for a deeper understanding and exploration of the cultural dynamics underlying this phenomenon from a constructivist perspective. It identifies "cultural value" as one of the key driving factors in the governance approaches of four representative countries and regions: the US, China, the EU, and Russia. We extract "attribute cognition" and "value pursuit" from the core of data culture to the center of data governance under the concept of "evaluative cognition." By observing how policy stances change, we separate different evaluative cognitions from a complex game field through a historical and comparative analysis, and thus provide a theoretical understanding of the current intense geopolitical game around data.

Keywords

cross-border data flows; cultural value; data governance; evaluative cognition

1. Introduction

The global understanding of data is changing. In recent years, China's policy stance on cross-border data flows has changed, and the "data *developmentalism*" of data cognition behind it has been clearly expressed. In 2024, China issued the Provisions on Promoting and Regulating Cross-Border Data Flows and the Global Initiative on Cross-Border Data Flows, which shows its change from a strict data localization stance. At the same time, we have seen the US revise its claim of data free flows, showing a trend of advocating data localization to a certain extent. Also, in 2024, the US Department of Justice issued final rules prohibiting the cross-border transfer of sensitive personal data to some countries, starting the process of data decoupling for some countries, and establishing a cross-border data flows regime based on national security rationale.

Earlier in 2018, Brazil enacted the General Personal Data Protection Act, aligning with the EU's GDPR and amending the data localization initiative proposed in the Marco Civil da Internet in 2014.

How to understand this seemingly fickle policy stance, and how to analyze the complex and ever-changing regulatory system of cross-border data flows? This becomes an important challenge in the study of global cross-border data flows governance. There is often a systematic value system behind national policies, and data culture research is an effective theoretical approach to understanding data development and governance (Oliver, 2024), especially regarding the value propositions carried in data. The most typical example is the globally popular slogan "Data is Oil," as well as the highly concerning concept of "dataism" (Brooks, 2013; Harari, 2016), that have crystallized a prescriptive idea about how people should see data and the value it contains. It is necessary to analyze the cognition of the attributes of data and the value it carries in different countries and regions. This article takes an explicitly constructivist approach and adopts the theoretical perspective of cultural value theory to use the conceptual tools of evaluative cognition to analyze this inherent law. The history of regulating cross-border data flows holds rich philosophical implications that go far beyond the academic value of analyzing specific regulatory policies. A deeper epistemological contestation behind the global cross-border data flows governance should be recognized, and forces with more far-reaching effects should be identified.

2. Data Awareness: Three Historical Tracks of Global Development

The debates over the regulation of cross-border data flows have emerged even before the mass commercialization of the Internet. In Western countries, they go as far as the early 1970s. From a global perspective, the history of this regulation unfolds along three tracks and sparks three waves (see Figure 1). The first and second tracks, namely the American Track and the European Track, are rulemaking efforts led by the US and Europe, respectively, while the third track, namely the Emerging Economies' Track, is dominated by emerging countries, advocating new rulemaking through domestic legislation. The first wave of regulation of cross-border data flows was initiated by European countries. In the game with the US, the basic version of the European model was formed, which was marked by the 108 Convention, the General Exception Rules of the General Agreement on Trade in Services (GATS) under the WTO framework, and Directive 95. The second wave was led by the US, which changed its previous defensive posture toward Europe. For instance, the US took the Asia-Pacific Economic Cooperation (APEC) as the rule-building field and led the construction of the APEC Privacy Framework in 2004. Finally, the APEC Cross-Border Privacy Rules System (CBPRs) was formally formed in 2011. Since then, the American model has become an important international template for "data free-flowing."

Europe and the US had a clear understanding of electronic data at the beginning. The cross-border data flows had become the focus of the transatlantic competition since the early 1970s. Before the 1990s, Europe took the lead in establishing rules, and after 2000, the US took the initiative to construct the American version of cross-border data flows management norms. In the past decade, the global cross-border data flows regulation has entered its third wave. In the past 50 years or so of the history of cross-border data flows governance, the main value of Western countries in the first four decades had been the protection of personal privacy.

The third wave, which also marks the rise of the third track, began around 2010, when emerging economies such as China, India, and Russia started to put forward requirements for data localization (Chander & Lê, 2014).

Snowden's revelations in 2013 significantly accelerated this trend. But unlike the previous two waves, when Europe and the US focused on privacy legislation, this new stage presented a novel struggle of power and interests around data rules among Europe, the US, and the emerging economies. This game has gradually moved from domestic legislation to the negotiation of international trade rules, and the object of regulation has also expanded from personal information to almost all data circulating with commercial value (Wang, 2018).

In the later decade, as emerging economies began to "wake up" to this issue, one after another, they joined these "construction of rules" from the perspective of their own national interests. The problem of cross-border data flows regulation became no longer a problem of personal privacy, but also a competition for national economic interests. In the global rise of digital trade, a new round of global debate on the governance of cross-border data flows has emerged, among which various understandings of data attributes have been manifested. The most typical countries that regard data as wealth are China and India. China proposed that "data is a basic strategic resource of the country" (State Council of the People's Republic of China, 2015) in the Outline of Action to Promote Big Data Development in 2015, and it proposed data as a factor of production in 2019. Also in 2019, in response to the then US President Donald Trump's criticism of data localization policies at the G20 summit, Indian Foreign Secretary Vijay Gokhale asserted that "data is also needs to take into account the requirements of developing countries," and "it is a new form of wealth" ("Data 'new form of wealth,'" 2019). With the rapid development of data-based artificial intelligence, it can be foreseen that the cognition of data attributes will further develop.

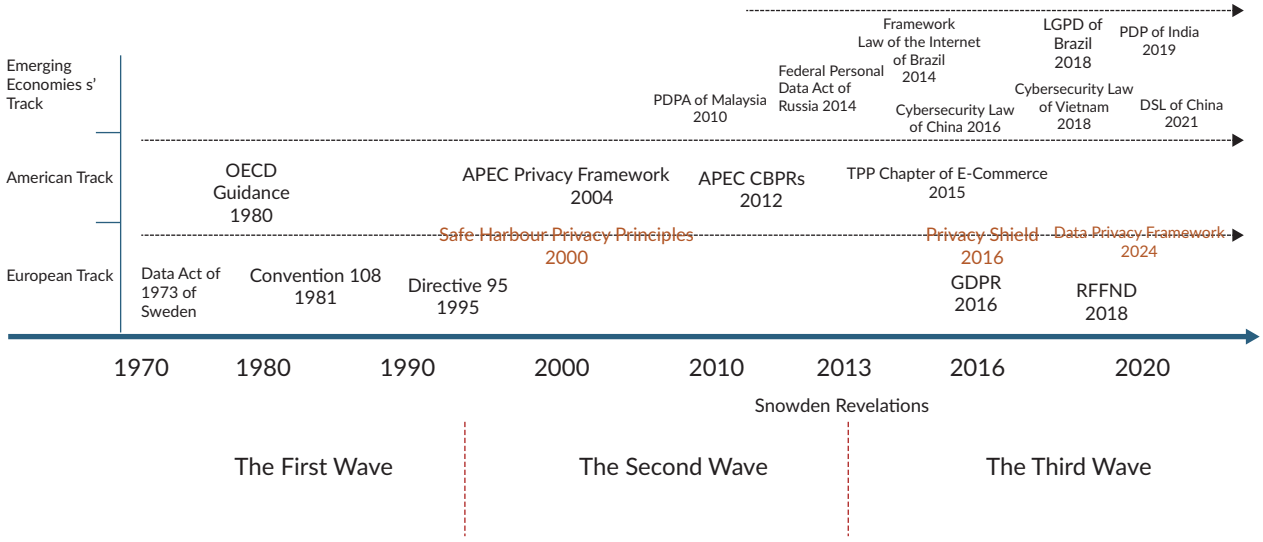


Figure 1. Three tracks of global cross-border data flows governance. Note: These represent significant historical milestones in global cross-border data flows governance, but do not encompass all the legislations and policies.

3. Cultural Value Paradigm of Data Governance Study

Governance, especially state decision-making, is highly complex and often involves multiple factors working together. There are multiple levels of research on the dynamics of cross-border data flows policies. Interest, power, and culture are all important analytical perspectives, and these three levels often jointly determine the formation of policies. Furthermore, the factors at these three levels also influence each other. A large number of research on the regulation game of cross-border data flows is mainly at the interest level,

assuming that countries are rational actors and try to select policies that maximize their national interests under existing international conditions, such as data localization theory (Chander & Lê, 2014) and data defensivism theory (Liu, 2020). Since cross-border data flows governance is often reproduced in the form of policies and rulemaking, a significant body of study has focused on material aspects, particularly rule analysis and policy recommendations (Xu, 2018). In contrast, there is a notable deficiency in analyses addressing the intrinsic cultural demands of data governance, as well as studies exploring historical depth and the underlying logic of contemporary realities.

Constructivism holds that society is largely constructed by human beings, and people's cultural value constantly influences decision-making in practice. Beyond the rationalist approach, this article advocates for further understanding and exploring of the cultural dynamics behind phenomena from a constructivist perspective, arguing also that cultural value should be taken as one of the most important driving factors of governance, which could be conceptualized as a cultural value paradigm (Liu & Cui, 2023). The relationship between cultural value and material society transpires in a process of mutual expression. However, through the accumulation of social history, culture has formed its own continuous logic and exerts a guiding role on the material society.

It should be noted that the cultural value paradigm is not an absolute cultural determinism, but rather a theory of the hierarchy of values. In other words, the cultural value paradigm holds that a series of values have an impact on real governance activities, but there are values that are given priority. The dominant values often run through the whole process of policy making, and even define the preconditions for policy makers to understand events and the perspective from which they view problems. Therefore, this study attempts to recognize the dominant values and analyze their impact on governance decision-making. At the same time, it aims to grasp the macro development laws, hoping to gain a more general understanding of the development context of global data governance.

Generally, data culture reflects and is influenced by people's values, attitudes, and behavior (Oliver et al., 2023). Actors conceptualize differently the meaning of data, the relevant stakeholder community, and the reasoning for their governance efforts, and these differences are directly related to whether data can be governed. (Obendiek, 2022) In fact, the objects pointed to by data culture are broad. This article selects "attribute cognition" and "value pursuit" as the core elements of data culture, which serve as key driving factors of data governance. I put the two elements under the concept of "evaluative cognition" as the operational tool of the cultural value analytical paradigm, which emphasizes human subjective initiative.

Evaluative cognition is an interdisciplinary concept, referring to the process in which, during cognition, not only the attributes of things are identified but also their values (such as good or bad, degree of importance, and legitimacy) are judged and asserted, which is a fundamental aspect of decision-making and planning. For instance, it is like recognizing the chemical properties of a certain drug (attribute cognition) and asserting that it has "therapeutic value" (value assertion). An important foundation of evaluative cognition is Richard Lazarus' cognitive appraisal theory in psychology, which emphasizes that emotions are not caused by events themselves, but by how these events are appraised in relation to personal goals (Lazarus, 1991, p. 135). Evaluative cognition is regarded as the core of attitudes, considering attitudes as the automatic association of "object-evaluation" (such as "apple → healthy → like"; see also Fazio, 2007). In the field of cognitive science, evaluative cognition is the computational process in which systems (humans or machines) compare

the values of options and prioritize them in decision-making, problem-solving, or goal-oriented behaviors. Typically, Herbert A. Simon proposed "bounded rationality," suggesting that the evaluative cognition of humans and machines is limited by information processing capabilities and tends to choose "good enough" options through the "satisficing" principle rather than the optimal solution (Simon, 1980). In summary, evaluative cognition is a value-driven information processing process.

Data evaluative cognition here refers to a country or a society's cognition of the attributes of data and their assertion of the value it carries. It is a kind of social epistemology in a broad sense. Lorraine Daston's historical epistemology (Daston, 1994, pp. 282–289; Daston & Galison, 2007) offers us significant inspiration that the nature, standards, and production methods of knowledge are not immutable but deeply rooted in specific historical, cultural, and social practices. Therefore, evaluative cognition helps to highlight the value expectations in a specific history and society from epistemology.

In terms of operational methods, this study takes evaluative cognition as the analytical variable and the more than half-century history of data cross-border flows regulation as the object, by observing the policy stance changes of major countries around the world. In the selection of case countries and regions, the US, China, the EU, and Russia were chosen because they all have a strong position tendency and relatively profound epistemological foundations. To some extent, these four countries/regions can be regarded as ideal types in Max Weber's sense, which have instrumental value for understanding the governance of global cross-border data flows. The other influential countries, such as India, Brazil, Japan, South Korea, and Iran, can be found in these four types accordingly or by similar logic. For example, India and Brazil hold a developmentalist stance similar to China's; Japan and South Korea follow a logic more like that of Europe and the US, and Iran aligns closer to Russia. Of course, it is difficult to match one individual country to one single position, and the situation of each country needs to be more accurately understood in the light of its history and reality. However, certainly, understanding each country's position from the perspective of cultural values is an effective approach. Data cognition is crucial for comprehending data governance on a global scale.

4. Starting Point and Development of Data Cognition

4.1. The Starting Point of Data Cognition

To accurately examine the data cognition, a historical perspective is needed. When examining the claims about data made by various countries and regions from the perspective of historical traditions, we can identify their starting point as the origin (see Table 1).

Table 1. The starting point for data cognition.

Country and region	Starting point of data cognition
US	Property carrier
China	Strategy carrier
EU	Rights carrier
Russia	Security carrier

The US views the Internet as a market product and as property that has been transferred from the state to private enterprises. Due to the Internet's "American-origin story," in the mid-1990s, the US privatized the

Internet and sold five access points of its backbone network to private enterprises, transferring the management of its root server system from the government to the private sector, to what is now well-known as the nonprofit corporation the Internet Corporation for Assigned Names and Numbers (ICANN; Leiner et al., 1997). Since then, the US has regarded the Internet as a market product, which became the fundamental logic supporting the later development of the American Internet industry. Under this kind of Internet cognition, the US generally regards data generated from the Internet as a market product and the property of enterprises. Moreover, the US believes that data is an indispensable element for the development of the Internet market; therefore, it has always supported the free flow of data along with the global market. In a transnational scenario, cross-border data is itself a kind of trade (Mueller & Grindal, 2018).

The EU has recognized the human rights embedded in data from the very beginning. During the Holocaust, in World War II, the Nazi German government identified and hunted the Jewish population by using census cards and other demographic statistics. This particular social memory has long raised deeply-embedded fears and concerns in Europe about the malign use of personal data. In the 1970s, the efficient data processing capabilities of large-scale computers in the US generated a sense of unease among Europeans (Fishman, 1980; Kirby, 1980; Novotny, 1980). The Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data, adopted in 1981, was a response to such concerns. Against this backdrop, the EU began to clearly define the rights and value of data itself (Kuner, 2011). The Charter of Fundamental Rights of the European Union, drafted in 2000 and enacted in 2009, clearly states the fundamental rights contained in the data under Article 8 on protection of personal data, and especially along with Article 7 on respect for private and family life. The GDPR, adopted in 2018, embodies the EU's claim to data rights, establishing data privacy and protection as a fundamental right. When it comes to digital technology, the EU emphasizes "European values." The EU's commitment to a safe, secure, and sustainable digital transformation that puts people first, aligning with the EU's core values and fundamental rights, is underlined in the *European Declaration on Digital Rights and Principles*, a high-level document signed by the Presidents of the Commission, the European Parliament, and the Council in 2022.

China has a tradition of technological nationalism, hoping that information technology can make the country rich and powerful, and treating data as a national development strategy (Liu, 2020). China sees the Internet as a force for national development and has put forward a "cyber power" (网络强国) strategy. In official statements, "big data" has been elevated to a national strategy. By 2020, China had officially proposed "data as a factor of production," raising expectations about the empowerment of data for national development to a new high (The Central Committee of the Communist Party of China & The State Council of China, 2020). To promote the development of data, China is working hard to build a "data factor market" (数据要素市场) and established, in 2023, the National Bureau of Data. The National Bureau of Data has released several definitions of data-related concepts, including data factor, data products and services, data assets, and market-based allocation of data factor, which have strong attributes of economic development and point to the market economy. For example, it defines "data resources" (数据资源) as "data with value creation potential" (National Data Administration of PRC, 2024). In this clear cognition, data is regarded as an element of national development and the carrier of development strategies. From the "big data strategy" to the data factor market strategy, we are constantly exploring the process of maximizing the energy of data.

China's expectation of a data development strategy also comes from earlier strategic propositions for national informatization and industrialization. Even we can see the logic behind China's pursuit of modernization since

the Reform and Opening Up program, which regards science and technology as the driving force of national development (Zheng, 2007, p.27). Therefore, data, as the basis of the latest information technology, is naturally regarded as the strategic carrier of national development.

In Russia, due to the Cold War, the understanding of Internet/cyberspace is dominantly based on national security, which is called "information security" instead. As early as 1998, in response to the international governance of the Internet, Russia put forward a proposal for an international information security aimed at the United Nations, calling on UN member states to pay attention to potential threats in the field of information security from a multilateral level. Since then, Russia has been firmly calling attention to the issue of international information security under the UN framework. In 2019, Russia promulgated the Federal Law No. 90-FZ, the so-called Sovereign Internet Law—with a set of amendments to existing Russian legislation—which lays out institutional arrangements for "autonomous and controllable sovereignty" over the Internet. Russia also has a strong tradition of control over content data (Zhuravlev & Brazhnik, 2018). In 2022, the Personal Data Act of the Russian Federation was amended to establish a strict management model for cross-border data both internally and externally.

4.2. Development/Adjustment of Data Cognition

Digital technology is developing rapidly, especially with the emergence of data-based AI. The tremendous energy released by data, as well as the continuous development of its functions, has exerted a strong influence on all aspects of society. People's understanding of the essence of data is constantly being updated. In recent years, as the regulation of global cross-border data flows has entered its third stage, the understanding and claims on data of various countries are undergoing obvious changes. At the same time, with the domestic development and the international pattern changing rapidly, information technology has become an important factor in the game among countries (Lang, 2021). To some extent, data cognition on a global scale is in a critical period of exploration.

People's understanding of the objective world is constantly being updated. In terms of data, it is in the development process from an emerging phenomenon to a social entity, which has only just begun. Therefore, people's understanding of the essential attributes of data is constantly evolving. For instance, in recent years, China has elevated the perception of data attributes to the level of production factors. As time goes by, the relative positions of different countries in the global landscape are also changing, and the expectations for the value carried in data are constantly evolving. For instance, the US increasingly emphasizes that there is national security value in exploring data. Overall, the understanding of data in societies of various countries has developed from a relatively simple single dimension to a complex multi-dimensional one. This can be ascribed to the fact that the demands of human society for data have become richer. We can observe this change in cognition from the change in policy propositions.

Based on the abovementioned considerations, the intention of this article is not to propose an absolute and static view of data cognition, but to construct a developing cognitive system for a more accurate grasp of history and reality. Below, several case countries and regions will be analyzed from this perspective (see Table 2).

Table 2. Data cognition and its development.

Country and region	Starting point of data cognition		Development/adjustment
US	Property carrier	⟶	privacy rights carrier, national security carrier
China	Strategy carrier	⟶	security carrier, economic carrier
EU	Rights carrier	⟶	societal (cultural, economic) carrier
Russia	Security carrier	⟶	national development carrier (domestic construction)

The understanding of data in the US has further evolved from "property carrier" to "carrier of privacy rights and national security." The "privacy rights carrier" refers to the personal rights value centered on privacy embodied in data, a concept that primarily stems from social developments within the US. The "national security carrier" lens regards data as a critical factor that may trigger national security risks, primarily arising from external threats.

After multiple rounds of interactive games with the EU, the US is paying more and more attention to the protection of personality rights, such as privacy in data. To a certain extent, due to the external pressure of the EU, the US began to revise the market concept of data *laissez-faire*, and constantly added elements of rights protection to its data governance regime (Voss, 2020). In addition to the external pressure, the rapid development of information technology itself and the increasing impact of data-based intelligent technology on people's lives will inevitably lead to the need for the US to respond to the issue of right protection in data. Historically, in the US, privacy rights are not equivalent to civil rights. However, in the digital environment, the call for privacy rights to be regarded as civil rights is gaining larger momentum (Allen & Muhawe, 2025). At the same time, the Clean Network Initiative launched by the US against China and the recent ban on TikTok both reflect a change in the US perception of data, which emphasizes national security and a protective national strategic orientation.

It is worth noting that the US has made progress in both legislation and judicial practice of data privacy protection. Since the enactment of the California Consumer Privacy Act in 2018, the number of comprehensive privacy bills proposed by US states, as well as the number of privacy laws passed, has largely increased (see Figure 2). Among the states that have enacted privacy laws that provide consumer data privacy rights, there is almost unanimous agreement that consumers should have the right to control their own data. The American Data Privacy and Protection Act, issued on June 3, 2022, served as the basis for the American Privacy Rights Act, a major legislative proposal at the federal level, which was proposed on April 7, 2024. In the draft text of the American Privacy Rights Act, it states that the congressional intent is to "establish a uniform national privacy and data security standard in the United States" (American Privacy Rights Act of 2024, 2024). The right to privacy has also gradually taken position in the US, where *Katz v. United States* (1967) pioneered the "reasonable expectation" standard of privacy, providing a theoretical basis for privacy protection. The *Carpenter v. United States* (2018) further adapted to the digital age, extending privacy protections to electronic data and records of long-term behavior. All these reflect the change in the understanding of the inherent attributes of data in the US.

China's evaluative cognition of data has further developed from "strategy" to multiple carriers of "security" and "economy." China is gradually transitioning from a single emphasis on data sovereignty to a more comprehensive framework of data developmentalism. Over the past decade, the emphasis on data cognition

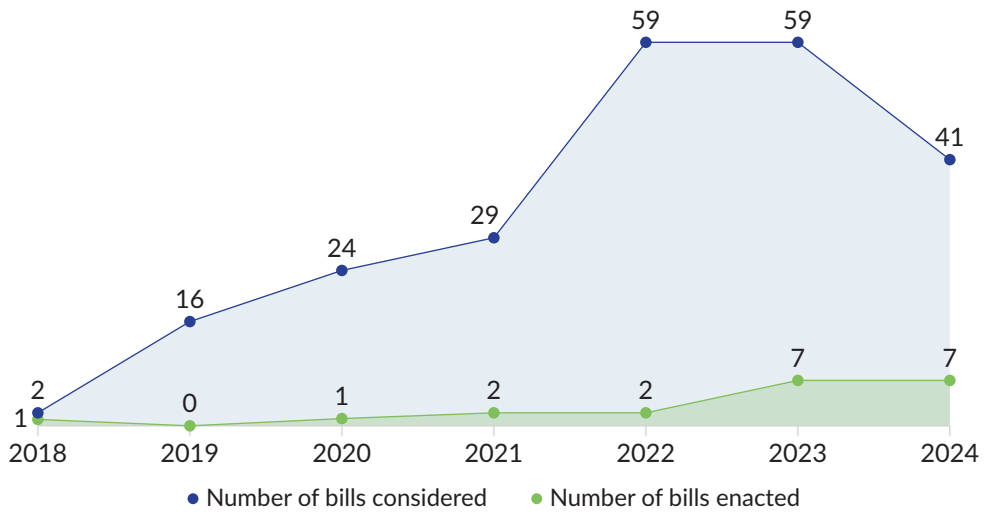


Figure 2. The growth of US state privacy legislation. Source: IAPP (2024).

in China has changed. After a period of excessive data defensivism, China has begun to shift its policy stance, representing a change in cognition as well. Shocked by Snowden's revelation in 2013, China embarked on a cybersecurity/data security as a stress response, elevating data security to a high priority. In this period, China is more inclined to recognize data as a security carrier, such as the investigation of Didi's IPO in the US in 2020. However, after the Sino–US trade war began in 2018, China began to recognize the overall beneficial role of data in the digital economy, putting forward the theory of "data as a factor of production," and starting to enrich its data cognition from the perspectives of market economy and industrial development. This shift is seen as a kind of "data developmentalism" (Meng, 2023). China has gradually transitioned from the proposition of data sovereignty to a more comprehensive data developmentism. The core of data developmentism is to regard data as a driving force for the all-round development of society, emphasizing that the priority value of data lies in promoting economic and social development. In fact, China has been developing its understanding of information technology and the Internet in a pragmatic way, and its governance methods have been constantly updated (Liu, 2023).

The EU has further extended its evaluative cognition of data from the carrier of rights to the carrier of cultural values, while separating the economic carrier, and generally placing the data in the position of societal comprehensive carrier, as the societal (cultural, economic) carrier. After the promulgation of GDPR, the data rights protection system has been basically established. Followed by the Regulation on a Framework for the Free Flow of Non-Personal Data in the European Union, it is a timely recognition of the economic value of data. In 2015, the European Commission published the European Digital Single Market Strategy, which aims to create an EU digital market to facilitate data flows. In 2020, the European Commission launched its European Data Strategy, which aims to make the EU a "world model" for better data-driven decision-making by businesses and the public sector, thereby creating an open data market for the world. The common data spaces proposed by the EU as the cornerstone of the European data strategy play a key role in combining the necessary infrastructure with data governance mechanisms. The ongoing Digital Fairness Act, the so-called "law of everything" for the digital economy and the digital world as a whole (Zhu, 2024), has heightened expectations for the social value that data carries.

Although Russia still regards national security as the primary value of data, it is increasingly focusing on the development value of data. In the context of Russia, this new evaluative cognition can be called "the carrier of national development," shifting from an overly emphasis on external threats to an internal construction perspective. Especially after the war began between Russia and Ukraine, under strong external sanctions, the external development of Russia's digital economy has been greatly challenged and even stalled. From the perspective of national security, Russia has implemented data localization more thoroughly, which also leads to Russia's attention on data being more focused on the development of its national economy. In other words, Russia is more concerned about how these local data can serve a social and economic utility. Although the legislation is strict, there is room for maneuver in judicial enforcement (He, 2016; Sun & Haritonova, 2022). The Russian courts have punished companies for not complying with relevant laws; although the amount of penalties is negligible for companies, it also shows the logic of Russian justice: to balance the dual goals of personal data protection and industrial development, and not to take an overly biased attitude (Sun & Haritonova, 2022). Under this cognition, Russia is actively promoting the compilation of the Digital Code, which is also an effort to actively promote the construction of a domestic digital economic development system.

5. The Choice of Governance Tools Under Data Cognition

Decision making and action are important aspects of evaluative cognition. Supported by the different evaluative cognitions of data, to realize their inherent value expectations, different countries and regions choose the corresponding governance tools, and each forms a complete set of governance propositions.

5.1. US: Market + Ideology: Advocating the Establishment of a Global System of Free Data Flows

Starting from the data property cognition, the US often puts cross-border data flows in the context of the Internet economy, and regards the data flows as an indispensable part of the market economy, including the internal business data flows of transnational corporations, the optimal configuration of data of Internet companies, and the free transaction of data itself as a product, etc. This proposition is embodied in the CBPR system under the APEC framework in 2012, which adheres to the principle of supporting data free-flow under the free market law. Therefore, the market is the basic tool for the governance of cross-border data flows for the US. This logic of taking the market economy as a governance tool has developed into a liberal ideology to a certain extent, with a strong color of exclusivity. In American logic, data free-flow is the proper meaning of a market economy: Opposing it represents a rejection of the market economy, and opposing the market economy means rejecting freedom.

With their two pillars of governance—market and ideology—the US advocates the establishment of a global system for the free flows of data. Taking the APEC privacy framework as the basic model, the US tried to build a competing global data governance system on the basis of the global digital economy by updating the TPP proposal (which was later withdrawn) and the trans-Atlantic data flows framework as its core component.

However, based on the continuous understanding of the carrier of privacy rights and the carrier of national security, the US began to pay attention to the data privacy protection system, promote the development of privacy rights in legal rules, and construct national security exceptions for data flows in the international system. Meanwhile, in the face of the international competition system, the US has introduced data

"decoupling" policies against "adversary" countries like China and even established a global export control regime for AI.

5.2. China: Sovereignty + Trade: Advocating a Global System of Secure and Orderly Data Flowing

China has taken an attitude of "Internet sovereignty" from the beginning of participating in the formulation of rules on cross-border data flows, and it has long advocated for its absolute sovereignty over data produced in China and requires data localization (Liu, 2020). This is based on China's original strategic cognition of data—a simple logic of "my data is mine." The most typical evidence is the provision on data localization in Article 37 of the Cybersecurity Law passed in 2016. However, as China's understanding of data has further shifted into a factor of production, the adoption of cross-border data flows governance has begun to pay more attention to the dimension of international trade. China is also paying increasing attention to participating in the negotiation and rulemaking of international digital trade-related agreements (He, 2022). It has actively participated in the World Trade Organization's e-commerce negotiations and signed the Joint Statement Initiative on e-commerce in 2021. At the same time, by advocating rules in multilateral international trade negotiations, it has joined the Digital Economy Partnership Agreement, the Regional Comprehensive Economic Partnership, and actively applied to join the Comprehensive and Progressive Agreement for Trans-Pacific Partnership.

In 2024, China stated that: "Cross-border data flows are crucial to the e-commerce, digital trade and even the economy, science, technology and culture of various countries…and realize a new type of globalization driven by data flows" (Cyberspace Administration of China, 2024). It further proposed to "encourage cross-border data transmission through electronic means for the needs of normal commercial and social activities, so as to realize that global e-commerce and digital trade will provide new impetus for economic growth and sustainable growth of all countries" (Cyberspace Administration of China, 2024).

5.3. EU: Moral + Market: Advocating a Global System With Data Rights Protection at Its Core

From the very beginning, the EU has been concerned about human rights embedded in data. When it comes to cross-border data flows, its code of conduct is more of a moral proposition. The GDPR provides a solid foundation for the free flow of data in line with European values. The European Data Strategy and the Shaping Europe's Digital Future initiative have repeatedly mentioned that "the EU is a global leader" and "the EU is setting global norms for the digital economy," which indicates that the EU has begun to utilize its regulatory capabilities to promote European rules and establish global standards (Xia, 2023). Later, the EU began to attach importance to the material value contained in data, advocating the market-oriented development of data to empower Europe's digital development, which is enacted in the Regulation on the Free Flow of Non-Personal Data, the European Data Act, and other later legislation.

5.4. Russia: Sovereignty, Advocating Independent and Controlled Data Flows

Russia sees data from the perspective of security, which still remains its core perspective. Russia faces an international landscape that has long been dominated by the Western bloc, so this demand for security is relative to that of the US and its allies. It is natural for Russia to choose sovereignty as the starting point of governance, from the service mode to the sovereign mode (Martynova & Shcherbovich, 2024). In the face

of an international system governing cross-border data flows, Russia advocates for the orderly flows of data under autonomy and control. By imposing legal obligations on enterprises, Russia has achieved comprehensive government control over data storage, cross-border transmission, processing, and other links, thereby taking the initiative in the cross-border flow of domestic data (see also He, 2016).

6. Changes in the Global Governance Landscape Under the Development of Data Cognition

The global pattern of cross-border data flows is not static, and it is not always solidified by ideology; it is a state of flows driven by cognitive changes. In terms of historical stages, the first phase was basically a transatlantic game between Europe and the US, about how data flowed from Europe to the US, and no other countries were involved. The second phase, based on the American data free market cognition and taking APEC as its starting point, tried to construct a global data free flow market system. In the third phase, in the "awakening" of developing countries to data, the rise of cognition theories—national security, privacy rights protection, and national strategy empowerment—the global pattern of cross-border data flows witnessed a trend towards data localization, fragmentation of rules, and strong institutional competition.

The US transitioned from a political system characterized by consistent freedom and openness to one that emphasizes defense and regulation. On 25 October 2023, during the WTO's Joint Declaration on e-Commerce Initiative meeting, the office of US Trade Representative Catherine Day announced that the US would abandon some of its long-held digital trade propositions, including the requirement for the free flow of cross-border data—indeed, the US is reviewing its current approach to trade rules in sensitive areas such as data and source code (Trachtenberg, 2025). In July 2024, the WTO officially issued the Joint Declaration on e-Commerce Initiative: WTO members negotiated on e-commerce rules and published the latest text of the agreement, requiring negotiating parties to prohibit tariffs on cross-border data transfers; the US did not support this initiative. "The current text falls short and more work is needed, including with respect to the essential security exception," the US ambassador to the WTO said in a statement (US Mission Geneva, 2024). With the profound realignment of global strategic competition, the US data regulatory policies have gradually shifted toward a model of "limited free flow under the premise of security" (Zhou & Yan, 2025). In the US, this policy shift also has its domestic political motivations; however, the shift towards cross-border data flows is closely related to the country's evaluative cognition of data, which aligns with the US' greater concern for the security value contained in data. Outside the international trade arena, the US has issued regulatory policies for data and artificial intelligence from a political perspective and has started to build a pan-national security political system that is different from what the free market had previously advocated.

China is moving from passive defense to integration into the global market system—from isolation to integration. Having gone through a strict data localization policy, China is moving from a passive defensive posture to a more active attitude of openness and integration into the international system. In 2024, China issued the Global Cross-Border Data Flow Cooperation Initiative, which sets out China's position and proposition on the issue of cross-border data flows, echoing the concerns of all parties in the international community about cross-border data flows and expressing a common willingness to promote cooperation. In March 2024, the Cyberspace Administration of China formulated the Regulations on Promoting and Regulating Cross-Border Data Flows—a move regarded as an important shift in China's policy stance on data localization and a practical measure to be actively integrated into the international system. It is worth noting

that China is now promoting mechanisms for cross-border data flow and exchanges between China and the EU for the second time in 2025. Such a shift makes China likely to gradually become one of the most dominant players in data transfer (Chen & Gao, 2024).

The EU is mining the economic benefits from the value of data rights, moving from a moral system to a comprehensive system of digital society. The EU attaches more and more importance to the economic and social value created by data. While insisting on the protection of data rights, the EU is also actively seeking the construction of a comprehensive governance system based on data. With GDPR at its core, the EU has set a global moral benchmark for data rights protection with the construction of a more comprehensive and more basic legal system in the digital field, such as the Digital Market Law, the Digital Services Law, and the Artificial Intelligence Act. The Digital Fairness Act constitutes the last piece of the "jigsaw puzzle" of digital society legislation. The EU's new claims on data are not only about the protection of information privacy rights, but also reframed itself at a level of a comprehensive governance system for the digital society. The EU is striving to become a "good global actor" in data governance (Chen & Gao, 2022) and intends to be the leader of the world's basic regime construction, playing an important leading role in the development of human digital civilization.

Russia is further seeking a way out of isolation for security and development. The Russia–Ukraine war is producing an impact on Russia's domestic politics and economy, and directly affecting Russia's cybersecurity. To deal with this situation, Russia has made detailed provisions on information legislation and the cross-border flows of information data in its national security strategy (Wen & Tan, 2024). In July 2022, the National Parliament of the Russian Federation made extensive amendments to the Law on Personal Data of the Russian Federation, adding the pre-procedure for cross-border transfer of personal data, limiting the range of countries in which cross-border transfer of data can be carried out, and adding the circumstances in which such transfer is prohibited or restricted, requiring the operators to inform the supervisory authorities of the intention to carry out the cross-border data transfer.

The digital sanctions imposed on Russia by Western countries have brought many challenges to Russia in the field of digital technology, but those pressures have also prompted Russia to accelerate the pace of independent innovation in digital technology. Russia has fundamentally reduced the risks associated with the adoption of foreign programs, computer technology, and telecommunications equipment, and has done its best to protect the digitalization process of the public administration system and the economic sector from any potential negative external influences, turning to build its domestic equipment, technologies, programs, and products. Data-based domestic development has therefore become an important strategic choice for Russia.

The pattern of cross-border data flows in the world demonstrates a new trend. The construction of a global data political system has accelerated, with the US becoming a strong leader in this system and constantly incorporating elements of privacy protection. China's shift has led to the further improvement of the global digital trading system and the strengthening of the national security element of the international trading system (Kalin, 2024, pp. 77,132). The EU has further evolved from a value system to a social system, transcending physical competition, and is likely to be a leader in the development of human right-based digital civilization. Russia's inward turn is a constant warning to countries that are unpopular with the West to pay more attention to data security, which turns to be the driving force of global Internet fragmentation rather than positive factor for global digital development.

The changes in China, the US, the EU, and Russia are naturally important forces for the change of the world, but other countries and regions are also in the overall trend of change and are equally important factors. However, for the reasons mentioned above, this article cannot analyze each country individually. However, from the theoretical perspective of cultural values, we can roughly witness such trends: The developing countries, represented by Brazil and India, actively advocate data developmentalism, and the developed countries are strengthening the pursuit of value leadership while maintaining the economic leadership; what's more, and the countries deeply involved in geopolitical conflicts, including the countries in the Middle East and Eastern Europe, are trapped in a growing security struggle. Under these trends, the global cross-border data flows governance has generally entered a period of comprehensive institutional construction of economy, politics, and culture. In addition to the realistic interest game, we must see the value proposition and the most fundamental epistemological changes in this system construction process.

7. Concluding Remarks

The demands and claims on data have been constantly changing, and the global consensus and rules for regulating cross-border data flows are still lacking. The lack of trust has seriously hindered the global circulation and sharing of data (OECD, 2023). The data flows that enable the Internet to function as a global network are increasingly adhering to geographical national boundaries, thereby delineating a map of cyberspace segregated by national territorial boundaries. This phenomenon has given rise to persistent concerns regarding the fragmentation of the Internet (Drake et al., 2016; Mueller, 2017). In this sense, ruling cross-border data flows becomes an important way for states to compete for control of cyberspace, as well as a challenge of the times for global Internet governance.

Data is the foundation of AI development, and understanding data inevitably shapes our understanding of AI. A theoretical path of data cognition can be extended to encompass the overall cognition of internet-data-AI-technology across different countries and regions. Since Martin Heidegger, philosophers and social theorists have been discussing how people should understand modern technology. The discussion of data cognition may contribute some new ideas to that question. This article attempts to present a timely overview of the development of the global data governance landscape from the perspective of evaluative cognition. However, the complex reasons driving the changes in evaluative cognition have not been fully studied. The ruling of cross-border data flows is not only a practical public policy issue but is also related to the future of digital civilization, requiring further exploration of its philosophical and historical significance.

Acknowledgments

Thanks are due to the thematic issue's editors Xinchuchu Gao and Xuechen Chen, as well as the reviewers for their valuable comments. The reasoning this article is based on was initially presented at the CAICT symposium in 2023—I thank Dr. Bo He for the invitation. Also, I would like to thank Letian Cheng and the editors for their meticulous proofreading.

Conflict of Interests

The author declares no conflict of interests.

References

Allen, A. L., & Muhawe, C. (2025). Is privacy really a civil right? *Berkeley Technology Law Journal*, *40*, Article 541. https://doi.org/10.15779/Z38KK94D6R

American Privacy Rights Act of 2024, § 118U.S.C. (2024).

Brooks, D. (2013, February 4). The philosophy of data. *New York Times*. https://www.nytimes.com/2013/02/05/opinion/brooks-the-philosophy-of-data.html

Cyberspace Administration of China. (2024). *Global cross-border data flow cooperation initiative*. https://www.cac.gov.cn/2024-11/20/c_1733706018163028.htm

Carpenter v. United States, 138 S.Ct. 2206 (2018).

Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory Law Journal*, *64*, Article 677. https://scholarlycommons.law.emory.edu/elj/vol64/iss3/2

Chen, X., & Gao, X. (2022). Comparing the EU's and China's approaches in data governance. In E. Fahey & I. Mancini (Eds.), *Understanding the EU as a good global actor* (pp. 209–225). Edward Elgar Publishing.

Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, *100*(6), 2419–2440. https://doi.org/10.1093/ia/iiae237

Daston, L. (1994). Historical epistemology. In K. Chandler, I. Davidson, & D. Harootunian (Eds.), *Questions of evidence: Proof, practice, and persuasion across the disciplines* (pp. 282—289). University of Chicago Press.

Daston, L., & Galison, P. L. (2007). *Objectivity*. Princeton University Press.

Data 'new form of wealth,' take it into account of developing nations' needs: India. (2019, June 28). *The Economic Times*. https://economictimes.indiatimes.com/tech/internet/data-new-form-of-wealth-needs-to-take-into-account-developing-nations-needs-india/articleshow/69988888.cms?from=mdr

Drake, W. J., Vinton, C. G., & Kleinwächter, W. (2016). *Internet fragmentation: An overview*. World Economic Forum.

Fazio, R. H. (2007). Attitudes as object–evaluation associations of varying strength. *Social Cognition*, *25*(5), 603–637. https://doi.org/10.1521/soco.2007.25.5.603

Fishman, W. L. (1980). Introduction to transborder data flows. *Stanford Journal of International Studies*, *16*(Summer 1980), 1–25.

Harari, Y. (2016). *Homo Deus: A brief history of tomorrow*. Vintage.

He, B. (2016). Legislation and enforcement of cross-border data flows rules in Russia. *Big Data Research*, *2*(6), 129–134.

He, B. (2022). Challenges and countermeasures for China's participation in international rules of the cross-border data flows. *Administrative Law Review*, *4*, 89–103.

IAPP. (2024). *Comprehensive US state privacy legislation in 2024*. https://iapp.org/resources/article/us-state-privacy-laws-overview

Kalin, R. P. (2024). *Digital trade and data privacy*. Springer Nature.

Katz v. United States, 389 U.S. 347 (1967).

Kirby, M. D. (1980). Transborder data flows and the basic rules of data privacy. *Stanford Journal of International Studies*, *16*, Article 27.

Kuner, C. (2011). *Regulation of transborder data flows under data protection and privacy law* (Digital Economy Paper No. 187). OECD Publishing. http://doi.org/10.1787/5kg0s2fk315f-en

Lang, P. (2021). How the internet changes international relations. *International Political Science*, *2*, 90–121.

Lazarus, R. S. (1991). *Emotion and adaptation*. Oxford University Press.

Leiner, B., Cerf, V., Clark, D., Robert, K., Kleinrock, L., Lynch, D., Postel, J., Roberts, L., & Wolff, S. (1997). *Brief history of the internet*. Internet Society. https://www.internetsociety.org/internet/history-internet/brief-history-internet

Liu, J. (2023). Rethinking Chinese multistakeholder governance of cybersecurity. In I. Johnstone, A. Sukumar, & J. Trachtman (Eds.), *Building an international cybersecurity regime: Multistakeholder diplomacy* (pp. 185–200). Edward Elgar Publishing.

Liu, J., & Cui, B. (2023). On the paradigm innovation of global governance in cyberspace. *Journalism & Communication Research*, *30*(7), 75–91.

Liu, J. (2020). China's data localization. *Chinese Journal of Communication*, *13*(1), 84–103. https://doi.org/10.1080/17544750.2019.1649289

Martynova, E., & Shcherbovich, A. (2024). Digital transformation in Russia. *Computer Law & Security Review*, *55*, Article 106075. https://doi.org/10.1016/j.clsr.2024.106075

Meng, Q. (2023, March 18). The establishment of the National Data Bureau will accelerate the construction of digital China. *IFENG NEWS*. https://cq.ifeng.com/c/8NzaXQDPi6m

Mueller, M. (2017). *Will the internet fragment?* Polity.

Mueller, M., & Grindal, K. (2018). *Is it "trade?" Data flows and the digital economy* [Paper presentation]. TPRC 46: The 46th Research Conference on Communication, Information and Internet Policy, DC, United States. http://doi.org/10.2139/ssrn.3137819

National Data Administration of PRC. (2024). *Explanations of common terms in the field of data (first batch)*. https://www.nda.gov.cn/sjj/zwgk/zcfb/1230/20241230160715745237413_pc.html

Novotny, E. J. (1980). Transborder data flows and international law: A framework for policy-oriented inquiry. *Stanford Journal of International Studies*, *16*, Article 141.

Obendiek, A. S. (2022). What are we actually talking about? Conceptualizing data as a governable object in overlapping jurisdictions. *International Studies Quarterly*, *66*(1), Article sqab080. https://doi.org/10.1093/isq/sqab080

OECD. (2023). *Moving forward on data free flow with trust: New evidence and analysis of business experiences* (Digital Economy Papers No. 353). OECD Publishing. https://doi.org/10.1787/1afab147-en

Oliver, G., Cranefield, J., Lilley, S., & Lewellen, M. (2023). Data cultures: A scoping literature review. *Information Research an International Electronic Journal*, *28*(1), 3–29. https://doi.org/10.47989/irpaper950

Oliver, G., Cranefield, J., Lilley, S., & Lewellen, M. J. (2024). Understanding data culture/s: Influences, activities, and initiatives: An Annual Review of Information Science and Technology (ARIST) paper. *Journal of the Association for Information Science and Technology*, *75*(3), 201–214. https://doi.org/10.1002/asi.24737

Simon, H. A. (1980). Cognitive science: The newest science of the artificial. *Cognitive Science*, *4*(1), 33–46.

State Council of the People's Republic of China. (2015). *Outline of action to promote big data development*. https://www.gov.cn/gongbao/content/2015/content_2929345.htm

Sun, Q., & Haritonova, Y. (2022). Legislative characteristics and trends of cross-border data flow in Russia in the context of data sovereignty. *Russian Studies*, *2*, 87–107.

The Central Committee of the Communist Party of China, & The State Council of China. (2020, March 30). *Opinions on building a more complete market-based mechanism for the allocation of factors* [Government document]. https://www.gov.cn/zhengce/2020-04/09/content_5500622.htm

Trachtenberg, D. (2025). *Digital trade and data policy: Key issues facing congress*. Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF12347

US Mission Geneva. (2024, July 26). *Statement by Ambassador María L. Pagán on the WTO e-Commerce Joint Statement Initiative*. https://geneva.usmission.gov/2024/07/26/statement-by-ambassador-maria-l-pagan-on-the-wto-e-commerce-joint-statement-initiative

Voss, W. G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*(3), Article 485. https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7

Wang, R. (2018). Cognition and recommendations of cross-border data flow policies. *Information Security and Communications Privacy*, *3*, 41–53.

Wen, M., & Tan, R. (2024). Regulatory cooperation on cross-border data flows under the threshold of data sovereignty and China's response. *International Trade*, *6*, 5–14. https://doi.org/10.14114/j.cnki.itrade.2024.06.003

Xia, H. (2023). EU Progress in Legislation for Data Governance and Implications for China. *Wuhan University International Law Review*, *7*(4), 106–118.

Xu, D. (2018). International pattern of personal data cross-border flow regulation and China's response. *Legal Forum*, *33*(3), 130–137.

Zheng, Y. (2007). *Technological empowerment: The Internet, state, and society in China*. Stanford University Press.

Zhou, H., & Yan, W. (2025). The shift in U.S. cross-border data regulation: From free flow to secure flow. *Chinese Review of International Law*, *3*, 100–114.

Zhu, Y. (2024, November 21). Oumeng shuzigongping faan qianzhan. *Legal Weekly*. http://m.legalweekly.cn/whlh/2024-11/21/content_9089351.html

Zhuravlev, M. S., & Brazhnik, T. A. (2018). Russian data retention requirements: Obligation to store the content of communications. *Computer Law & Security Review*, *34*(3), 496–507. https://doi.org/10.1016/j.clsr.2017.11.011

About the Author

Jinhe Liu is an assistant professor at the School of Journalism and Communication, Peking University. He earned his PhD at Tsinghua University, focusing on Internet governance, medium governance, and communication theory. He has an interdisciplinary background in journalism and communication, law, and management, and is recruiting doctoral students.

Politics and Governance
2025 • Volume 13 • Article 10461
https://doi.org/10.17645/pag.10461

ARTICLE

Open Access Journal

Beyond the Ban: TikTok and the Politics of Digital Sovereignty in the EU and US

Fabio Cristiano [1] and Linda Monsees [2]

[1] Department of History and Art History, Utrecht University, The Netherlands
[2] Institute of International Relations Prague, Czechia

Correspondence: Fabio Cristiano (f.cristiano@uu.nl)

Submitted: 1 April 2025 **Accepted:** 19 August 2025 **Published:** 8 October 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance", edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

This article explores the emergence of TikTok as a central issue in contemporary debates on foreign interference, platform regulation, and the governance of transnational data flows. Both the European Union and the United States have expressed concerns about TikTok's potential risks and have implemented various regulations. Through a comparative analysis of EU and US regulatory discourses, this article examines how claims to digital sovereignty are mobilised in efforts to govern the Chinese-based platform. In doing so, this study advances ongoing debates on the regulation of large-scale digital platforms and data infrastructures. Our analysis reveals that whereas the EU emphasises regulatory autonomy, public health, and democratic integrity in governing cross-border data flows, the US frames TikTok in a more overtly securitised approach rooted in techno-nationalism and strategic infrastructural decoupling from China. More broadly, the article also argues that when framed as a countermeasure to foreign interference, digital sovereignty is increasingly rearticulated as a security-centric concept that subsumes broader societal harms, and it risks assuming authoritarian connotations.

Keywords

digital sovereignty; European Union; foreign interference; platform regulation; public health; TikTok; transnational data governance; United States; youth protection

1. Introduction

Foreign interference, cybersecurity, and disinformation are among the key concerns policymakers have regarding the role of large social media platforms. In recent years, TikTok—the short-video platform owned by the Chinese company ByteDance—has become a catalyst for these concerns, prompting exceptional

global scrutiny and policy interventions, including national bans and ad-hoc restrictions in several countries (Gray, 2021; Jia & Liang, 2021). Both the EU and the US have placed TikTok at the top of their policy agendas, with ongoing procedures targeting the platform over concerns of foreign interference. For example, in December 2024, the European Commission launched an investigation into whether TikTok had played a role in facilitating electoral interference during Romania's annulled elections. A few weeks later, on his inauguration day in January 2025, President Trump announced the decision not to go ahead with the long-discussed US ban on the app, instead floating the idea of a takeover by an American sovereign fund. These most recent interventions point to a significant development: TikTok evolved from a video-sharing app popular among Gen Z into a central element of geopolitical struggles over digital technology and regulation.

Central to policymakers' concerns about TikTok are three interconnected issues: First, TikTok's ownership structure raises fears that Chinese authorities might access user data under China's expansive national security laws (Su & Tang, 2023). Second, permissive content moderation policies on the platform have been criticised for facilitating disinformation and amplifying authoritarian narratives (Bösch & Divon, 2024; Zeng & Kaye, 2022). Third, TikTok's unique personalised algorithm has sparked additional worries regarding mental health, addiction, and youth protection (Grandinetti & Bruinsma, 2023). Scholarship on TikTok has broadly explored these multiple concerns from a geopolitical perspective (see Bernot et al., 2024; Gray, 2021; Lin & de Kloet, 2023). In this article, we examine the EU and US regulatory discourses targeting TikTok as elements of enacting digital sovereignty against foreign interference. We situate the discussion firmly in the rising geopolitical and geoeconomic debates that shape contemporary platform and data governance efforts (Bellanova et al., 2022; Broeders, 2021; Fägersten et al., 2023).

Digital sovereignty is usually understood as the attempt to keep tighter control over digital infrastructure and data flows within national borders (Pohle & Thiel, 2020). In today's tense geopolitical context, it is often discussed alongside the threat of foreign interference, states or non-state actors trying to shape political and social life abroad through digital means (Dowling, 2021; Ördén & Pamment, 2022). What makes digital sovereignty particularly complex is the tension between the global, decentralised character of digital platforms and governments' territorial ambitions to regulate them. This article addresses this contradiction, paying particular attention to the way data localisation efforts illustrate it. In doing so, we draw attention to the way many different policy issues are deliberately wrapped into the language of digital sovereignty. This broadens the term's political usefulness, but at the same time leaves it increasingly vague. Taken together, these contradictions come to the fore when digital sovereignty is invoked as a framework for regulating platforms against the backdrop of today's tense geopolitical environment (Casero-Ripollés et al., 2023; Flyverbom et al., 2019; Monsees, 2024).

This article compares the EU and US approaches to regulating TikTok, examining two actors with seemingly distinct policies aimed at establishing digital sovereignty and/or strategic autonomy through decoupling from foreign partners and strengthening domestic supply chains. While both recognise the strategic importance of an autonomous digital infrastructure and share concerns about foreign interference, including from China, the EU and US approaches diverge significantly (Couture & Toupin, 2019). The EU articulates its digital sovereignty ambitions as a comprehensive strategic normative project that brings together democratic, economic, and geopolitical objectives (Bellanova et al., 2022). This framing manifests in systematic regulatory instruments such as the General Data Protection Regulation (GDPR), the Digital Services Act (DSA), and the Digital Markets Act (DMA). Conversely, the US prioritises digital sovereignty

through the lens of national security and technological supremacy over adversaries (Couture & Toupin, 2019). It thus favours more targeted interventions such as executive orders, investment screening, and targeted bans, such as the recent Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA). The relationship between the EU and the US on these matters is more ambivalent. While more autonomy is the mutual goal, they continue to perceive each other as partners in many areas. Yet, since the start of the second Trump administration, mutual trust in future cooperation has been eroding.

Regulating TikTok is embedded in a (re-)negotiation about the relationship with China. For the EU and US, policy debates around TikTok are to be understood considering broader geopolitical efforts to curb Chinese ambitions in establishing technological and market influence globally. These have been characterised as the "Beijing effect," emphasising how China reshapes data governance through infrastructural exports and normative influence (Erie & Streinz, 2021). This model challenges Western paradigms by promoting data sovereignty in other countries, albeit via centralised control by China (Creemers, 2022). As such, TikTok is increasingly viewed as a potential vector of Chinese influence and, therefore, an element of the broader geopolitical struggle over technology. TikTok is also the only non-US-based large social media platform, thus presenting a unique case study for testing and comparing EU and US approaches to digital sovereignty and the regulation of a digital platform which is "foreign" to both. In this article, we argue that both the US and the EU use TikTok as a trial case to test regulatory mechanisms despite their differences in threat depiction.

To explore these dynamics, our study employs a qualitative policy analysis of regulatory discourses. These include legislative texts, public statements, judicial rulings, and media reports from 2020 to mid-2025. This interpretative analysis focuses on the discursive construction of TikTok as a policy concern and security threat and how digital sovereignty is mobilised as a "discursive tool" within this scope (Pohle & Thiel, 2020). Considering the asymmetry in nature between the two compared actors, we focus on regulatory logics rather than deploying a systematic policy comparison. More concretely, we examine how the main themes in digital sovereignty debates—economic questions like trade and market access, geopolitical concerns such as surveillance and great power rivalry, and democratic issues including free speech and electoral integrity—find their way into regulatory discussions about TikTok (Floridi, 2020; Monsees & Lambach, 2022). We then consider TikTok's reactions to EU and US policies, noting both its moves toward compliance and the moments when it has openly pushed back. This helps us understand how digital sovereignty is shaped in relational terms. After this introduction, Section 2 sets out the conceptual tension between digital sovereignty and transnational data governance, with particular attention to the risk of foreign interference on social media platforms. Sections 3 and 4 turn to EU and US regulatory discourses on TikTok, examining how each frames the problem and the kinds of policy responses that follow. In Section 5, we compare the different approaches, pointing out where they overlap and where they diverge. The final section then considers what our findings mean, both for theory and for the practice of digital sovereignty.

2. Platform Regulation Meets Digital Sovereignty: From Foreign Interference to Data Localisation

This section outlines how the idea of digital sovereignty evolved across different political contexts. It then considers how it collides with platform regulation, most clearly around questions of foreign interference and efforts to localise data.

2.1. Digital Sovereignty: An Evolving Agenda

Digital sovereignty has become a prominent theme in policy and academic debates. In its earlier formulations, it has traditionally been understood as the authoritarian alternative to democratic platform and data governance, particularly in countries like China and Russia, where state control over digital infrastructures drifted away from multistakeholder models (Pohle et al., 2025; Litvinenko, 2021). In recent years, however, the term has also gained ground in liberal contexts. Within the EU, in particular, it relates to debates on strategic autonomy and the European ambition to reassert control over digital platforms (Broeders et al., 2023). Policy initiatives under the banner of digital sovereignty combine different aims: protecting the economy, reducing reliance on foreign actors, and building more resilient infrastructures (Floridi, 2020). Related language—"technological sovereignty," "strategic autonomy," or even "de-risking"—is often used interchangeably to describe the same rationale to secure financial, digital, and infrastructural resources (Bellanova et al., 2022).

At the heart of these debates lies the question of how far states can, and should, regulate the activities of transnational tech companies operating within their borders, and in doing so, reassert public authority over them (Floridi, 2020; Kelton et al., 2022). Some scholars consider this a necessary reassertion of public authority over private power (Farrand & Carrapico, 2022). In contrast, others warn that digital sovereignty may legitimise protectionist or illiberal policies under the guise of national security or strategic autonomy (Broeders et al., 2023). While digital sovereignty is often conceptualised within Western discourses as a liberal project promoting resilience and openness, its authoritarian roots reemerge nowadays in a geopolitical tense situation where security measures are enacted through the regulation of technology (Musiani, 2022; Pearson, 2024). As we argue in this article, this development is evident in recent digital sovereignty efforts enacted to counter foreign interference on social media platforms.

2.2. Foreign Interference and the Localisation of Data

The issue of foreign interference is thoroughly entangled with academic and policy conceptualisations of digital sovereignty. Pohle and Thiel (2020, p. 8) define digital sovereignty as "a state's ability to govern, regulate, and protect its digital infrastructure, data flows, and online activities independently, without undue external influence or interference." In its critique of the concept, Mueller (2020) argues that states think that by lacking digital sovereignty, they remain vulnerable to foreign interference through data manipulation, infrastructural control, or cyber espionage. They thus conceive and prioritise reasserting authority over digital platforms as an ontological aspect of their sovereignty. Foreign interference is, however, an elusive concept. On the one hand, it refers to illegitimate, covert manipulation efforts by a foreign entity aimed at interfering with democratic processes and sovereignty. The idea has also faced pushback when it is stretched to cover activities that, while adversarial, are considered lawful—like lobbying or political influence campaigns (Fridman, 2024). At times, it is muddled together with less precise concepts such as hybrid warfare, information warfare, or grey-zone tactics (Cristiano & van den Berg, 2024). Many European civil society groups have warned that leaving "foreign interference" loosely defined risks harming freedom of expression ("EU: Foreign interference directive," 2024). The TikTok case exemplifies the tensions around foreign interference, as states grapple with asserting territorial authority and sovereignty over a platform that crosses national boundaries and whose regulation is entangled with geopolitical competition with China.

Digital sovereignty's ambition to reassert public authority over transnational tech companies also intersects with strategies to govern data and its localisation within national borders (Komaitis, 2017). While states seek to assert territorial authority over digital infrastructures, efforts to impose borders on data are complicated by the decentralised global networks through which data flows operate (Meltzer, 2015). While some advocate for localisation measures, such as requiring data to be stored on servers within national borders, critics argue that such strategies are technically complex, economically costly, and risk fragmenting the internet into competing national silos (Mueller, 2017; Pohle & Santaniello, 2024; Radu, 2019). A growing body of scholarship challenges the binary opposition between transnational data flows and state territory. Lambach (2019) shows how it is continually deterritorialised and reterritorialised through practices like content filtering, infrastructure monitoring, and jurisdictional claims. Similar critiques have been developed in relation to different empirical contexts (Cristiano, 2019; Glasze et al., 2023; Salamatian et al., 2019).

Claiming sovereignty over data also introduces a legal and geopolitical dimension to the discussion on platforms and transnational data governance (Irion, 2012; Woods, 2018). Regarding TikTok, the platform's Chinese ownership raises fears that user data could be accessed by Chinese authorities, thereby undermining national sovereignty and user privacy. In addition, states are concerned with regulating platform content, especially the spread of disinformation and the lack of tools to control it. In this context, the issue is not only where the data are physically located but also which legal regimes apply to them and what this means for accountability and enforcement of data governance (Voss, 2020). In its ideal type, traditional platform governance models emphasise digital platforms' multi-actor dynamics and infrastructural politics. In contrast, digital sovereignty emphasises a state-centred claim to control digital technologies and infrastructures (ten Oever et al., 2024). In recent years, however, the concept has been reformulated in ways that increasingly dictate platform regulation (Pohle & Voelsen, 2022). States now seek to govern—or in some cases exclude—platforms in the name of protecting national interests, securing data, or shoring up political legitimacy. These moves extend beyond strategy and markets. They also reach into the terrain of fundamental freedoms and liberal values (Broeders et al., 2023). As discussed earlier in this section, both digital and data sovereignty intersect in the broader concern over foreign interference, which becomes the disruptive element in otherwise open digital ecosystems. When digital platforms are, or are even thought to be, influenced by a foreign entity, the legitimacy of transnational data flows becomes contested. This is particularly sensitive in places such as the EU, where openness of markets and protection of individual freedoms are taken as core principles (Broeders et al., 2023). Against this backdrop, the use of outright bans to safeguard digital sovereignty reveals another, and more fundamental, tension: how to reconcile liberal values with the need to assert control over data and infrastructures.

3. The EU and TikTok

This section explores the EU's multifaceted regulatory approach to TikTok as part of the Union's broader push for digital sovereignty and an increasingly assertive role in the digital domain. As the previous section highlighted, regulating platforms and countering foreign interference have become central to this project.

3.1. Frameworks and Regulations

The EU's concern with privacy and tech regulation can be traced back to the Snowden revelations, which set off intense debates about surveillance and state power (Deibert, 2015; Der Derian, 2022). Since then, its

regulatory mechanism has expanded dramatically. It now covers not only the largest social media platforms but also a broader set of multinational tech companies (Flonk et al., 2024). The DSA stands out among these measures. It is intended to protect consumers and safeguard citizens' rights (Heldt, 2022). It primarily protects privacy and freedom of speech. Through the DSA, the European Commission has initiated several investigations targeting TikTok and other companies, including X and Alibaba. The DSA is only one aspect of a broader trend of the EU's attempts to strongly regulate digital platforms, which also includes specific policies on foreign interference and data localisation—such as the EU's Cybersecurity Strategy (2020), the Network and Information Security (NIS2) Directive (2022), and data localisation initiatives like the GAIA-X project. In 2023, the European Commission issued a proposal to introduce harmonised EU-wide rules to ensure transparency of lobbying and interest representation activities conducted on behalf of third countries (European Commission, 2023). In line with the EU's quest for digital sovereignty and strategic autonomy, these attempts aim to strengthen the EU's position in relation to the regulation, control, and access to digital data and services. As discussed in the previous section, platform regulation, enhanced digital security, and geoeconomic aims are all interrelated in EU frameworks.

At the EU level, a series of proceedings has been opened against TikTok in recent years, as TikTok was accused of breaking the DSA and DMA regulations. In April 2023, TikTok was designated as a *very large online platform* under the DSA. In September 2023, ByteDance received the gatekeeper status under the DMA together with Alphabet, Amazon, Apple, Meta, and Microsoft. In February 2024, the Commission opened formal proceedings against TikTok under the DSA in areas "linked to the protection of minors, advertising transparency, data access for researchers, as well as the risk management of addictive design and harmful content" (European Commission, 2024a). In April 2024, proceedings were opened against TikTok Lite's reward programme in France and Spain, resulting in the withdrawal of TikTok Lite in August 2024 (European Commission, 2024c). In December 2024, TikTok was additionally asked to freeze and preserve data related to upcoming elections in the EU, and later, formal proceedings were subsequently opened regarding breaches of the DSA in the context of the Romanian election and TikTok's responsibility to mitigate risks of foreign interference. These proceedings are still open and remain unresolved at the time of writing. Within a relatively short timeframe, multiple proceedings have been initiated, targeting different concerns, including the protection of minors, consumer protection, and foreign interference with elections. The following sub-section will explore these distinct justifications in more detail.

3.2. Areas of Justification

One of the recurring themes in both public debate and EU policy about TikTok is the protection of minors, along with worries about addiction and mental health. These concerns are closely related to issues surrounding electoral interference as they both involve algorithmic design and control over platforms. However, they are distinct in that mental health concerns explicitly address health effects beyond solely political implications. The TikTok proceeding under the DSA is still ongoing. Nevertheless, the justification for the opening of the investigation by the DSA highlights how different concerns have been mobilised (European Commission, 2024a). The main areas of concern are risk management related to addictive designs, "rabbit holes," protection of minors, privacy and safety of minors, advertising transparency, and data access to researchers. The first three concerns fall predominantly under consumer protection and safeguarding minors. The European Commission (2024a) highlights explicitly "potentially addictive design" and the need to protect minors from harmful content. Furthermore, it emphasises general mental health concerns related

to the general concern about shared content on the platform. The text also explicitly mentions "the service's risk of leading users down 'rabbit holes' of harmful content," which already highlights that harmful content is not only content that is inappropriate to a specific age group but harmful for all users, e.g., dis- and misinformation or other anti-democratic content (European Commission, 2024a).

Mental health concerns are also at the forefront in the proceedings against TikTok Lite, which was accused of being "launched without prior diligent assessment of the risks it entails, in particular those related to the addictive effect of the platforms" (European Commission, 2024b). A quote by Thierry Breton, the former Commissioner for Internal Market of the European Union from 2019 to 2024, puts the EU's preoccupations in a nutshell:

> Endless streams of short and fast-paced videos could be seen as fun, but also expose our children to risks of addiction, anxiety, depression, eating disorders, low attention spans….We suspect TikTok 'Lite' could be as toxic and addictive as cigarettes 'light.' We will spare no effort to protect our children. (European Commission, 2024b)

The quote presents a strong-worded example of the Commission's portrayal as the primary agent protecting vulnerable children, creating a stark image of the EU's struggle against the robust tobacco industry.

This imagery finds a continuation when we look closer at the security concerns raised against TikTok and ByteDance. In 2023, the Commission banned TikTok from its employees' phones, citing cybersecurity concerns stemming from China (Chee, 2023). These security concerns are interlinked with fears of harmful content and disinformation. However, they differ in that the focus is less on TikTok's algorithms and their effects (e.g., addiction) and more on the security impact a Chinese-based company might have. In the justifications about the latest proceedings against TikTok regarding the EU elections and TikTok's negligence regarding risk reduction, familiar themes from the disinformation discourse reappear. Commission President Ursula von der Leyen summarises the concerns as follows:

> We must protect our democracies from any kind of foreign interference…..Following serious indications that foreign actors interfered in the Romanian presidential elections using TikTok, we are now thoroughly investigating whether TikTok violated the Digital Services Act by failing to tackle such risks. It should be crystal clear that in the EU, all online platforms, including TikTok, must be held accountable. (European Commission, 2024d)

Governing digital technology companies thus have the distinct aim of protecting democracy against foreign interference. The EU presents itself as a powerful and determined actor committed to safeguarding its citizens, whether concerning the mental health of minors or ensuring the integrity of democratic elections.

3.3. TikTok's Response

TikTok has responded to the EU's policy interventions unevenly. On some fronts, the company chose compliance. It signed the EU Code of Practice on Disinformation in June 2020 and later published a compliance roadmap. By June 2022, it had also accepted changes to meet EU consumer law requirements (European Commission, 2022). In other instances, TikTok embraced contestation. The company opposed its

designation as a gatekeeper under the DMA (TikTok, 2023). TikTok quickly removed its "Lite" program. Still, the EU believes it did not implement adequate measures in the context of the Romanian election, despite the data freeze and efforts to maintain order. TikTok's defence in the EU mainly relies on market-based arguments, claiming they are neither gatekeepers nor quasi-monopolists. When the app was banned from EU employees' phones, TikTok appealed by citing the importance of politicians and policy-makers to stay in touch with citizens:

> TikTok is enjoyed by 125 million EU citizens and potentially depriving users of access to their representatives is a self-defeating step, especially in our shared fight against misinformation and when this action is being taken on the basis of fears rather than facts. (Chee, 2023)

Thus, TikTok does not engage the EU, at least so far, in a language game of national military security but focuses instead on consumer rights, market freedoms, and the importance of social connection facilitated by the app. Security is only addressed through the topic of foreign interference via disinformation, which is perceived as a *threat* to democracy. The analysis of the different proceedings against TikTok shows how the EU is primarily concerned about foreign interference, which is getting tightly linked to notions of mental health and consumer protection. The regulation of TikTok fits within the broader regulation of all kinds of large platforms, but it is exceptional as it is a Chinese-based platform.

4. The US and TikTok

This section examines the shifting regulatory discourse on TikTok in the US, where the platform has become entangled in the geopolitical rivalry with China over technological dominance. We trace the evolution of state interventions, the justifications attached to them, and TikTok's attempts to respond.

4.1. Frameworks and Regulations

For most of the internet era, the US favoured a "light" normative approach. Platforms and tech companies were expected to regulate themselves. In this context, free speech and market liberalism outweighed state intervention. However, since the Russian interference in the 2016 presidential election, the US regulatory landscape shifted decisively to a more security-oriented approach, focusing particularly on foreign interference, data privacy, and geoeconomic competition (Flew & Gillett, 2021). Since early 2019, TikTok has been subject to multiple regulatory interventions focusing on data privacy violations, national security risks, electoral interference, and public health concerns. The PAFACA is the backbone of the US's attempts to restrict TikTok. The act authorises the executive branch to compel divestiture of any application designated a "foreign adversary-controlled application" (United States Congress, 2024, Section 2). Such a designation applies to applications that have more than one million users and are operated by entities domiciled, headquartered in, or organised under the laws of a country designated as a US foreign adversary (China, Russia, North Korea, or Iran) or by companies with at least 20% ownership by such entities (The White House, 2024). PAFACA thus targets ownership/control of the application and associated data access and dictates a divest-or-ban intervention.

PAFACA is the landing point of a longer federal trajectory. At the federal level, scrutiny of TikTok in the US began in February 2019, when the Federal Trade Commission fined Musical.ly/TikTok $5.7 million for

violating children's privacy under COPPA legislation. In August 2020, President Trump signed Executive Order 13942 and a divestment order aimed at forcing the sale of TikTok's US assets. Both were justified on grounds of national security and the risk of foreign interference (The White House, 2020). This move was quickly challenged. Preliminary injunctions blocked the orders later that year, and in June 2021, President Biden formally revoked them, replacing the measures with a broader directive to review foreign-controlled applications. In December 2022, the Biden administration passed the No TikTok on Government Devices Act (effective February 2023). Over the course of 2023, legislation expanded further, through bills such as the RESTRICT Act and the DATA Act, which were introduced to provide federal authority to limit or ban foreign-owned platforms (and thus circumvent the earlier preliminary injunctions). In April 2024, Congress finally enacted PAFACA, giving ByteDance a deadline in early 2025 to divest TikTok or face a nationwide ban. In January 2025, following his return to office, President Trump signed an executive order delaying enforcement by 75 days to allow negotiations on compliance, including ownership and data-localisation measures. At the time of writing (July 2025), the TikTok ban under PAFACA remains postponed.

4.2. Focus Areas

Central to the US policy discourse is the risk that Chinese authorities might access the data of American users or influence TikTok's systems. Trump's 2020 order warns that TikTok's "data collection threatens to allow the Chinese Communist Party access to Americans' personal and proprietary information" (The White House, 2020). Biden's substitute order reframed the issue at the level of classes of "connected software applications" controlled by foreign adversaries, emphasising unacceptable national-security risk from access to "vast swaths" of personal and business information (The White House, 2020). The two orders differ mainly in how directly they call out TikTok and its supposed links to Chinese authorities. What they share, however, is a focus on the danger that personal data could fall into the hands of a foreign adversary. Put differently, TikTok is cast less as a privacy issue in its own right than as a national security problem. In this framing, questions of data protection are absorbed into broader security imperatives. This is reflected in an official public discourse centred on a martial framing of TikTok. Exemplifying this trend, in a 2023 congressional hearing, House Energy & Commerce Committee Chair McMorris Rodgers bluntly told TikTok's CEO: "TikTok is a weapon by the Chinese Communist Party to spy on you, manipulate what you see and exploit [you] for future generations" (Knight First Amendment Institute at Columbia University, 2024).

Concerns about the risk of the Chinese acquisition of data, and the threat this poses to national security, are bundled together with different types of threats, including disinformation and health issues. Trump's 2020 order further contended that TikTok "may also be used for disinformation campaigns that benefit the Chinese Communist Party," referencing, for example, "TikTok videos [that] spread debunked conspiracy theories about the origins of the 2019 novel Coronavirus" (The White House, 2020). Other authorities have stressed the risk of influence associated with TikTok's Chinese ownership. In November 2022, the FBI director warned about "the possibility that the Chinese government could use [TikTok] to control data collection on millions of users or control the recommendation algorithm, which could be used for influence operations" (Shepardson, 2022). Lawmakers mobilise a diverse set of threats in their arguments against TikTok. Among these, US officials also frequently use public health analogies. These are meant to convey TikTok's perceived harm to society, particularly to children. For example, Rep. Gallagher, the initiator of the PAFACA bill, has called TikTok "digital fentanyl, addicting our kids, and just like actual fentanyl, it ultimately goes back to the Chinese Communist Party" (Hendrix, 2022). Interestingly, this analogy frames the app as addictive as a deadly opioid, and thus a

public health emergency caused by a hostile foreign power, a discourse resonating with the perceived Chinese responsibility for the Covid-19 pandemic. US lawmakers have also equated TikTok to other events related to China, such as a "spy balloon in your phone," and urged addressing the issue as was done with tobacco (Paul & Bhuiyan, 2023). These framings reinforce the bundling of security and health discourses, broadening the scope of digital sovereignty debates beyond geopolitical risk to societal resilience.

Finally, the US regulation of TikTok consistently conveys a focus on geoeconomic objectives by embedding them into a national security discourse. By allowing the restriction of platforms based on their physical location and their designation, the PAFACA's divestment provisions explicitly represent an extension of federal powers over the market. PAFACA highlights risks to the digital economy from undue foreign influence. This situates TikTok regulation within a geoeconomic logic linking market competitiveness and control to national security. Aiming to establish a new ownership structure "through the right deal"—a "sovereign wealth fund" or "a partnership with very wealthy people"—to mitigate national security concerns, Trump's second administration approach to TikTok also directly embraces economic objectives beyond the ban (Sutton & Mui, 2025). Finally, TikTok is also fully ingrained in the geopolitical debate on tariffs, with President Trump indicating his administration's willingness to reduce tariffs on China if Chinese authorities approve the sale of TikTok's US operations (Hoskins, 2025). In its latest reconfiguration, this ownership approach to platform regulation seems to mirror the authoritarian practices it claims to deter.

4.3. TikTok's Response

Against the backdrop of extensive regulatory pressure in the US, TikTok set out a broad compliance strategy intended to counter fears of geopolitical risk. At the centre of this effort was Project Texas, a $1.5 billion plan to localise American user data and cut operational dependencies on ByteDance's infrastructure in China. Under the proposal, all US user data would be stored on Oracle-managed servers located within the country, with access overseen by a newly created subsidiary, TikTok US Data Security. TikTok presented the project as an unprecedented step (Perault & Sacks, 2023). The company argued that the arrangement demonstrated its willingness to adapt to US regulatory expectations while offering safeguards framed in terms of national security. TikTok's efforts were also designed to anticipate and counter the enforcement logic of the PAFACA, which authorises the executive branch to ban or compel divestiture of applications deemed controlled by foreign adversaries. In a viral testimony before Congress, TikTok CEO Shou Zi Chew (2024) insisted that the platform was not "an agent of China or any other country" and repeatedly emphasised the independence of US operations from ByteDance. As soon as the PAFACA was approved, TikTok filed legal challenges, but the US Supreme Court upheld its constitutionality. In January 2025, in anticipation of the PAFACA ban, TikTok had suspended its services in the US, but these were restored as a result of Trump's postponement and ongoing negotiations.

5. Banning TikTok, Securing Sovereignty?

In this section, we compare the EU and US approaches to TikTok. We focus on convergences and differences in frameworks and regulations, as well as their focus areas and broader digital sovereignty frameworks.

Both the EU and the US approach TikTok with the same broad aim: to tighten control over foreign-owned digital platforms and to cast the app as a geopolitical issue. The similarity ends there. The EU targets platform

conduct within a codified legislative regime consistent with its "normative power" tradition of rule-based governance, consumer protection, and market oversight (Broeders et al., 2023). The US targets *ownership/control* through a more ad hoc, security-led, and executive-driven approach. While both approaches have extraterritorial reach, the EU embeds TikTok regulation in a generalised regime covering all very large platforms. In contrast, the US uses TikTok-specific and foreign adversary-targeted instruments that explicitly link regulation to geopolitical competition with China. Within the larger frameworks of platform regulation and transnational data governance, these responses demonstrate two approaches that differ by object—conduct (EU) versus control (US)—and remedy—risk mitigation (EU) versus divestiture/ban (US).

Although they seem to overlap—most clearly on foreign interference, data access, and risks to minors—the EU and US debates are fundamentally disaligned. Each highlights different problems and frames them in distinct ways. In the EU, TikTok is portrayed as a complex, systemic risk. In this framing, foreign interference is positioned alongside algorithmic harms such as addictive design, the spread of disinformation, and the mental health risks these dynamics pose—particularly for minors. Taken together, these concerns illustrate how the EU's digital sovereignty agenda folds public health, democratic integrity, and consumer protection into a single regulatory project. In this light, the EU's remedies emphasise risk assessments, design changes, transparency, and data access for researchers. On the other hand, the US places national security at the core, framing TikTok primarily as a vector for Chinese state influence through potential data access, espionage, and influence operations. Remedies emphasise structural separation (divestiture), prohibition, and device bans. While US discourse also invokes public health analogies, these primarily serve to reinforce the security frame by portraying social harms as the work of a hostile foreign adversary. The geoeconomic dimension is more explicit in the US case, where divestment is presented as both a security remedy and a market policy tool favouring domestic tech firms. In contrast, in the EU, it remains secondary to regulatory compliance.

In both cases, TikTok's responses combine compliance with selective contestation, but the strategic emphasis differs. The EU frames sovereignty as regulatory capacity to shape platform behaviour within a rules-based internal market, integrating security with consumer and democratic protections. The US frames it as the power to exclude or restructure foreign-controlled platforms to preserve national technological supremacy. In practice, both approaches blur the line between security governance and economic protectionism, illustrating that digital sovereignty is simultaneously a defensive and assertive project in platform regulation.

Taken together, the EU and US approaches to TikTok show that digital sovereignty cannot be treated as a single unified project. Instead, it operates as a shifting assemblage of security, economic, and societal objectives, each shaped by specific institutional traditions and geopolitical settings. Both the EU and the US invoke sovereignty claims to legitimise far-reaching interventions in platform regulation. Yet the reasoning behind them diverges. The EU favours a codified, multi-issue framework that reflects a regulatory sovereignty rooted in market and rights protection rationales. Contrarily, the US's executive-led security-centric measures embody a sovereignty grounded in strategic control and techno-nationalism. These differences highlight that digital sovereignty is best understood as a flexible, context-dependent repertoire of governing practices rather than a fixed doctrine. As such, it can accommodate liberal-democratic values even as it adopts interventionist or protectionist measures. At the same time, the US example—particularly its divestment provisions—shows how sovereignty discourses on digital technology can take on more authoritarian characteristics when used to legitimise expropriation or forced ownership

restructuring, practices more commonly associated with the approaches of China and Russia toward platforms (Polyakova & Meserole, 2019). This highlights the need to analyse digital sovereignty not only as a response to external threats such as foreign interference, but as an affirmative framework through which authority and internal scrutiny can be promoted or preserved.

6. Conclusion

This article has examined the regulation of TikTok in the EU and the US to analyse how digital sovereignty is operationalised in the governance of foreign-owned digital platforms. Both cases show how TikTok regulation forms part of broader strategies to (re-)assert some form of authority over digital infrastructures, reflecting an ongoing shift towards further geopoliticisation of transnational data governance. Specifically, both cases demonstrate how liberal democracies increasingly depend on the language and territorial logic of sovereignty to regain control over digital infrastructures. In doing so, they pursue seemingly different but substantively similar approaches that depart from earlier models of regulatory convergence and multistakeholderism. While the US emphasises national security and the EU prioritises broader societal harms, both cases illustrate the institutionalisation of a geopolitical approach to digital governance, combining concerns about foreign interference, market dominance, and security.

Regulating TikTok is thus not an exceptional endeavour but part of a broader shift in platform and data governance. At the same time, in both contexts, sovereignty claims extend beyond standard regulatory tools to include exceptional measures such as forced divestiture or market exclusion—policies more often associated with the approaches of China and Russia. What unites the EU and US approaches is a strategic reterritorialisation of digital governance, where regulating transnational platforms becomes a form of geopolitical intervention. This move fragments the global digital landscape and weakens the shared norms and interoperability on which the internet has long relied. At the core is a structural contradiction: digital infrastructures function across borders, but states continue to press for territorial control. Invoking digital sovereignty captures this contradiction. It demonstrates the concept's flexibility but also shows how easily it can be used to legitimise securitised—and at times authoritarian—forms of data governance. As our analysis indicates, we observe a normalisation of extraordinary measures and the bypassing of established channels for accountability, transparency, and public debate. Future research should examine how these trends affect countries outside the Global North (i.e., how the "Beijing effect" generates normative compliance and contestation). Of equal importance, further research is needed to understand how platforms adapt through compliance, legal contestation, or infrastructural reorganisation in the current tense geopolitical context.

Funding

Publication of this article in open access was made possible through the institutional membership agreement between Utrecht University and Cogitatio Press. Linda Monsees' work has been supported by the European Regional Development Fund project "Foreign Interference in the Context of Geopolitical and Technological Change" (reg. no.: CZ.02.01.01/00/23_025/0008692).

Conflict of Interests

The authors declare no conflict of interests.

References

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Bernot, A., Cooney-O'Donoghue, D., & Mann, M. (2024). Governing Chinese technologies: TikTok, foreign interference, and technological sovereignty. *Internet Policy Review*, *13*(1), 1–27. https://doi.org/10.14763/2024.1.1741

Bösch, M., & Divon, T. (2024). The sound of disinformation: TikTok, computational propaganda, and the invasion of Ukraine. *New Media & Society*, *26*(9), 5081–5106. https://doi.org/10.1177/14614448241251804

Broeders, D. (2021). Private active cyber defense and (international) cyber security—Pushing the line? *Journal of Cybersecurity*, *7*(1), Article tyab010. https://doi.org/10.1093/cybsec/tyab010

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*, *61*(5), 1261–1280. https://doi.org/10.1111/jcms.13462

Casero-Ripollés, A., Tuñón, J., & Bouza-García, L. (2023). The European approach to online disinformation: Geopolitical and regulatory dissonance. *Humanities and Social Sciences Communications*, *10*(1), Article 657. https://doi.org/10.1057/s41599-023-02179-8

Chee, F. Y. (2023, February 28). European Parliament latest EU body to ban TikTok from staff phones. *Reuters*. https://www.reuters.com/technology/european-parliament-ban-tiktok-staff-phones-eu-official-says-2023-02-28

Chew, S. Z. (2024). *Testimony before the US Senate Committee*. United States Congress. https://www.judiciary.senate.gov/imo/media/doc/2024-01-31_-_testimony_-_chew.pdf

Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? *New Media & Society*, *21*(10), 2305–2322. https://doi.org/10.1177/1461444819865984

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), 1–12. https://doi.org/10.1093/cybsec/tyac011

Cristiano, F. (2019). Deterritorializing cyber security and warfare in Palestine: Hackers, sovereignty, and the national cyberspace as normative. *CyberOrient*, *13*(1), 28–42. https://doi.org/10.1002/j.cyo2.20191301.0002

Cristiano, F., & van den Berg, B. (2024). (Eds.). *Hybridity, conflict, and the global politics of cybersecurity*. Bloomsbury Publishing.

Deibert, R. (2015). The geopolitics of cyberspace after Snowden. *Current History*, *114*(768), 9–15. https://doi.org/10.1525/curh.2015.114.768.9

Der Derian, J. (2022). Quantum espionage: A phenomenology of the Snowden affair. *Intelligence and National Security*, *37*(6), 920–936. https://doi.org/10.1080/02684527.2022.2076341

Dowling, M. E. (2021). Democracy under siege: Foreign interference in a digital era. *Australian Journal of International Affairs*, *75*(4), 383–387. https://doi.org/10.1080/10357718.2021.1909534

Erie, M. S., & Streinz, T. (2021). The Beijing effect: China's Digital Silk Road as transnational data governance. *Journal of International Law & Politics*, *54*(1), 1–92.

EU: Foreign interference directive poses risks to freedom of expression. (2024, September 4). *Article 19*. https://www.article19.org/resources/eu-foreign-interference-directive-poses-risks-to-freedom-of-expression

European Commission. (2022, June 1). *EU Consumer protection: TikTok commits to align with EU rules to better protect consumers* https://ec.europa.eu/commission/presscorner/detail/en/ip_22_3823

European Commission. (2023). *Proposal for a Directive of the European Parliament and of the Council establishing harmonised requirements in the internal market on transparency of interest representation carried out on behalf of third countries*. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52023PC0637

European Commission. (2024a, February 19). *Commission opens formal proceedings against TikTok under the Digital Services Act* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_926

European Commission. (2024b, April 22). *Commission opens proceedings against TikTok under the DSA regarding the launch of TikTok Lite in France and Spain, and communicates its intention to suspend the reward programme in the EU* [Press release]. https://ec.europa.eu/commission/presscorner/detail/fen/ip_24_2227

European Commission. (2024c, August 5). TikTok commits to permanently withdraw TikTok Lite Rewards programme from the EU to comply with the Digital Services Act [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_24_4161

European Commission. (2024d, December 17). *Commission opens formal proceedings against TikTok on election risks under the Digital Services Act* [Press release]. https://digital-strategy.ec.europa.eu/en/news/commission-opens-formal-proceedings-against-tiktok-election-risks-under-digital-services-act

Fägersten, B., Lovcalic, U., Regnér, A. L., & Vashishtha, S. (2023). *Controlling critical technology in an age of geoeconomics: Actors, tools and scenarios*. Swedish Institute of International Affairs. https://www.ui.se/globalassets/butiken/ui-report/2023/ui-report-no.1-2023.pdf

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Flew, T., & Gillett, R. (2021). Platform policy: Evaluating different responses to the challenges of platform power. *Journal of Digital Media & Policy*, *12*(2), 231–246. https://doi.org/10.1386/jdmp_00061_1

Flonk, D., Jachtenfuchs, M., & Obendiek, A. (2024). Controlling internet content in the EU: Towards digital sovereignty. *Journal of European Public Policy*, *31*(8), 2316–2342. https://doi.org/10.1080/13501763.2024.2309179

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

Flyverbom, M., Deibert, R., & Matten, D. (2019). The governance of digital technology, big data, and the internet: New roles and responsibilities for business. *Business & Society*, *58*(1), 3–19. https://doi.org/10.1177/0007650317727540

Fridman, O. (2024). *Defining foreign influence and interference*. INSS Special Publication. https://www.inss.org.il/publication/influence-and-interference

Glasze, G., Cattaruzza, A., Douzet, F., Dammann, F., Bertran, M. G., Bômont, C., Braun, M., & Zanin, C. (2023). Contested spatialities of digital sovereignty. *Geopolitics*, *28*(2), 919–958. https://doi.org/10.1080/14650045.2022.2050070

Grandinetti, J., & Bruinsma, J. (2023). The affective algorithms of conspiracy TikTok. *Journal of Broadcasting & Electronic Media*, *67*(3), 274–293. https://doi.org/10.1080/08838151.2022.2140806

Gray, J. E. (2021). The geopolitics of 'platforms': The TikTok challenge. *Internet Policy Review*, *10*(2), 1–26. https://doi.org/10.14763/2021.2.1561

Heldt, A. P. (2022). EU Digital Services Act: The white hope of intermediary regulation. In T. Flew & F. R. Martin (Eds.), *Digital platform regulation: Global perspectives on internet governance* (pp. 69–84). Springer. https://doi.org/10.1007/978-3-030-95220-4_4

Hendrix, J. (2022, December 19). Is TikTok "digital fentanyl?". *TechPolicy Press*. https://www.techpolicy.press/is-tiktok-digital-fentanyl

Hoskins, P. (2025, March 27). China tariffs may be cut to seal TikTok sale, Trump says. *BBC News*. https://www.bbc.com/news/articles/c241ezrpg69o

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

Jia, L., & Liang, F. (2021). The globalization of TikTok: Strategies, governance and geopolitics. *Journal of Digital Media & Policy*, *12*(2), 273–292. https://doi.org/10.1386/jdmp_00062_1

Kelton, M., Sullivan, M., Rogers, Z., Bienvenue, E., & Troath, S. (2022). Virtual sovereignty? Private internet capital, digital platforms and infrastructural power in the United States. *International Affairs*, *98*(6), 1977–1999. https://doi.org/10.1093/ia/iiac226

Knight First Amendment Institute at Columbia University. (2024). *Speech & the Border—Episode five: The free speech costs of banning TikTok*. https://www.knightcolumbia.org/content/speech-the-border-transcriptepisode-five-the-free-speech-costs-of-banning-tiktok

Komaitis, K. (2017). The 'wicked problem'of data localisation. *Journal of Cyber Policy*, *2*(3), 355–365. https://doi.org/10.1080/23738871.2017.1402942

Lambach, D. (2019). The territorialization of cyberspace. *International Studies Review*, *21*(3), 482–509. https://doi.org/10.1093/isr/viz022

Lin, J., & de Kloet, J. (2023). TikTok and the platformisation from China: Geopolitical anxieties, repetitive creativities and future imaginaries. *Media, Culture & Society*, *45*(8), 1525–1533. https://doi.org/10.1177/01634437231209203

Litvinenko, A. (2021). Re-defining borders online: Russia's strategic narrative on internet sovereignty. *Media and Communication*, *9*(4), 5–15. https://doi.org/10.17645/mac.v9i4.4292

Meltzer, J. P. (2015). The internet, cross-border data flows and international trade. *Asia & the Pacific Policy Studies*, *2*(1), 90–102. https://doi.org/10.1002/app5.60

Monsees, L. (2024). The paradox of semiconductors—EU governance between sovereignty and interdependence. *Cambridge Review of International Affairs*, *38*(1), 3–21. https://doi.org/10.1080/09557571.2024.2405915

Monsees, L., & Lambach, D. (2022). Digital sovereignty, geopolitical imaginaries, and the reproduction of European identity. *European Security*, *31*(3), 377–394. https://doi.org/10.1080/09662839.2022.2101883

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

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

Musiani, F. (2022). Infrastructuring digital sovereignty: A research agenda for an infrastructure-based sociology of digital self-determination practices. *Information, Communication & Society*, *25*(6), 785–800. https://doi.org/10.1080/1369118X.2022.2049850

Ördén, H., & Pamment, J. (2022). *What is so foreign about foreign influence operations?* Carnegie Endowment for International Peace. https://carnegieendowment.org/2021/01/26/what-is-so-foreign-about-foreign-influence-operations-pub-83706

Paul, K., & Bhuiyan, J. (2023, March 23). Key takeaways from TikTok hearing in Congress—And the uncertain road ahead. *The Guardian*. https://www.theguardian.com/technology/2023/mar/23/key-takeaways-tiktok-hearing-congress-shou-zi-chew

Pearson, J. S. (2024). Defining digital authoritarianism. *Philosophy & Technology*, *37*(73), 1–19. https://doi.org/10.1007/s13347-024-00754-8

Perault, M., & Sacks, S. (2023, January 26). Project Texas: The details of TikTok's plan to remain operational in the United States. *Lawfare*. https://www.lawfaremedia.org/article/project-texas-the-details-of-tiktok-s-plan-to-remain-operational-in-the-united-states

Pohle, J., & Santaniello, M. (2024). From multistakeholderism to digital sovereignty: Toward a new discursive order in internet governance? *Policy & Internet*, *16*(4), 672–691. https://doi.org/10.1002/poi3.426

Pohle, J., & Thiel, T. (2020). Digital sovereignty. *Internet Policy Review*, *9*(4), 1–19. https://doi.org/10.14763/2020.4.1532

Pohle, J., & Voelsen, D. (2022). Centrality and power. The struggle over the techno-political configuration of the Internet and the global digital order. *Policy & Internet*, *14*(1), 13–27. https://doi.org/10.1002/poi3.296

Pohle, J., Nanni, R., & Santaniello, M. (2025). Unthinking digital sovereignty: A critical reflection on origins, objectives, and practices. *Policy and Internet*, *16*(2), 666–671. https://doi.org/10.1002/poi3.437

Polyakova, A., & Meserole, C. (2019). *Exporting digital authoritarianism: The Russian and Chinese models*. Brookings Institution.

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

Salamatian, L., Gill, P., Ensafi, R., & Gill, H. (2019). The geopolitics behind the routes data travels: A case study of Iran. In *Proceedings of the 2019 ACM Internet Measurement Conference* (pp. 49–62). Association for Computing Machinery. https://doi.org/10.1145/3355369.3355592

Shepardson, D. (2022, November 15). U.S. FBI director says TikTok poses national security concerns. *Reuters*. https://www.reuters.com/business/media-telecom/us-fbi-director-says-tiktok-poses-national-security-concerns-2022-11-15

Su, C., & Tang, W. (2023). Data sovereignty and platform neutrality–A comparative study on TikTok's data policy. *Global Media and China*, *8*(1), 57–71. https://doi.org/10.1177/20594364231154340

Sutton, S., & Mui, C. (2025, February 3). Trump orders creation of sovereign wealth fund, hints it could buy TikTok. *Politico*. https://www.politico.com/news/2025/02/03/trump-sovereign-wealth-fund-tiktok-00202154

ten Oever, N., Perarnaud, C., Kristoff, J., Müller, M., Resing, M., Filasto, A., & Kanich, C. (2024). Sanctions and infrastructural ideologies: Assessing the material shaping of EU digital sovereignty in response to the war in Ukraine. *Policy & Internet*, *16*(4), 692–710. https://doi.org/10.1002/poi3.422

TikTok. (2023, November 16). *Appealing our 'gatekeeper' designation under the Digital Markets Act*. Newsroom TikTok. https://newsroom.tiktok.com/appealing-our-gatekeeper-designation-under-the-digital-markets-act?lang=en-150

The White House. (2020). *Executive order 13942: Addressing the threat posed by TikTok, and taking additional steps to address the national emergency with respect to the information and communications technology and services supply chain*. https://www.presidency.ucsb.edu/documents/executive-order-13942-addressing-the-threat-posed-tiktok-and-taking-additional-steps

The White House. (2024). *Executive order 14117: Preventing access to Americans' bulk sensitive personal data and United States government-related data by countries of concern*. https://www.presidency.ucsb.edu/documents/executive-order-14117-preventing-access-americans-bulk-sensitive-personal-data-and-united

United States Congress. (2024). *Protecting Americans from Foreign Adversary Controlled Applications Act*. https://www.congress.gov/bill/118th-congress/house-bill/7521

Voss, W. G. (2020). Cross-border data flows, the GDPR, and data governance. *Washington International Law Journal*, *29*(3), 485–532. https://digitalcommons.law.uw.edu/wilj/vol29/iss3/7

Woods, A. K. (2018). Litigating data sovereignty. *Yale Law Journal*, *128*(2), 328–406. https://www.yalelawjournal.org/pdf/Woods_i233nhrp.pdf

Zeng, J., & Kaye, D. B. V. (2022). From content moderation to visibility moderation: A case study of platform governance on TikTok. *Policy & Internet*, *14*(1), 79–95. https://doi.org/10.1002/poi3.287

About the Authors

Fabio Cristiano is an assistant professor in conflict studies at Utrecht University. His research explores the intersections of international security and emerging technologies, with a particular focus on cybersecurity and digital sovereignty. He is the editor of *Artificial Intelligence and International Conflict in Cyberspace* (2023) and *Hybridity, Conflict, and the Global Politics of Cybersecurity* (2024).

Linda Monsees is a senior researcher at the Institute of International Relations, Prague. Her research covers topics such as cybersecurity, disinformation, and digital sovereignty. Her work has been published in *International Political Sociology*, *International Affairs*, and *Security Dialogue*, among others.

Politics and Governance
2025 • Volume 13 • Article 10331
https://doi.org/10.17645/pag.10331

cogitatio

ARTICLE

Open Access Journal

EU Data Sovereignty: An Autonomy–Interdependence Governance Gap?

Helena Carrapico [1] and Benjamin Farrand [2]

[1] Social Sciences Department, Northumbria University, UK
[2] Law School, Newcastle University, UK

Correspondence: Helena Carrapico (helena.farrand-carrapico@northumbria.ac.uk)

Submitted: 14 March 2025 **Accepted:** 14 May 2025 **Published:** 16 July 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

The EU has explicitly linked the concept of data sovereignty to its ambitions as an international regulatory agenda-setter in its position as self-described geopolitical union. In particular, the EU has expressed repeatedly its desire to ensure its strategic autonomy, reducing its dependence on third countries and their key industries. The purpose of this article is to explore EU data governance ambitions by highlighting the gap between those autonomy aspirations and the reality of data interdependence on the ground. More specifically, through the framework of the "autonomy-interdependence" governance gap, the article proposes to analyse the clash between the EU's desire to ensure autonomy and the inherently interdependent nature of data flows between states, and its dependence on non-EU data servers. Using the case study of semiconductor supply chains, this article analyses the data dimension of this EU-designated critical technology, and the flows of information relating to the research, design, and fabrication of these chips. Considering the EU's attempts to control data under its Data Act and Data Governance Act, it argues that the EU will have considerable difficulty in operationalising these data sovereignty ambitions, particularly as they relate to ensuring that all data stays within the EU, or within its sphere of regulatory influence.

Keywords

data localisation; data sovereignty; European Union; interdependence; semiconductors; strategic autonomy

1. Introduction

The concept of digital/technological sovereignty has become a central pillar of the EU's technological and industrial policies, reflecting a growing ambition to assert control over critical digital infrastructures, data

flows, and technological standards. As discussed below, the Commission uses the two terms, digital sovereignty and technological sovereignty, interchangeably, and for this reason, we have chosen to frame this as "digital/technological" sovereignty, which encapsulates the broader sovereignty aims of the Commission's policies in technology governance. Against the backdrop of escalating geopolitical tensions, technological rivalries, and vulnerabilities exposed by the Covid-19 pandemic, the EU has increasingly framed digital/technological sovereignty as essential to its economic resilience, security, and global leadership (Carrapico & Farrand, 2020; Farrand et al., 2024). As highlighted in Thierry Breton's statement that "Europe may have lost the battle to create digital champions capable of taking on US and Chinese companies harvesting personal data, but it can win the war of industrial data" (Breton, 2020, as cited in "Europe can win global battle," 2020), the concept of data sovereignty is central to the digital/technological sovereignty agenda, encompassing the control and governance of data generated, processed, and stored within the EU and by its stakeholders. Furthermore, increased autonomy and presence in semiconductor supply chains, are seen by the EU as essential to securing this sovereignty as the essential building blocks of digital technologies (European Commission, 2022a). Data sovereignty is intricately tied to the EU's broader vision of digital autonomy, forming the basis for initiatives that aim to develop a robust European data economy and establish the EU as a global norm-setter in data governance. While these ambitions are reflected in strategic documents such as the European Strategy for Data and the European Chips Act, the challenges in implementing the EU's ambitions expose its dependence on global supply chains and external actors. This article examines the feasibility of the EU's data sovereignty ambitions by exploring the case study of the semiconductor industry—a critical and highly interconnected sector underpinning the digital economy and security. Semiconductor data plays a key role at every stage of the supply chain, from research and design to manufacturing and distribution. However, the industry's complexity and reliance on transnational networks highlight the tension between the EU's aspirations for autonomy and the realities of interdependence, effectively underscored by Monsees (2025).

To explore this tension between expectations and outcomes, the article starts by discussing its proposed analytical framework, the EU's data autonomy-interdependence gap, which enables us to evaluate the EU's data sovereignty initiatives against political, legal, and operational criteria, both internally and externally. As will be explained in Section 2, the theoretical framework takes inspiration from Christopher Hill's capability—expectations gap; where he highlighted that the EU's capabilities (as an international actor) had been promoted to the point where an important gap between its capabilities and expectations had emerged (Hill, 1993), which was starting to impact the EU's practices and outcomes as an international actor. Similarly to Hill, the authors hope to bring a much-needed reality check, in this case, to the field of data governance. The remainder of the article applies the analytical framework to the EU semiconductor data governance case study: Section 3 explores the EU's data governance expectations by focusing on its ambition for this area, and Section 4 contrasts the EU's rhetoric with its implementation by considering whether the outcomes are in line with expectations. In doing so, the article aims to shed light on the EU's role in shaping the future of global data governance and reflects on the broader implications for the EU's digital/technological sovereignty agenda and its wider geopolitical ambitions. Methodologically, the authors make use of thematic analysis of European Commission and European Union Council documents published between 2018 and 2024 to, first, identify trends in EU ambitions and, second, to analyse subsequent governance practices. Overall, the authors propose to contribute to the fast-growing academic literature focusing on the EU as a cybersecurity actor (Christou, 2015; Dunn Cavelty, 2013; Farrand et al., 2024; Obendiek & Seidl, 2023) by exploring the sub-field of data governance. Although it constitutes a key aspect

of cybersecurity, and it has received substantial attention in science and technology studies (see for example Bellanova & Glouftsios, 2022), it remains severely underexplored within the international relations literature.

2. Digital/Technological Sovereignty and the EU: Is There a Gap Between Expectations and Outcomes?

In this section, we outline the EU's digital/technological sovereignty ambitions and how they link to the concept of data sovereignty, before outlining the analytical framework used to explore the autonomy-interdependence gap. The first von der Leyen Commission made digital/technological sovereignty central to its technology-related policies, whether they relate to technical standards, the protection of democracy online, or green energy policies. Despite using the terms "digital" and "technological" sovereignty interchangeably (Bellanova et al., 2022), the Commission identified the key purpose of digital/technological sovereignty as an initiative aimed at ensuring Europe's autonomy by reducing technological dependencies on the rest of the world, reinforcing the EU's ability to define its own rules and values, and asserting those rules and values as the basis for cooperation with those outside of its borders (European Commission, 2020d, p. 3). As such, the study of the EU's digital/technological sovereignty initiatives has become the significant focus of a number of academics working on EU policies, ranging from considerations of industrial policy (Seidl & Schmitz, 2023), cybersecurity (Farrand et al., 2024) and internal market regulation (Heidebrecht, 2024), to discrete policy areas such as artificial intelligence (Calderaro & Blumfelde, 2022) and reflections on normative implications for European governance (Floridi, 2020; Thumfart, 2024). Digital/technological sovereignty is subsequently becoming a core element of EU relations with the external world, as well as an internal motivator for action. The second von der Leyen Commission has established a new mandate around the concept, with the creation of an Executive Vice President for Tech Sovereignty, Security and Democracy. In the mission letter outlining the brief, von der Leyen stated that this sovereignty agenda was central to guaranteeing Europe's global leadership and its security, resilience, and future (von der Leyen, 2024b, p. 6).

A key element of this is "data sovereignty." As with "technological" sovereignty, there are some indications that at least some users of the terms do so interchangeably (see Hummel et al., 2021). Data sovereignty may be distinguished from digital/technological sovereignty insofar as it relates specifically to control over data, whether through data protection law, competition law, or national security law, and thereby can be considered a subcategory of digital/technological sovereignty (Chander & Sun, 2023, p. 7). For the Commission, data infrastructure was identified as a core component of digital/technological sovereignty in the Shaping Europe's Digital Future communication (European Commission, 2020d, p. 3), with data becoming "a key factor of production…we need to build a genuine European single market for data—a European data space based on European rules and values" (European Commission, 2020d, p. 5). However, concern was also raised about the market power of large players referred to as "big tech," based outside of the EU's borders (European Commission, 2020d, p. 5). In this communication, we are able to see both an internal and an external dimension to data sovereignty, combining the desire to build European infrastructure akin to an "internal" industrial policy and to ensure that data outside of the EU's borders is governed by European rules and values, representing an "external" leadership ambition focused on setting global standards (see Farrand et al., 2024). The concept of data sovereignty builds upon the perceived strengths of the EU as a regulatory power, first considered in the context of the protection of *personal* data under the General Data Protection Regulation (GDPR) as representing a "Brussels effect," in which the EU is able to dictate the terms of global standards for data regulation without needing explicit forms of cooperation or coercion (Bradford, 2021).

However, as this article explores, while this may have been arguable in the context of the personal data of EU citizens in the geopolitical context in which the GDPR was enacted, the EU is not necessarily as powerful on the world stage as previously argued, and data sovereignty efforts are instead motivated by a sense of insecurity based on a perception that the EU is at a competitive disadvantage with countries such as the US and China (European Commission, 2020a; see also Farrand & Carrapico, 2022). In this context, there is the potential for the EU's data sovereignty ambitions to be unrealised due to a gap between the EU's desires for autonomy and its ability to reduce external interdependencies.

As mentioned in the Introduction, the article explores the EU data governance's autonomy–interdependence gap by developing an analytical framework that takes inspiration from Hill's capability—expectations gap (Hill, 1993), as well as from previous work carried out on EU cybersecurity policy (Carrapico & Farrand, 2024). By taking this analytical route, the authors are consciously favouring a pre-theoretical and more pragmatic approach, which they hope will be of use for the development of future theoretical development. Hill focuses on both *actorness* and *presence* to understand what kind of international actor the EU is, conceptualising the EU's role through its various activities in the world. Actorness as an international actor entails being delimited from others, autonomous in the sense of making its own laws and decisions, and possessing legal personality, diplomatic agents, and the ability to conduct negotiations with third parties (Hill, 1993). Presence emphasises the EU's "variable and multidimensional presence" in international affairs (Hill, 1993, p. 309), yet where our approach diverges is that Hill argues that presence is used to "get [the author] off the hook of analysing [European Political Cooperation] in terms of sovereignty and supranationalism" (Hill, 1993, p. 309), whereas we instead incorporate the Commission's sovereignty discourse and supranational actions into the analysis in order to demonstrate how it promotes an understanding of the EU's desires of autonomy as a sovereignty actor that has a feasibility gap in terms of the EU's interdependencies in the studied field. Similarly to Hill's work, the article maps the rhetorical ambitions of the EU and contrasts them with the pattern of EU activity that has been observed. More specifically, given the article's focus on the feasibility of the EU's data sovereignty ambitions, the authors propose to identify political, legal, and operational criteria to ascertain whether EU ambitions are shared, enforceable, or implementable, both within the EU and in its relations with third countries (see Table 1). Where the political criteria are concerned, the framework asks, overall, whether the EU ambitions of data autonomy are clearly expressed and shared among EU actors and EU member states, as well as whether there are possible obstacles or incentives to these ambitions. The legal criteria interrogate the existence of legal instruments in this field and whether they are enforceable. Finally, the operational criteria questions the extent to which EU data ambitions are being implemented by private actors and third countries, and whether existing critical infrastructures and data supply chains can support such autonomy ambitions. As discussed in the Introduction, we shall explore this specifically using the case study of data flows for semiconductor research, design, and fabrication.

3. The EU's Autonomy Ambitions in the Area of Data Governance

To assess the autonomy–independence gap in EU data sovereignty, it is necessary to first outline what ambitions the EU has in this field, as they relate to the political, legal, and operational criteria. The political ambitions of the Commission can be found in the European Strategy for Data (European Commission, 2020b), which was published shortly after Shaping Europe's Digital Future. It is worth mentioning that the EU had already demonstrated a desire to develop a common European data space in 2018, but this was

Table 1. EU data sovereignty–autonomy–interdependence gap framework.

	Internal dimension	External dimension
Political criteria	• Is the EU's data sovereignty ambition clearly stated in political documents? Does this ambition align itself with broader EU objectives, such as digital/technological sovereignty? • Are the EU's data sovereignty ambitions shared among EU institutions and EU member states? Are the ambitions supported by a shared understanding of data sovereignty? • What are the political obstacles/incentives among EU institutions and EU member states?	• Is the EU's data sovereignty ambition towards third countries clearly stated in political documents? • Are the EU's data sovereignty ambitions towards third countries shared among EU institutions and EU Member States? • What are the political obstacles/incentives regarding exporting EU data sovereignty norms and standards? • Do existing policies address data sovereignty norms and standards for exporting to third countries? Have those policies been co-created with third countries?
Legal criteria	• Do legal instruments reflect data sovereignty ambitions? • Do legal instruments contain clear and enforceable legal provisions?	• Do legal instruments reflect the EU's data sovereignty ambitions towards third countries? • Do legal instruments contain clear and enforceable legal provisions towards third countries?
Operational criteria	• Are private actors implementing EU ambitions and policies? • Is critical infrastructure able to support EU data sovereignty ambitions? • Are EU data supply chains compatible with EU data sovereignty ambitions? • Are there mechanisms to monitor policy implementation?	• Are third countries adopting EU norms and standards? • Are third countries' critical infrastructure able to support EU data sovereignty ambitions? • Are international data supply chains compatible with EU data sovereignty ambitions? • Are there mechanisms to monitor EU policy implementation in third countries?

framed solely in economic terms, rather than in security or sovereignty terms (European Commission, 2018). By way of comparison, and while the European Strategy for Data is still concerned with economic benefits, security and sovereignty are identified as being central to the EU's survival and are explicitly linked to actions in the fields of personal data protection and cybersecurity, with the EU positioned as vulnerable to the advanced levels of competitiveness of the US "free market" and the Chinese "state surveillance" models of Big Tech development (European Commission, 2020b, p. 3). Therefore, the political ambition in data governance is based explicitly on ensuring EU digital/technological sovereignty in enabling data technologies and infrastructures. There is an element of internal industrial policy through creating infrastructures that allow for the EU's share of the data economy, "data stored, processed and put to valuable use in Europe—at least corresponds to its economic weight, not by *fiat* but by choice" (European Commission, 2020b, p. 4). There is also an element of external norm setting through "building upon the strength of the Single Market's regulatory environment [to shape] global standards and [create] an

environment in which economic and technological development can thrive, in full compliance with EU law" (European Commission, 2020b, p. 23). Furthermore, as former Commissioner Breton made clear, initiatives in the context of ensuring data sovereignty have been focused on industrial data, classified as any non-personal data, and having significant commercial value (European Commission, 2020b, p. 1). Of particular relevance to the semiconductor industry, beyond manufacturing, sales, and other forms of "logistical" data is intellectual property (considered as industrial data), whether in the form of copyright schematics, typographical circuit information, patents, or trade secrets (Farrand, 2025).

As a result of these ambitions, legal responses are strongly based on the logic of "data localisation," in which there is an emphasis on retaining data within a country or region's geographical control (Fratini & Musiani, 2024). Two legislative proposals around this have been central to the EU's ambitions: The first was a Proposal for a Data Governance Act (European Commission, 2020c) and the second was a Proposal for a Data Act (European Commission, 2022c). The Data Governance Act was intended to make data sharing easier in the EU area and it was implemented as Regulation 2022/868. This Regulation facilitates the re-use of public sector data and eases the transfer of data shared between businesses, including where that data is non-personal and protected by confidentiality or intellectual property rights (Article 3 of the Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022, 2022). Data intermediation services, which offer services by which data holders can make the data available for potential data users are able to offer those services under Article 10, and they can be based outside of the Union so long as they agree to abide by EU law and appoint a representative in an EU member state under Article 11. Under Article 12, these services are obliged to ensure that where data may be processed outside of the EU, specify the third-country jurisdiction in which the data use is intended to take place, allowing for opt-outs from this usage (Article 12(n)). Furthermore, all services are obliged to take all required measures to prevent international transfer or governmental access to non-personal data held in the Union, where such transfer or access would create a conflict with Union law under Article 31. The Data Act, adopted as Regulation 2023/2854 goes further; it applies its laws to any products or services made available in the Union regardless of where the service or product supplier is based under Article 1 and it places a specific emphasis on non-access by third countries. Under Article 32, strict limits are placed on data transfer to third countries, or requests to access EU data (including non-personal data) by third countries, with requests only being permitted where they are considered proportionate, legitimate, and compliant with EU law. This has been identified as important in restricting the ability of third countries or actors within them being able to access sensitive industrial data of importance to the EU's economic and security interests (European Commission, 2020b, p. 9). It also seeks to facilitate internal data interoperability as a means of fostering a common European Data Space (Article 33). A key intention behind the Data Act is to provide extra-territorial reach, particularly in light of the dependence upon American and Chinese companies providing cloud-based data-storage servers (Casolari et al., 2023). With this in mind, digital/technological sovereignty may be considered as the underlying rationale for the interpretation and application of the Act (Ryan et al., 2024).

In terms of practical operationalisation of this ambition to create more European services in the context of a European Data Space, and reduce dependency on external suppliers, the Commission proposed some concrete steps. Internally, this is focused on increasing the attractiveness of the EU as somewhere for data to be based. This includes infrastructure investment and support for European cloud services and member state initiatives such as Gaia-X (European Commission, 2020b, pp. 15–17), launching an EU cloud marketplace (European Commission, 2020b, pp. 18–19), as well as promoting the development of Common European

Data Spaces in areas of strategic economic sectors, with manufacturing identified as one of the key areas for providing investment and common governance models (European Commission, 2020b, pp. 21–22). Furthermore, the EU intends that creating these favourable conditions would "attract the storage and processing of data from other countries and regions" (European Commission, 2020b, p. 24), in essence operationalising increased levels of data localisation within EU territory. Where this is not feasible, the EU instead states the ambition of ensuring that any access or use of EU personal or non-personal data is done on the basis of EU rules and values (European Commission, 2020b, p. 23), working through multinational fora so as to "promote the European model around the world" (European Commission, 2020b, p. 24). Along these lines, the EU has concluded a Joint Declaration on a Digital Alliance with Latin America, with data governance, security, and infrastructure forming part of its informal dialogue remit (European Union & Latin America and Caribbean, 2023, p. 2), as well as having concluded an EU–Singapore Digital Trade Agreement in July 2024, which facilitates cross-border transfers of data and an agreement not to unjustifiably enforce data localisation requirements (European Commission, 2024a). However, the effectiveness of these activities is open to question, as will be discussed in the next section, using the case study of semiconductor data supply chains to identify the gaps between promoting autonomy and continued interdependence.

4. The Interdependence Dilemma and Unfeasible Ambitions: The Case Study of Semiconductor Data

This final section of the article considers the EU data governance's autonomy–interdependence gap by exploring the case study of semiconductor data. It does so, firstly, by introducing why this case study is well-placed to challenge the EU's data sovereignty ambitions, and, secondly, by applying the analytical framework presented in Section 2 (see Table 1).

4.1. Semiconductor Data: A Case Study on Complexity and Interconnectedness

The control of industrial data for semiconductor supply chains is a particularly interesting case study, not only given the centrality of microchips in powering almost everything in contemporary society, but also due to their high level of supply chain complexity, specialisation, and interdependence. Semiconductors are materials, such as silicon or germanium, that can conduct electricity and that can be processed to create intricate circuit designs, which we commonly call chips. Chips power all modern electronic devices, ranging from microwaves to calculators, from smartphones to intercontinental ballistic missiles (Orton, 2009). The semiconductor industry is therefore central to the EU's digital/technological sovereignty, given that "there is no digital without chips" (von der Leyen, 2021, p. 4). For the Commission, the EU's digital/technological sovereignty is entirely dependent upon guaranteeing its supply of microchips and the resilience of its semiconductor supply chains (European Commission, 2022a, p. 22). This, in turn, is intended to secure the EU's autonomy and sovereignty in associated technological fields. However, the production of microchips is dependent upon industrial research data, which may be protected as trade secrets or as intellectual property rights (Hoeren, 2016). For this reason, the security of this data is critical. As highlighted by Khan et al. (2021), global semiconductor supply chains, which are currently evaluated at half a trillion dollars, are highly dispersed and see individual chips in production crossing an average of 70 international borders, with multiple companies feeding into the process of their production. Whereas considerable semiconductor research takes place in the US and the EU, the raw materials that are used to produce EU semiconductors (silicon, gallium, and germanium) mainly stem from China, Russia, Japan, and Germany,

where they are refined and cleaned of impurities. The raw materials are then transformed into wafers, which serve as the base for semiconductors, in facilities mainly located in South-East Asia, in particular South Korea, Taiwan, and Malaysia, as well as the US and China. The wafers are then used to design integrated circuits, whose market is led by American, Japanese, and Chinese companies ("Semiconductor manufacturing facilities," 2024). The production of the manufacturing equipment is also a particularly important element of the supply chain, with the EU, the US, and Japan being responsible for most of the manufacturing equipment. The wafers containing the designed circuits are then cut into individual microchips, assembled, and packaged into different final technological products. This phase of the supply chain mainly takes place in Taiwan, South Korea, the US, Germany, The Netherlands, France, and Ireland (Council of the European Union, 2022). For the EU, this sector has been valued at €52.1 billion (European Semiconductor Industry Association, 2022). The EU has large firms involved in the research and design of microchips and controls over IP, such as Extoll (Germany) and Menta (France), as well as being a key provider of tools such as lithography devices for production through ASML (based in the Netherlands). However, this data and these tools are then exported to third countries, such as TSMC in Taiwan and Samsung in South Korea. It has integrated device manufacturers (that design and manufacture their own semiconductor chips for use in their own devices) but these are almost exclusively limited to the automobile industry (European Semiconductor Industry Association, 2022).

The data dimension of the semiconductor supply chain mirrors its manufacturing complexity, involving numerous types of data (Ji et al., 2023; TSMC, n.d.), such as (a) research data (produced in universities, businesses, and governmental centres); (b) the proprietary data concerning the design and architecture of the chip; (c) material and equipment data integration (the quality of raw materials, delivery schedules, and equipment performance); (d) manufacturing and production data (photolithography, etching and wafer testing, as well as data analytics on the optimisation of the production process); (e) quality control and testing data (chip defects and their origin); (f) logistics and distribution data (inventory levels, shipping routes, and delivery times); and (g) customer feedback and performance monitoring data (product performance and usage). This type of supply chain generates enormous datasets, which feed into different elements of the manufacturing of semiconductors and evolve throughout the lifespan of the supply chain. This data then requires the necessary infrastructure to be stored safely, processed, and analysed (Mönch et al., 2018).

Looking at the semiconductor supply chain as a whole, three immediate challenges emerge regarding EU data sovereignty: (a) the development of EU infrastructures that are safe and able to store, process, and analyse this volume of data; (b) the difficulty in determining the data owner given the transborder complexity of the supply chain and the cumulative nature of semiconductor data; and (c) the dependence on non-EU data and data infrastructures, which is linked to the absence of the EU from large parts of the supply chain. These challenges highlight the interconnected and transnational nature of semi-conductor data and question whether the EU's ambitions of data autonomy are at all realisable. The following sub-section of the article reflects on these questions by applying the autonomy–interdependence gap framework discussed in Section 2 (see Table 1).

4.2. The Internal and External Dimensions of the Autonomy–Interdependence Gap

As mentioned in Section 2, the article's framework foresees the application of three criteria (political, legal, and operational) to the EU's internal and external dimensions of data sovereignty governance, as understood specifically through the lenses of EU semiconductor data (see Table 2).

Where the challenges in the context of the internal dimension are concerned, there is an indication that the data sovereignty ambition is clearly stated in a considerable range of EU political documents. From the European Strategy for Data (European Commission, 2020b) to the Digital Compass 2030 (European Commission, 2021) and the European Data Act (Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023, 2023), the EU presents a united front on the centrality of data in driving economic innovation and security, and on the need to regulate how ever-growing quantities of data are stored, processed, and utilised in line with EU priorities. The European Chips Act reflects this same level of prioritisation for semiconductor data, which it presents as being central to achieving digital/technological sovereignty (European Commission, 2022b). Semiconductor data is understood as having a key role in the research, design, and manufacturing of technology, as well as in identifying vulnerabilities in supply chains and fostering trust among stakeholders. It is also perceived as being instrumental in enhancing the EU's ability to bridge the gap between advanced semiconductor research and sustainable industrial application while reducing dependence on third countries and contributing to achieving the EU's aim to double its global semiconductor production share from 10% to 20% by 2030. The Council and the Parliament share this enthusiastic support for semiconductor data, as can be seen from the Member States' Declaration on Processors and Semiconductor Technologies (European Commission, 2020e), as well as from the Council and the Parliament's limited changes to and absence of resistance to the Commission's proposal for the EU Chips Act (Kleinhans, 2024).

From a legal perspective, the European Chips Act introduces the necessary provisions to align semiconductor data governance with broader data sovereignty ambitions (as expressed in the Data Act and Data Governance Act). The regulation establishes mechanisms to monitor and secure semiconductor data flows and imposes obligations on stakeholders to ensure data security and interoperability. It also seeks to ensure full protection of confidential information and intellectual property rights under Article 33. Combined with the Data Act and Data Governance Act, this framework provides for a well-defined set of provisions intended to ensure data sovereignty, with recital 43 of the Chips Act making clear the concerns regarding data accessed from outside the Union and the need to reduce dependencies on external states and sectors. However, the enforceability of these provisions is open to question. In fact, a number of member states are currently subject to Commission proceedings for not complying with the Data Governance Act's requirement to provide an oversight body (European Commission, 2024b). Furthermore, as will be discussed below, with regard to operationalisation, the complexity of semiconductor supply chains makes full oversight of data flows exceptionally difficult to achieve. The EU has recently funded a Common European Data Space for manufacturing (Data Space 4.0), which has as a semiconductor research and design project (Chips Joint Undertaking) aiming at securing sovereignty in this field (Chips JU, n.d.). Another initiative is the European Processor Initiative, which has financed the French company SiPearl to design microprocessors for high-performance computing. However, SiPearl only engages in research and design, as manufacturing takes place in Taiwan (SiPearl, 2023), presumably necessitating data outflows.

Regarding the operationalisation of EU data governance, and despite the apparent political alignment, questions remain about whether the EU's ambitions for semiconductor data sovereignty are shared uniformly among member states and institutions. While member states largely support the idea of reducing dependence on third-country suppliers, divergences have emerged over implementation strategies, particularly concerning resource allocation and the role of state aid (Poitiers & Weil, 2024). For example, member states with strong semiconductor industries, such as Germany, France, and the Netherlands, have

advocated for aggressive investments in research and development, while others, with fewer capabilities, have expressed concerns about the equitable distribution of EU funds (Haeck, 2022). Furthermore, there has been additional disagreement as to where the €43 billion necessary to deliver on the EU's ambition to transform the semiconductor landscape will come from. In this context, the Council of the European Union voted unanimously in 2022 to prevent the Commission from using Horizon Europe's leftover funds to support the Chips for Europe Initiative—which was created by the European Chips Act (Tani & Zubascu, 2022). This financial uncertainty has also been made worse by the private sector's cautious approach to investing in the EU semiconductor industry, despite the Commission's announcement that EU funding would be accompanied by large-scale private investment. In 2024, for example, Intel decided to shelve and delay a number of important investments, including a €30 billion semiconductor factory in Germany and a €5 billion production facility in Poland (Haeck, 2024). These divergences point to a potential misalignment in operationalising the shared vision of data sovereignty.

Additional operational challenges further exacerbate the autonomy–interdependence gap. While initiatives such as the EU Chips Joint Undertaking and European Data Spaces, including the project Gaia-X, aim to enhance the EU's semiconductor and data infrastructure, progress has been uneven. The lack of pan-European coherence in infrastructure development has led to fragmentation, with member states prioritising national projects over collective efforts. Moreover, while EU-based semiconductor firms, like ASML and STMicroelectronics, play a significant role in specific segments of the supply chain, their global operations often depend on non-EU partners for critical components, raw materials, and advanced manufacturing equipment. Similarly, the EU continues to be over-reliant on non-EU companies' investment in order to increase its semiconductor production capacity. It is the case, for example, of the creation, in 2024, of the European Semiconductor Manufacturing Company (ESMC), a joint venture between the Taiwan Semiconductor Manufacturing Company and three EU companies (Bosh, Infineon, and NXP). ESMC is currently in the process of building a semiconductor production facility in Dresden, which will be 70% owned by the Taiwanese company (Iskyan, 2024). These different forms of interdependence may enable the expansion of semiconductor production, but they also complicate efforts to achieve true data autonomy, as a significant portion of semiconductor data may be generated, processed, or stored outside EU jurisdiction.

Regarding the external dimension, the EU's ambition to export its regulatory approach also encounters significant geopolitical challenges. While the EU Chips Act and the broader European Strategy for Data emphasise the importance of establishing global norms, the EU faces competition from the US and China, which pursue their own regulatory and industrial strategies. The US CHIPS and Science Act, for instance, offer substantial subsidies to domestic semiconductor firms, creating competitive pressure for EU companies that rely on transatlantic partnerships. In addition, the US has, since the start of 2025, been pursuing a more aggressive semiconductor strategy: the Biden administration made the decision to limit the export of artificial intelligence semiconductors on security grounds, affecting 17 member states (Haeck, 2025); and the Trump administration has actively encouraged semiconductor companies to relocate their production facilities to American territory through the threat of increased tariffs (Mariani, 2025). Similarly, China's state-driven semiconductor strategy prioritises self-sufficiency, making it less receptive to adopting EU standards. China has its own "cyber sovereignty" ambitions (Jiang, 2010; Shen, 2016) that are heavily based on controlling data outflows, as well as exporting its own approach to data governance through its agreements and infrastructure support for other states through initiatives such as the Digital Silk Road (Hussain et al., 2024). Furthermore, in the face of increasing trade hostility from the US, China is seeking to

develop its own advanced chip production capacities, facilitated through significant investments at home and increased cooperation in East Asia (Kim & Rho, 2024). Additionally, while the EU has engaged in bilateral and multilateral initiatives to promote its data sovereignty norms, these efforts have had mixed results. Agreements such as the EU–Singapore Digital Trade Agreement demonstrate a willingness among third countries to align with EU principles, but the absence of similar agreements with major players like the US and China, each seeking to support its own ambitions in this sector, limits the EU's influence in shaping global semiconductor data governance. Finally, the fragmented nature of global supply chains makes it difficult for the EU to monitor compliance with its rules once semiconductor data leaves its jurisdiction.

Table 2. EU data sovereignty–autonomy–interdependence gap applied to the EU semiconductor case study.

	Internal dimension	External dimension
Political criteria	• The EU's semiconductor data sovereignty ambitions are clearly stated in political documents and this ambition aligns itself with broader EU objectives • EU's semiconductor data ambitions are shared among EU institutions and EU member states. Understanding of data sovereignty is, however, vague and often used interchangeably with digital/technological sovereignty • No political obstacles have been identified	• The EU's semiconductor data sovereignty ambition towards third countries is clearly stated in political documents • The EU's semiconductor data sovereignty ambitions towards third countries are shared among EU institutions and EU member states; • No political obstacles have been identified
Legal criteria	• Legal instruments set out obligations for the protection of industrial data • While provisions appear clear, questionable ability to enforce	• Legal obligations codify approach to data sovereignty vis-à-vis third countries • Enforcement dependent upon internal dimension, extraterritoriality of regulation difficult to achieve
Operational criteria	• Operationalisation reveals divergence among member states regarding resource allocation • Disagreement between member states and Commission as to the source of the funding for this area • The private sector has adopted a cautious approach and investment has been limited	• The EU has a limited number of agreements with third countries covering semiconductor data. There is therefore a limited number of countries adopting EU norms and standards • EU's influence in shaping global semiconductor data governance is quite limited • The fragmented nature of global supply chains makes it difficult for the EU to monitor third-country compliance

5. Conclusion

The article proposed examining the EU's ambitions for data sovereignty through the lens of semiconductor data, using the autonomy–interdependence gap framework in order to assess whether the EU's political, legal, and operational initiatives match up with its ambitions. It argued that while the EU has established a clear vision for data sovereignty, buttressed by strategic policies and regulatory tools, such as the European

Data Act and the European Chips Act, it is faced with considerable challenges in operationalising its ambitions. While the EU seeks to ensure autonomy, its ability to do so is hindered by the extent of interdependence in semiconductor production. Internally, inconsistencies among member states in terms of funding, investment in infrastructure, and industrial strategy have cast uncertainty over the EU's capacity to muster a coherent and unified approach to this field. Externally, the highly transnational and interdependent nature of semiconductor supply chains has exposed the EU's continued dependence on third countries for raw materials, technology, and investment. Further, the EU's leverage over global data governance norms is limited in the face of alternative regulatory visions from the US and China. Overall, this case study identifies the broader complexities in the EU digital/technological sovereignty agenda. While the EU hopes to become a regulatory leader, its global influence in semiconductor data governance is subject to it being able to negotiate geopolitical competition, secure critical supply chains, and balance its autonomy ambitions with the realities of interdependence. At a greater level of generality, the control of data relevant to semiconductor development is reflective of a broader potential autonomy–interdependence gap in the pursuit of the EU's data sovereignty goals. The feasibility of increasing data localisation and reducing dependency on third-country services is questionable given the high levels of interdependence in industrial data flows, particularly where research, design, production, and distribution, are all steps in supply chain processes that take place in different states. The Commission has not yet produced its new Union Data Strategy, announced in the context of the von der Leyen II political guidelines (von der Leyen, 2024a), yet we argue that greater recognition of the complexities that interdependence creates in the pursuit of autonomy should be explicitly addressed. In terms of future research, we consider that expanding the analysis to different sectors in which data interdependence, or other forms of interdependence, is a predominant characteristic would help to further reinforce the findings regarding the autonomy–interdependence gap in the EU's pursuit of its digital/technological sovereignty ambitions.

Acknowledgments

We would like to thank the academic editors, Dr Xuechen Chen and Dr Xinchuchu Gao, for their efforts in organising this thematic issue, and for their helpful comments during the drafting stages. We would also like to thank all the participants in the thematic issue workshop, which took place in January 2025, for all their comments and questions.

Funding IM

Publication of this article in open access was made possible through the institutional membership agreement between the Northumbria University and Cogitatio Press.

Conflict of Interests

The authors declare no conflict of interests.

References

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Bellanova, R., & Glouftsios, G. (2022). Formatting European security integration through database interoperability. *European Security*, *31*(3), 454–474. https://doi.org/10.1080/09662839.2022.2101886

Bradford, A. (2021). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Calderaro, A., & Blumfelde, S. (2022). Artificial intelligence and EU security: The false promise of digital sovereignty. *European Security*, *31*(3), 415–434. https://doi.org/10.1080/09662839.2022.2101885

Carrapico, H., & Farrand, B. (2020). Discursive continuity and change in the time of Covid-19: The case of EU cybersecurity policy. *Journal of European Integration*, *42*(8), 1111–1126. https://doi.org/10.1080/07036337.2020.1853122

Carrapico, H., & Farrand, B. (2024). Cybersecurity trends in the European Union: Regulatory mercantilism and the digitalisation of geopolitics. *JCMS: Journal of Common Market Studies*, *62*(S1), 147–158. https://doi.org/10.1111/jcms.13654

Casolari, F., Buttaboni, C., & Floridi, L. (2023). The EU Data Act in context: A legal assessment. *International Journal of Law and Information Technology*, *31*(4), 399–412. https://doi.org/10.1093/ijlit/eaae005

Chander, A., & Sun, H. (2023). Introduction: Sovereignty 2.0. In A. Chander & H. Sun (Eds.), *Data sovereignty: From the digital silk road to the return of the state* (pp. 1–31). Oxford University Press. https://doi.org/10.1093/oso/9780197582794.003.0001

Chips JU. (n.d.). *Our vision*. https://www.chips-ju.europa.eu/Our-vision

Christou, G. (2015). *Cybersecurity in the European Union: Resilience and adaptability in governance policy*. Palgrave Macmillan.

Council of the European Union. (2022). *The semiconductor ecosystem—Global features and Europe's position*. https://www.consilium.europa.eu/media/58112/220712-the-semiconductor-ecosystem-global-features-and-europe-s-position.pdf

Dunn Cavelty, M. (2013). *A resilient Europe for an open, safe and secure cyberspace* (Working paper No. 23). Swedish Institute of International Affairs.

Europe can win global battle for industrial data, Breton says. (2020, February 17). *Euractiv*. https://www.euractiv.com/section/digital/news/europe-can-win-global-battle-for-industrial-data-breton-says

European Commission. (2018). *Towards a common European data space* (No. COM(2018) 232). https://digital-strategy.ec.europa.eu/en/news/communication-towards-common-european-data-space

European Commission. (2020a). *2020 strategic foresight report: Charting the course towards a more resilient Europe* (No. COM(2020) 493). https://commission.europa.eu/strategy-and-policy/strategic-foresight/2020-strategic-foresight-report_en

European Commission. (2020b). *A European strategy for data* (No. COM(2020) 66). https://digital-strategy.ec.europa.eu/en/policies/strategy-data

European Commission. (2020c). *Proposal for a regulation on European data governance* (No. COM(2020) 767). https://digital-strategy.ec.europa.eu/en/policies/data-governance-act

European Commission. (2020d). *Shaping Europe's digital future*. https://digital-strategy.ec.europa.eu/en

European Commission. (2020e). *Joint declaration on processors and semiconductor technologies*. https://digital-strategy.ec.europa.eu/en/library/joint-declaration-processors-and-semiconductor-technologies

European Commission. (2021). *2030 digital compass: The European way for the digital decade* (No. COM(2021) 118 final/2). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118

European Commission. (2022a). *A Chips Act for Europe* (No. COM(2022) 45). https://commission.europa.eu/strategy-and-policy/priorities-2019-2024/europe-fit-digital-age/european-chips-act_en

European Commission. (2022b). *Proposal for a regulation establishing a framework of measures for strengthening Europe's semiconductor ecosystem (Chips Act)* (No. COM(2022) 46). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0046

European Commission. (2022c). *Proposal for a regulation on harmonised rules on fair access to and use of data (Data Act)* (No. COM(2022) 68). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022PC0068

European Commission. (2024a). *Agreement on digital trade between the European Union and the Republic*

of Singapore—Working text. https://www.bilaterals.org/IMG/pdf/eu-singapore_text_of_the_digital_trade_agreement.pdf

European Commission. (2024b, December 16). *Commission calls on 10 Member States to comply with the Data Governance Act | Shaping Europe's digital future* [Press release]. https://digital-strategy.ec.europa.eu/en/news/commission-calls-10-member-states-comply-data-governance-act

European Semiconductor Industry Association. (2022). *Welcome to ESIA*. https://www.eusemiconductors.eu/esia

European Union & Latin America and Caribbean. (2023). *Joint declaration on a digital alliance*. https://international-partnerships.ec.europa.eu/document/download/15512057-a80d-4428-bf34-24608adfb0e4_en?filename=EU-Latin_America_and_Caribbean__Joint_Declaration_on_a_Digital_Alliance.pdf

Farrand, B. (2025). The economy–security nexus: Risk, strategic autonomy and the regulation of the semiconductor supply chain. *European Journal of Risk Regulation*, *16*(1), 279–293. https://doi.org/10.1017/err.2024.63

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453. https://doi.org/10.1080/09662839.2022.2102896

Farrand, B., Carrapico, H., & Turobov, A. (2024). The new geopolitics of EU cybersecurity: Security, economy and sovereignty. *International Affairs*, *100*(6), 1–24.

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

Fratini, S., & Musiani, F. (2024). Data localization as contested and narrated security in the age of digital sovereignty: The case of Switzerland. *Information, Communication & Society*. Advance online publication. https://doi.org/10.1080/1369118X.2024.2362302

Haeck, P. (2022, November 15). In the global chips race, EU's cash engine sputters. *Politico*. https://www.politico.eu/article/budget-squabbles-put-eu-on-the-back-foot-in-the-chips-race

Haeck, P. (2024, September 17). The EU's chips plan implodes as Intel pauses investments. *Politico*. https://www.politico.eu/article/intel-germany-chips-plant-competitiveness-eu-ambition

Haeck, P. (2025, January 14). US limits on AI chips split EU. *Politico*. https://www.politico.eu/article/eu-warns-back-against-us-artificial-intelligence-chip-export-china-limits

Heidebrecht, S. (2024). From market liberalism to public intervention: Digital sovereignty and changing European Union digital single market governance. *JCMS: Journal of Common Market Studies*, *62*(1), 205–223. https://doi.org/10.1111/jcms.13488

Hill, C. (1993). The capability-expectations gap, or conceptualizing Europe's international role. *Journal of Common Market Studies*, *31*(3), 305–328.

Hoeren, T. (2016). The semiconductor chip industry—The history, present and future of its IP law framework. *International Review of Intellectual Property and Competition Law*, *47*(7), 763–796.

Hummel, P., Braun, M., Tretter, M., & Dabrock, P. (2021). Data sovereignty: A review. *Big Data & Society*, *8*(1), 1–17. https://doi.org/10.1177/2053951720982012

Hussain, F., Hussain, Z., Khan, M. I., & Imran, A. (2024). The digital rise and its economic implications for China through the digital Silk Road under the Belt and Road initiative. *Asian Journal of Comparative Politics*, *9*(2), 238–253. https://doi.org/10.1177/20578911231174731

Iskyan, K. (2024, September 3). TSMC starts building its first European chip plant. *Global Finance Magazine*. https://gfmag.com/technology/tsmc-chip-plant-germany

Ji, K., Nauta, L., & Powell, J. (2023). *Mapping global supply chains—The case of semiconductors*. Rabobank.

https://www.rabobank.com/knowledge/d011371771-mapping-global-supply-chains-the-case-of-semiconductors

Jiang, M. (2010). Authoritarian informationalism: China's approach to internet sovereignty. *SAIS Review of International Affairs*, *30*(2), 71–89.

Khan, S. M., Mann, A., & Peterson, D. (2021). *The semiconductor supply chain: Assessing national competitiveness*. Center for Security and Emerging Technology. https://doi.org/10.51593/20190016

Kim, Y., & Rho, S. (2024). The US–China chip war, economy–security nexus, and Asia. *Journal of Chinese Political Science*, *29*(3), 433–460. https://doi.org/10.1007/s11366-024-09881-7

Kleinhans, J.-P. (2024, July 30). *The missing strategy in Europe's chip ambitions*. Interface. https://www.interface-eu.org/publications/europe-semiconductor-strategy

Mariani, M. (2025). *Trump's proposed tariffs on semiconductors*. Z2Data. https://www.z2data.com/insights/impact-report-trumps-proposed-tariffs-on-semiconductors

Mönch, L., Uzsoy, R., & Fowler, J. W. (2018). A survey of semiconductor supply chain models part I: Semiconductor supply chains, strategic network design, and supply chain simulation. *International Journal of Production Research*, *56*(13), 4524–4545. https://doi.org/10.1080/00207543.2017.1401233

Monsees, L. (2025). The paradox of semiconductors—EU governance between sovereignty and interdependence. *Cambridge Review of International Affairs*, *38*(1), 3–21. https://doi.org/10.1080/09557571.2024.2405915

Obendiek, A. S., & Seidl, T. (2023). The (false) promise of solutionism: Ideational business power and the construction of epistemic authority in digital security governance. *Journal of European Public Policy*, *30*(7), 1305–1329. https://doi.org/10.1080/13501763.2023.2172060

Orton, J. W. (2009). *Semiconductors and the information revolution: Magic crystals that made IT happen*. Academic Press.

Poitiers, N., & Weil, P. (2024, November 12). *Is the EU Chips Act the right approach?* Bruegel. https://www.bruegel.org/blog-post/eu-chips-act-right-approach

Regulation (EU) 2022/868 of the European Parliament and of the Council of 30 May 2022 on European data governance and amending Regulation (EU) 2018/1724 (Data Governance Act). (2022). *Official Journal of the European Union*, L 152/1. https://eur-lex.europa.eu/eli/reg/2022/868/oj/eng

Regulation (EU) 2023/2854 of the European Parliament and of the Council of 13 December 2023 on harmonised rules on fair access to and use of data and amending Regulation (EU) 2017/2394 and Directive (EU) 2020/1828 (Data Act). (2023). *Official Journal of the European Union*, L 2023/2854. http://data.europa.eu/eli/reg/2023/2854/oj/eng

Ryan, M., Gürtler, P., & Bogucki, A. (2024). Will the real data sovereign please stand up? An EU policy response to sovereignty in data spaces. *International Journal of Law and Information Technology*, *32*(1), Article eaae006. https://doi.org/10.1093/ijlit/eaae006

Seidl, T., & Schmitz, L. (2023). Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy. *Journal of European Public Policy*, *31*(8), 2147–2714.

Semiconductor manufacturing facilities map. (2024, May 27). *Technology in Global Affairs*. https://technologyglobal.substack.com/p/semiconductor-manufacturing-facilities

Shen, Y. (2016). Cyber sovereignty and the governance of global cyberspace. *Chinese Political Science Review*, *1*(1), 81–93. https://doi.org/10.1007/s41111-016-0002-6

SiPearl. (2023). *SiPearl*. https://sipearl.com/european-processor

Sjostedt, G. (1977). *External role of the European Community*. Lexington Books.

Tani, C., & Zubascu, F. (2022, December 1). EU ministers stop €400M of decommitted Horizon Europe money

being diverted to the Chips Act. *Science|Business*. https://sciencebusiness.net/news/eu-ministers-stop-eu400m-decommitted-horizon-europe-money-being-diverted-chips-act

Thumfart, J. (2024). *The liberal internet in the postliberal era: Digital sovereignty, private government, and practices of neutralization*. Palgrave Macmillan.

TSMC. (n.d.). *A look at semiconductor supply chains—Taiwan semiconductor manufacturing company limited*. https://www.tsmc.com/english/aboutTSMC/dc_infographics_supplychain

von der Leyen, U. (2021). *2021 state of the Union address by President von der Leyen: Strengthening the soul of our Union* (No. SPEECH/21/4701). European Commission. https://ec.europa.eu/commission/presscorner/detail/ov/SPEECH_21_4701

von der Leyen, U. (2024a). *Europe's choice: Political guidelines for the next European Commission*. https://commission.europa.eu/document/download/e6cd4328-673c-4e7a-8683-f63ffb2cf648_en?filename=Political%20Guidelines%202024-2029_EN.pdf

von der Leyen, U. (2024b). *Mission letter to Henna Virkkunen, Executive Vice-President-designate for tech sovereignty, security and democracy*. European Commission. https://commission.europa.eu/document/download/3b537594-9264-4249-a912-5b102b7b49a3_en?filename=Mission%20letter%20-%20VIRKKUNEN.pdf

About the Authors

Helena Carrapico is a professor of international relations and European politics at Northumbria University. Her research is centrally concerned with addressing how internal security concerns, including cybersecurity, are constructed, represented, and responded to by different actors, as well as how those responses impact society at large. She hopes that one day her love of watching science fiction and her love of research may be unified.

Benjamin Farrand is a professor of law and emerging technologies at the Newcastle University Law School. His research focuses on the interactions between law and politics in the regulation and governance of new technologies, including in fields such as cybersecurity and online platforms. It also focuses on the interactions between academic scholarship and caffeine intake, which requires continuous experimentation.

Politics and Governance
2025 • Volume 13 • Article 10474
https://doi.org/10.17645/pag.10474

cogitatio

ARTICLE

Open Access Journal

Digital Policy as a Driver of Integration: Spillover Effects and European Commission Empowerment

Sebastian Heidebrecht

Department of Political Science, University of Vienna, Austria

Correspondence: Sebastian Heidebrecht (sebastian.heidebrecht@univie.ac.at)

Submitted: 3 April 2025 **Accepted:** 22 July 2025 **Published:** 23 October 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

The Russian invasion of Ukraine and the global impact of the pandemic brought digital technology to the forefront of geopolitical strategy and geo-economic considerations, prompting European policymakers to embrace strategic autonomy and digital sovereignty. While existing scholarship has examined EU rhetorical and policy responses, its institutional dynamics have received less attention. This article addresses this gap by examining the growing political influence of the European Commission in terms of both its breadth (the range of issues it engages with) and depth (its decision-making authority). Using primary and secondary sources together with expert interviews, the study reveals that the EU responded to geopolitical threats in two key policy areas: digital service regulation (Digital Services Act and Digital Markets Act) and allocating digital-related financial resources in the context of the Recovery and Resilience Facility. Based on recent theoretical advances regarding EU geo-politicalisation and its geo-economic shift, the article argues that the increased power of the Commission is a result of neofunctional processes broadening its influence. However, this dynamic is more evident in the context of digital service regulation than in the context of financial resources. By analysing this transformation, the study offers a new perspective on the emergence of a more empowered and geopolitically assertive Commission in the era of transnational data governance.

Keywords

digital policy; internet; European integration; European Commission; neofunctionalism; platform regulation; recovery and resilience facility

1. Introduction

In the 2020s, digital technologies and data are evolving into vital economic assets and strategic resources. Consequently, digital governance has become a pivotal arena of geopolitical contention, transcending its

former status as a mere technical or regulatory matter. As major global powers such as the US and China adopt different data regulatory approaches based on conflicting political, economic, and ideological priorities (Bradford, 2023), strategic rivalry and assertions of national sovereignty are increasingly shaping the global digital landscape. These geopolitical challenges (Xuechen & Gao, in press) have prompted a rethink of liberalisation and market integration, with its adoption of more geopolitical approaches triggering the EU "geo-economic turn" (Herranz-Surrallés et al., 2024; McNamara, 2024). While many scholars have investigated policy areas related to digitalisation that have changed in the context of more assertive rhetoric (Lambach & Oppermann, 2022; Pohle & Thiel, 2020), this article demonstrates a development that has often been overlooked. Alongside Commission efforts to make "Europe fit for the digital age" (European Commission, 2020a), institutional and legal changes have resulted in shifts in the EU polity empowering the European Commission. For the first time, the Commission has been granted substantial powers in digital service regulation accompanied by strong fiscal powers to direct digital-related investments.

This article argues that the increased powers of the European Commission—defined as its involvement in a broader range of issues and greater authority in decision-making processes—can be explained as a response to geopolitical tensions and the transnational nature of digital policy (Xuechen & Gao, in press). Taking a neofunctionalist stance, the article posits that the Commission's recent expansion of its core competencies in the digital sphere was prompted not only by geopolitical pressures but also by the intrinsic features of digital policy. As digital policy intersects with multiple sectors, including economic resilience, environmental aims, and security, effective governance often requires integration beyond national borders. The growing engagement by the Commission in areas such as overseeing major online platforms and coordinating funding for the twin transitions exemplifies this trend. Furthermore, the Commission has cultivated a persuasive discourse that portrays digitalisation as both inevitable and desirable while emphasising the need for European-level governance to shape it. This rhetoric has helped to overcome national resistance by presenting integration as a prerequisite for effective policy implementation in an interconnected world rather than as a loss of sovereignty.

The article contributes to two streams of literature. First, it addresses the debate surrounding changes to the EU's institutional framework. Previous studies have demonstrated an increase in the powers of various EU institutions (e.g., Heidebrecht, 2017; Rittberger, 2014; Stone Sweet & Sandholtz, 1997). For example, with a specific focus on the EU Commission, Bauer and Becker (2014) found that its competences had expanded in response to the euro crisis. This article focuses on institutional changes in the EU in relation to developments in the emerging field of digital policy and demonstrates that the characteristics of this field, coupled with changes in the external environment, created momentum towards empowerment of the European Commission. Second, the article contributes to the emerging debate on digital policy changes in the EU. Although the EU initially lacked formal expertise in this area, it has gradually established a legislative framework aimed at regulating the digital sphere. Research in this area has examined shifts in EU rhetoric towards concepts such as digital sovereignty, open strategic autonomy (Lambach & Oppermann, 2022; Pohle & Thiel, 2020; Schmitz & Seidl, 2023) and policy changes aimed at greater digital control (Donnelly et al., 2024; Farrand & Carrapico, 2022). This article demonstrates how and why the EU Commission's stronger role accompanies these policy changes.

In the light of recent events, it is interesting to note that the growing powers of the Commission over digital issues predate the Russian invasion of Ukraine and more complicated relations with the US and China.

Nevertheless, these developments undoubtedly make EU digital policymaking more relevant and raise questions about how the EU adapts its institutional architecture in the digital age. Understanding how the EU responds to external challenges and internal dynamics is essential to grasp how it can assert its powers both internally and externally. Before presenting its findings, the article discusses the development of EU digital policy and geopolitics considering the existing literature, details its theoretical argument, and sets out its empirical strategy. The final section draws conclusions.

2. EU Digital Policy and Institutional Change

Digitalisation has emerged as the central political issue of the 21st century, with Commission President Ursula von der Leyen describing it as a "make-or-break issue" (von der Leyen, 2021) for Europe. The second priority of the von der Leyen Commission for 2019–2024 was to make "Europe fit for the digital age" (European Commission, 2020a). EU digital policy encompasses a wide array of regulatory, industrial, and strategic initiatives aimed at shaping the governance of data, platforms, and emerging technologies (Bonnamy & Perarnaud, 2023). Amid mounting concerns about issues such as disinformation (Howard, 2020), surveillance (Zuboff, 2019), and excessive market power (Khan, 2017), the EU aims to champion its distinctive "human-centric" digital sphere model (European Commission, 2021a). This model envisions a "fundamental-rights-based, inclusive, transparent and open digital environment where secure and interoperable digital technologies and services observe and enhance Union principles, rights and values and are accessible to all, everywhere in the Union" (European Parliament and of the Council of 14 December 2022, 2022, Article 3.1(a)).

The EU approach is often viewed as positioned between the laissez-faire approach adopted by the US and the state-controlled model in China. As major powers pursue divergent and competing approaches to digital technologies and policies (Bradford, 2023), strategic rivalry and national assertions of sovereignty increasingly shape the global digital order. Geopolitical challenges (Xuechen & Gao, in press) have led to a rethinking of liberalisation and market integration. As a response, the EU is found to pursue a "geo-economic turn" (Herranz-Surrallés et al., 2024; McNamara, 2024). Increasingly, this policy area is marked by a pronounced geopolitical dimension, with the EU seeing digital technologies and economies as tools to achieve geopolitical objectives (Broeders et al., 2023). For example, the European Commission mobilises digital regulation and industrial policy tools not only to foster innovation and protect fundamental rights but also to enhance EU strategic autonomy in a global digital order shaped by systemic competition and technological dependencies.

In the context of an increasingly geopolitical world, states are seeking to secure and advance their model of digital governance (Haggart & Keller, 2021), and the EU is grappling with the task of preserving its "digital sovereignty" and the promotion of "open strategic autonomy" (Falkner et al., 2024; Schmitz & Seidl, 2023). In this context, academic studies have analysed the concept of EU digital sovereignty and focused inter alia on its discursive dimensions (Bellanova et al., 2022; Pohle & Thiel, 2020). One finding on the topic is that the concept can also assert European values (Roberts et al., 2021). Another line of research demonstrates that digital sovereignty contributes to more control of the digital sphere and its different layers, like data, software, protocols, infrastructure, and the like (Floridi, 2020). In this context, the promotion of this new EU digital agenda is found to trigger policy changes and a redefined approach to internet governance. Inter alia, geopolitical challenges have necessitated a more dirigiste competition policy on a new "ex-ante" approach

(Cini & Czulno, 2022; Hoeffler & Mérand, 2023) and more pronounced inclusion of cyber security concerns in related areas such as EU foreign policy (Carver, 2023) and regulation of digital finance (Donnelly et al., 2024). In broad terms, the EU is observed to be moving away from its "neoliberal bias" (Laurer & Seidl, 2021) and transitioning from a market-liberal to a more public interventionist approach (Farrand & Carrapico, 2022; Heidebrecht, 2024).

However, despite a growing body of literature on EU digital policy, little is known about how the EU has adapted its institutional framework to meet the demands of the digital age. This article is one of the few publications to trace key institutional changes in digital policymaking and one of the first to shed light on the processes through which the European Commission is empowered. It contributes to the debate on EU digital policy and EU institutional governance by demonstrating how the Commission is empowered in digital policymaking.

3. Explaining the Empowerment of the European Commission

This article explains that the European Commission has become more empowered in digital policy by combining three elements: (a) the geopolitical context of digital interdependence; (b) a conceptual framework for measuring institutional and political change; and (c) insights from neofunctionalist theory, particularly neo-neofunctionalist reformulations. The article builds on neofunctionalist theory by showing how useful it is in explaining the dynamics of integration in cross-sectoral and digitally driven policy areas—something that was not addressed by previous studies.

The outcome is captured using the concept of empowerment, which is understood as institutional change in two dimensions (Börzel, 2005): depth, or vertical transfer of competences from member states to EU institutions; and breadth, or expansion of EU authority into new policy domains. This approach is based on well-established literature examining EU integration during crises (Bickerton et al., 2015; Heldt & Mueller, 2021; Schimmelfennig, 2015).

To explain this change, the article draws on neofunctionalist theory which emphasises the dynamic and incremental process of integration. Unlike liberal intergovernmentalism, which views member states as primary actors with fixed preferences, neofunctionalism emphasises spillover effects, feedback loops, and institutional entrepreneurship (Nicoli, 2020; Niemann & Ioannou, 2015; Schmitter, 2013). While liberal intergovernmentalism is well suited to explaining treaty-level decisions driven by state bargaining, it struggles to account for institutional change without a direct government initiative. Examples of this include the evolving role of the European Central Bank (Heidebrecht, 2025) and the creation of the European Financial Stabilisation Mechanism (Gocaj & Meunier, 2013). Although liberal intergovernmentalism is still effective in explaining grand bargains and intergovernmental negotiations, this article explores the explanatory value of neofunctionalist theory in understanding EU policies and strategies related to the digital sphere. Neofunctionalism is particularly relevant when analysing this area because data and digital infrastructure are inherently transnational, transcending national boundaries and regulatory frameworks. Despite its potential, neofunctionalism has largely been overlooked in this context. This article is among the first to apply it systematically to EU digital policy (for another application of neofunctionalism to EU digital policy, see Mazur & Ramiro Troitiño, 2024). In doing so, the analysis contributes to the assessment of the utility of the theory in this critical and emerging area of EU integration.

Three types of spillover are central in neofunctional analysis. Functional spillover is when integration in one area (e.g., market regulation) creates pressure to integrate in others. Political spillover involves shifting loyalties and expectations regarding EU institutions when national-level solutions are inadequate (Haas, 1958). Cultivated spillover is supranational actors, particularly the Commission, proactively extending their remit through agenda-setting, brokering, and framing (Ioannou et al., 2015).

Neofunctionalist theory also identifies the conditions under which spillover, and therefore potential Commission empowerment, is more likely to occur. First, digital policy is highly interdependent and cross-cutting making it a prime example of functional spillover. Regulatory fragmentation increases the "costs of non-integration" which incentivises EU-level solutions. Second, the Commission already has an established role in governance of the digital single market, making a cultivated spillover—for example, in the form of an extension of existing authority—more likely (Deters & Falkner, 2021; Schmidt, 2000). Third, the geo-political dimension of digitalisation, such as cybersecurity threats and global tech competition, acts as a systemic crisis similar to Schmitter's (1970) "crisis-provoked decisional cycles," in which uncertainty enables EU institutions to expand their authority. Fourth, digital policy has relatively low salience and enjoys a positive public perception, particularly as part of the EU green and digital transitions (Gao, 2025; Nicoli, 2020), thus providing fertile ground for political and cultivated spillover.

This article builds on so-called neo-neofunctionalist reasoning by combining developments in the international environment with internal dynamics in the theoretical argument, specifically the "synergy" perspective. (Brooks et al., 2023). From this perspective, external crises are viewed as forces mediated by existing institutional structures rather than as exogenous shocks that automatically trigger change. Accordingly, empowerment depends not only on external pressures but also internal spillover dynamics and the ability of the Commission to leverage existing competencies in a path-dependent system. A growing geo-economic framing of EU policy (Bradford, 2023; Herranz-Surrallés et al., 2024) and intensified digital rivalry (Xuechen & Gao, in press) provide the context and opportunity for the Commission to empower itself strategically in the digital domain. Table 1 draws on these theoretical strands to summarise the main types of spillover, their enabling conditions, and the corresponding hypotheses regarding Commission empowerment.

Table 1. Theoretical assumptions.

Type of Spillover	Conditions	Assumptions on Empowerment
Functional Spillover	High policy interdependence and fragmentation in cross-border domains (e.g., digital, economic, environmental) increase the cost of national-level action.	Functional pressures trigger a vertical transfer of competences and expansion into adjacent policy areas via supranational solutions.
Political Spillover	National solutions prove inadequate; shared challenges shift preferences toward EU institutions.	Political realignments facilitate the empowerment of the Commission by legitimising a stronger supranational authority and central coordination.
Cultivated Spillover	The Commission has pre-existing competences; affirmative public discourse and institutional entrepreneurship enhance its agenda-setting role.	Strategic framing enables the Commission to actively expand its authority, reinforcing existing powers and creating new roles.

4. Empirical Strategy

To explore the explanatory power of neofunctional processes empowering the European Commission in the area of EU digital policy, this article traces different spillover processes and looks at the effect of a set of four enabling conditions by means of two case studies on (a) disposal of digital-related financial resources and (b) regulation of digital services. The case selection is guided on the one hand by an approach to confirm the article's neofunctional assumptions by conducting a cross-sectional case study research design (Gerring, 2004). On the other hand, the cases are also chosen to illustrate important phenomena under consideration, namely empowerment of the Commission in important digital-related issues, which is of intrinsic academic and political value, and therefore justifies a case study method (Van Evera, 1997, pp. 67–68).

The selection of cases combines a confirmatory logic with a selection based on crucial cases. In particular, digital service regulation in the EU can be considered a most likely case for neofunctional processes to occur, given the transnational character of data and other elements discussed in Section 3. This means it can serve as a most likely case that in the absence of confirmatory evidence allows theoretical assumptions to be disconfirmed (Seawright & Gerring, 2008). Furthermore, expansion of financial resources is crucial, as they have long been governed by a dedicated intergovernmental structure since the euro crisis. Institutions such as the European Stability Mechanism, the rescue fund set up during the euro crisis, are still not integrated into EU law but are based on international law and run by the governments of the euro area member states. Therefore, the establishment of the Next Generation EU instrument (NGEU) has received much scholarly attention (e.g., Schramm et al., 2022). However, the digital dimension of this has not yet been reflected in the literature. The second case, the design and structure of digital service regulation in the EU, has also received some attention (e.g., Farrand, 2023; Heidebrecht, 2024; Hoeffler & Mérand, 2023). However, most contributions have focused on policy changes that have taken place in the digital policy area, while the institutional dimension has received less attention.

This article applies an in-depth confirmatory case study approach. It is built on an extensive analysis of primary and secondary sources including all the legislative EU documents related to the two cases, official EU institution documents relating to the two cases, and also those of member states, like position papers. The article further uses six issue-oriented interviews with persons holding specialised information and who have been involved in or closely followed the EU policymaking process. The interviews are used for "aggregation" (von Soest, 2023), as experts are well-suited to reducing real-world complexity and bundling together multifaceted phenomena. Thus, the interviews focused on the development of the two cases and in a descriptive manner helped to reconstruct important events while also providing additional information. As expert interviews lend themselves to purposeful, non-probability sampling (Goldstein, 2002; Tansey, 2007), the selection of interviewees combined insider and outsider perspectives and higher- and lower-level inside experts (see Table 2 for an overview). Publicly available data, such as media documents and press releases, were used to further triangulate the information obtained.

Table 2. List of interviews.

Interview	Position	Place	Date
Interview 1	Policy advisor, European Parliament	Brussels	28 June 2023
Interview 2	Policy advisor, European Parliament	Brussels	27 June 2023
Interview 3	Policy analyst, DG Connect	Brussels	26 June 2023
Interview 4	Policy advisor, European Parliament	Brussels	26 June 2023
Interview 5	Policy advisor, European Party	Brussels	25 March 2022
Interview 6	Former member of the European Parliament	Brussels	22 March 2022

5. European Commission Empowerment and EU Digital-Related Policies

The following empirical analysis contrasts two areas of EU digital policy—fiscal resource allocation and digital service regulation—to evaluate the extent and nature of Commission empowerment. Although there is substantial supranational empowerment of the Commission in both areas, the degree to which neofunctionalist spillover mechanisms are evident varies, with digital service regulation providing a more classical example of a functional and cultivated spillover.

The 2020 NGEU package is an unprecedented project as it is the first time the EU is borrowing joint debt. The package is therefore presented as the EU's "Hamiltonian" moment by some (Kaletsky, 2020), while others are more wary and point to the strict temporary character of the project (Howarth & Quaglia, 2021; Schoeller & Heidebrecht, 2024). At the heart of the NGEU is a large fund of over €670 billion—for consistency and in line with the regulation establishing the Recovery and Resilience Facility (RRF; (EU) 2021/241), the article uses figures based on 2018 prices as defined in Article 6(1) of the RRF regulation—of which 20% is earmarked for digital-related measures. The second case focuses on the 2022 EU digital services package. The package consists of two regulations that realign the powers of large companies with European businesses and citizens, and protect fundamental rights in the EU. Inter alia, the package has been described as a new constitution of the internet (Geese, 2022) and it has been found to increase the accountability of large platform companies (Heidebrecht, 2023).

5.1. Disposal of Digital-Related Financial Resources

The economic contraction triggered by the onset of the unprecedentedly severe global pandemic in early 2020 was particularly acute in the EU (Quaglia & Verdun, 2023). Beyond its immediate health and economic consequences, the crisis revealed significant vulnerabilities in global supply chains, technological dependencies, and data security (European Commission, 2023). The pandemic accelerated the shift towards digitalisation and established technological resilience as a vital aspect of economic security. Lockdowns and social distancing measures led to an unprecedented increase in remote working, digital services, and e-commerce. These developments showed the transnational nature of digital infrastructure and highlighted the need for EU-level coordination concerning resilience, cybersecurity, and data flows. Against this backdrop, the EU's reliance on foreign digital infrastructure, particularly that of large US-based technology companies, and critical supply chains linked to China put it in a vulnerable position in an increasingly competitive and volatile global order (Interviews 1, 3, 5, and 6). Against this backdrop, the digital domain emerged as a source of strategic vulnerability and a target for integration, creating space for cultivated

spillover. This recognition led the European Commission to launch several initiatives and new strategies, all of which advocate a stronger push towards technological sovereignty. Examples include large-scale investments in AI, cybersecurity, and digital infrastructure to enhance Europe's global competitiveness (European Commission, 2025).

From a digital policy perspective, what sets NGEU apart is that 20% of its €670 billion allocation was earmarked for digital projects—effectively embedding digital transformation in the EU fiscal framework. This design element extended the Commission's influence in national digital strategies supporting the breadth and depth of integration. The massive economic shock of the crisis, combined with existing structural vulnerabilities, prompted some observers to draw parallels with the supreme emergency experienced during the euro crisis (Schoeller & Heidebrecht, 2024). Ultimately, this underscored the need for robust coordinated European action. In response to the unprecedented economic downturn caused by the pandemic, EU leaders recognised a need for a coordinated supranational recovery strategy. This culminated in the European Commission proposing a comprehensive recovery plan aimed at revitalising the European economy, which was unveiled on 27 May 2020. Following extensive negotiations, on 21 July 2020, EU leaders reached an agreement securing an €1.8 trillion recovery package that has been described as constituting an unprecedented historic and paradigmatic change (Buti & Fabbrini, 2023; Kaletsky, 2020).

The creation of the RRF is an instructive test case for the neofunctionalist framework. Although it granted the Commission significant fiscal powers and the ability to influence the digital agendas of member states, this was primarily achieved through strategic political alignment and compromise at the elite level rather than through spillover dynamics. The agreement on the NGEU package is in many ways puzzling as it marked a sharp departure from the austerity-driven approach in the eurozone crisis (de la Porte & Jensen, 2021). The package includes an EU Multiannual Financial Framework of over one trillion euros for 2021–2027 with the €670 billion RRF as its main spending instrument. The RRF represents a paradigmatic shift in European integration. This is driven by the scale of the financial intervention and the novel mechanism of collective borrowing. For the first time, the Commission was authorised to issue common EU debt to finance €390 billion in grants and €360 billion in loans. While the Commission had issued loans before, this was the first large-scale use of non-repayable transfers and it effectively transformed the Commission into a central fiscal actor.

However, a Commission empowered by fiscal integration was highly contested. Consensus among the member states was difficult to achieve due to long-standing divisions over fiscal priorities, economic vulnerabilities, and national philosophies (Interviews 1, 3, and 6; Matthijs & McNamara, 2015; Quaglia & Verdun, 2023). Echoing the dynamics of the euro crisis, the "Frugal Four"—Austria, Denmark, the Netherlands, and Sweden—insisted on strict conditionality, more loans than grants, and robust national oversight (de la Porte & Jensen, 2021). A breakthrough was reached when Germany backed France in proposing a bold grant-based recovery instrument (Howarth & Schild, 2021; Schoeller & Heidebrecht, 2024). The final compromise comprised €338 billion in grants and €385 billion in loans, together with new oversight tools designed to appease fiscally conservative states. This financial innovation expanded the Commission's role from regulatory oversight to coordinating national recovery planning, including digital transformation, which marked a shift towards more proactive fiscal steering (Hodson & Howarth, 2024).

One important feature of the NGEU is its strong and explicit focus on digital transformation. The Commission required at least 20% of the RRF funds to be allocated to digital projects, which reflected

the widespread view that digital sovereignty, cybersecurity, and infrastructure modernisation are strategic imperatives (Interviews 2, 5, and 6). Investments in areas such as artificial intelligence, 5G, cloud computing, and digital skills are aimed at reducing the technological dependence of Europe and boosting its competitiveness in the global digital economy. The earmarked digital funding established a direct channel through which the Commission can influence national digital agendas and align supranational objectives with national implementation—a strategy that conforms with initiatives such as the 2030 Digital Compass (European Commission, 2021a).

This digital dimension is closely tied to what is arguably the most transformative aspect of the NGEU: empowerment of the Commission in fiscal governance. Historically, fiscal policy was decentralised with debt issuance controlled by member states. However, the NGEU broke with this model by introducing common EU-level borrowing and transferring significant fiscal authority to the Commission. The RRF grants the Commission unprecedented influence over national budgets and reforms. This enables the Commission to assess their alignment of recovery plans not only with RRF objectives (Schramm et al., 2022) but also with country-specific recommendations in the European Semester. Many of these recommendations include digital policy priorities (Regulation 2021/241, Article *19*(3-b)). This link to the semester embeds digital governance in a broader framework of conditionality, thereby expanding the Commission's agenda-setting and oversight role in an area that has historically been under the control of national governments (Vanhercke & Verdun, 2022).

While the establishment of the RRF exhibits many characteristics of intergovernmental bargaining, several features also suggest the presence of conditions that promote neofunctional dynamics, in particular functional and cultivated spillover. Functional spillover occurs when integration in one area requires further integration in related areas. Prior to the NGEU, the Commission had limited fiscal capacity to directly support digital policy which reflected the EU's historical regulatory rather than fiscal approach. However, the cross-sectoral nature of digitalisation and its deep links with other areas, particularly the green transition, created a demand for more integrated solutions (Gao, 2025). The alignment of digital, environmental, and fiscal goals created favourable conditions for the Commission to attempt to incorporate digital planning in the broader recovery framework, thereby expanding its fiscal toolbox and influence over digital policy.

The earlier reliance by the Commission on regulatory mechanisms resulted in uneven digital development among member states and failed to close the digital divide (European Commission, 2021a). In response, the Commission advocated financial interventions in digital infrastructure, AI, and cybersecurity—areas that required more than harmonisation. The cross-sectoral interdependencies that these interventions created justified the expansion of supranational tools. At the same time, the Commission promoted additional measures such as EU industrial policy and relaxed state aid rules, thereby further reinforcing its institutional role (Meunier & Mickus, 2020; Schmitz et al., 2025).

Since the pandemic, the Commission has increasingly framed the green and digital transitions as mutually reinforcing and strategically aligned with post-pandemic recovery. This alignment is reflected in flagship initiatives such as the European Green Deal (European Commission, 2019), EU industrial strategies (European Commission, 2020b, 2021b), and the action plan for digitalising the energy system (European Commission, 2022b). These initiatives strengthened the case for EU-level coordination. By portraying digital investment as vital to achieve economic resilience, improve energy efficiency, and achieve climate neutrality,

the Commission legitimised deeper policy and budgetary integration through crisis framing and strategic agenda-setting, indicating a cultivated spillover dynamic. This discursive strategy also supported political spillover. The Commission's focus on the "twin transition" helped foster elite consensus and institutional support, including from the European Parliament (Interview 2). National governments expressed this dual commitment in declarations such as the Berlin Declaration (Council of the EU, 2020), the Green and Digital Transformation Declaration (Council of the EU, 2021), and the Toulouse Call (Council of the EU, 2022). These developments are characteristic of the synergistic model of neo-neofunctionalism, whereby crises mediated by institutional entrepreneurship enable lasting changes to governance.

5.2. Digital Services Regulation and the Empowerment of the Commission

From the 2010s, a series of events—ranging from the Arab Spring, Snowden's revelations of the Cambridge Analytica scandal, and Russian interference in the 2016 US election—demonstrated the importance of digital technologies (Farrell, 2012; Ziegler, 2018). These developments raised public and political awareness of the geopolitical implications of digital interdependence (Farrell & Newman, 2019). Large US-based companies such as Google, Amazon, Facebook, Apple, and Microsoft, often referred to as "Big Tech," were scrutinised for their role in market concentration, democratic disruption, and privacy violations (Srnicek, 2017; Zuboff, 2019). Against this backdrop, the European Commission began to reposition itself as a geopolitical actor. This was reflected in Ursula von der Leyen's announcement of a "geopolitical Commission" in 2019, followed by Thierry Breton's calls for "digital sovereignty" (Breton, 2020; von der Leyen, 2019). The subsequent pandemic and war further intensified calls for strategic autonomy and established platform regulation as a central pillar of the EU digital sovereignty agenda. The Commission framed its interventions as being essential not only for consumer protection but also to safeguard democracy and reduce foreign dependencies. This initiated a cultivated spillover process. By linking digital regulation to fundamental rights and European values (European Commission, 2022a), the Commission effectively transformed technical governance into a political imperative.

Against the backdrop of growing geopolitical tension and the increasing power of foreign tech giants, the Commission officially proposed the digital services package in December 2020. The package comprised two regulations, the Digital Services Act (DSA; Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022, 2022) and the Digital Markets Act (DMA; Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022, 2022). This initiative was built on prior consultations and regulatory concerns started under the Juncker Commission which had already identified challenges related to content moderation, platform accountability, and digital market concentration (European Commission, 2016). Furthermore, the Commission recognised that the rules governing the provision of digital services in the EU had remained largely unchanged since the adoption of the e-Commerce Directive in 2000. In the eyes of many, the DSA and DMA represent the EU's most ambitious attempt to regulate the digital economy (Kausche & Weiss, 2024). They reflect a broader transformation in its governance of online platforms and digital markets and result in an empowerment of the Commission. Following extensive negotiations (Heidebrecht, 2024; Hoeffler & Mérand, 2023), the legislative process concluded under the French Council Presidency in April 2022.

The DSA reflects the Commission's ambition to recalibrate the balance of power in the digital space between online platforms, users, and public authorities (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022, 2022). Aligned with the broader digital strategy (European Commission,

2021a), it asserts EU sovereignty over online services while safeguarding fundamental rights, market fairness, and democratic resilience. Central to the DSA is a tiered regulatory framework which differentiates obligations based on the size and impact of service providers (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022, 2022, Articles 1–3). By categorising entities from basic intermediaries to very large online platforms—ones with at least 45 million active monthly EU users—the EU ensures proportional regulation. The regulation also strengthens due diligence requirements (Articles 10–15) by mandating legal representatives and compliance with EU standards, even for non-EU firms. A key element is its illegal content moderation mechanism (Articles 16–20), which requires prompt action while upholding freedom of expression as required by the Charter of Fundamental Rights. This dual obligation is operationalised with safeguards such as user redress and transparency requirements.

The DMA complements this shift which marks a structural change in regulating digital markets. Its core concept is the identification of "gatekeepers"—dominant firms that act as systemic intermediaries (DMA-R, 2022, Article 3). Gatekeeper status is based on thresholds such as €7.5 billion in annual revenue or €75 billion in market capitalisation and significant user bases in member states. The DMA imposes ex-ante obligations (Articles 5–7) to address market distortions before they materialise. These include bans on self-preferencing, data monopolisation, and exclusionary bundling—practices that have historically entrenched platform dominance. For example, Article 6 prohibits favouring a firm's own services in rankings and marketplaces while Article 5 prevents cross-service leveraging.

Both regulations significantly expand the Commission's authority, both in terms of depth by granting vertical enforcement powers and in terms of breadth by establishing new areas of intervention in platform governance at the supranational level. They differ in important elements from previous far-reaching regulations like the General Data Protection Regulation (GDPR), which is enforced at the member state level but suffers from enforcement bottlenecks (Ryan & Toner, 2021). In the DSA, the Commission assumes a central enforcement role for very large online platforms alongside national Digital Services Coordinators (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022, 2022, Art. 49–74), and by mandating risk assessments, independent audits and transparency reports (Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022, 2022, Article 24–30, 33–43) the Commission institutionalises ex ante oversight of platform behaviour, thus moving beyond reactive enforcement to a more structured governance model. The concept is mirrored in the DMA, in which the concentration of enforcement power in the European Commission is a defining feature (Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022, 2022, Article 29–37). Unlike traditional competition law, which involves national competition authorities and often relies on ex-post assessments, the DMA gives the Commission direct control over gatekeepers, coupled with ex-ante measures. This shall allow for rapid intervention and preventive structural measures. The empowerment of the Commission is also reflected in the power to impose fines, which is significantly higher than in the GDPR, for example, up to 6% of global turnover in the DSA and up to 10% of global turnover in the DMA. The latter can even rise to 20% for repeated infringements.

The transnational nature of platform services creates clear conditions for functional spillover, as digital platforms operate in multiple member states simultaneously, thus bypassing traditional territorial governance. The failure of previous self-regulatory and market-driven models, which was exposed by persistent abuses of market power, misinformation, and privacy violations (Farrand, 2023), revealed the

growing "costs of non-integration" and the systemic risks posed by Big Tech. National authorities struggled to enforce fragmented rules, particularly in legal domains spanning competition, consumer protection, and fundamental rights. This made the case for supranational governance increasingly compelling (Interview 2). In response, the Commission positioned itself as the central actor capable of coordinating cross-border enforcement, primarily through the DSA and the DMA.

Beyond addressing functional demands, the Commission also framed platform regulation strategically in a broader narrative of protecting European values and digital sovereignty (Falkner et al., 2024), thereby indicating a cultivated spillover dynamic. By invoking widely resonant concepts such as "open strategic autonomy" and the need to defend fundamental rights against non-European corporate power (Schmitz & Seidl, 2023), the Commission was able to legitimise deeper integration and central oversight. Broadly supportive public discourse also played a key role in shaping the attitudes of national governments which suggests the presence of political spillover. Many of the issues raised by large platform companies, such as unfair competition, the spread of illegal content, and harmful online behaviour, were recognised as shared challenges by member state governments (Bertuzzi, 2021; Council of the EU, 2022; Kayali, 2021). This positive framing was reinforced by high-profile events and testimony from Frances Haugen, a former Facebook employee, before the European Parliament on 6 May. Haugen revealed that Facebook algorithms had contributed to the dissemination of misinformation and toxic content (Haugen, 2021) thereby helping to galvanise political momentum for stronger EU-level action.

Not all governments were equally enthusiastic, however. Ireland, home to the European headquarters of several major tech firms, voiced scepticism about ex-ante regulation in the Digital Services package. The country asked the Commission to demonstrate that so-called "gatekeeper platforms" were genuinely stifling innovation or limiting market contestability (Stalton, 2020). Conversely, countries such as Germany and France, which had already introduced national legislation such as the NetzDG and Avia laws, recognised the limitations of fragmented national approaches and began to advocate a unified EU framework (Gorwa, 2021; Kayali, 2021). These experiences catalysed political spillover by showing national policymakers that unilateral approaches were insufficient, thus shifting elite expectations and reinforcing demands for EU-wide solutions (Interviews 2, 3, 5). The presence of these dynamics suggests that as the perceived need for coherent cross-border oversight increased, national leaders became more open to the European Commission playing a stronger role—especially as it became clear that unilateral action was insufficient to address the scale and complexity of digital platform governance.

6. Conclusion

Following the adoption of the digital services package (DSA and DMA) in 2022 and the launch of the RRF in 2021, the European Commission became a more interventionist institution with greater decision-making power over digital policy. It has grown in both the depth and breadth of its authority—engaging with national-level digital initiatives through the RRF—and in its decision-making power, particularly through its supervisory role regarding major digital platforms. While this shift is often presented as part of a broader EU push for digital sovereignty (Falkner et al., 2024), this article has demonstrated that digital policymaking has triggered institutional changes concerning Commission empowerment. Furthermore, the article has demonstrated spillover dynamics relating to the characteristics of the digital policy area and its relationship with other areas, particularly the EU twin digital and green transitions, in terms of the Green Deal.

The results of this article align with, but also extend beyond, existing scholarship on the evolving role of the Commission. Scholars such as Hoeffler and Mérand (2023) and Seidl and Schmitz (2023) describe the role of the Commission as increasingly dirigiste and emphasise its ability to influence national policy agendas. Similarly, Farrand and Carrapico (2022) identify a broader shift towards a "neo-mercantilist" model of governance. These trends are part of a wider geopolitical shift in EU governance (Herranz-Surrallés et al., 2024; McNamara, 2024). However, this article has revealed a novel aspect of this transformation: a combination of increased regulatory activism with substantial fiscal powers via the RRF. Taken together, these developments move the EU beyond Majone's (1994) classic model of the regulatory state.

This article has adopted a neofunctionalist approach to explain this institutional evolution. It has shown that the Commission's empowerment does not arise solely in response to external crises but also through the interplay of incremental integration dynamics. The influence of the Commission over the design and implementation of the RRF illustrates that fiscal integration is promoted by an entrepreneurial Commission and spillovers between fiscal integration and digital policy. The article has also aligned with the neo-neofunctionalist "synergy" perspective (Brooks et al., 2023) which views crises as mediated by pre-existing institutional capacities rather than as exogenous shocks that mechanically drive integration. While traditional neofunctionalism emphasises endogenous spillovers, this article has shown that geopolitical events such as the war in Ukraine and the global impact of the pandemic can reinforce these processes, particularly in the context of digital-specific conditions. These include regulatory interdependence in the context of transnational data flow, established Commission competences in governing the single market, the perceived weaponisation of digital interdependence, and a positive discursive environment for EU action in the digital sphere.

Although neofunctionalist theory suggests that functional interdependence naturally leads to integration, this framework is particularly effective in explaining the development of regulations on digital services. In this area, spillover dynamics are strong and are closely aligned with the core assumptions of the theory, given the presence of all four conditions mentioned above (interdependence, established competences, perceived external threat, and positive discursive environment). However, the explanatory power of neofunctionalism is more limited when applied to digital-related financial resources. While the framework identifies some enabling conditions and spillover effects (fewer explicit problems arising from regulatory fragmentation, no established Commission competences, a potentially conflictive public discourse along the lines of the euro crisis), integration in this area is more strongly shaped by member state bargaining, particularly given the controversial nature of fiscal integration. In this context, integration did not arise solely from objective interdependence between policy areas. Instead, the European Commission actively shaped the trajectory of integration by constructing a narrative that legitimised the NGEU initiative. By linking the NGEU to broader EU strategic priorities, namely digital transformation and the green transition, the Commission framed fiscal innovation as essential to achieve the EU's long-term aims. This helped generate political support for deeper EU-level planning in the digital domain.

Table 3 illustrates these empirical dynamics by summarising the types of spillover observed in the two case studies—NGEU and digital service regulation—and their respective contributions to Commission empowerment. Overall, this article has demonstrated that although neofunctionalism provides valuable insights into the dynamics of supranational empowerment, particularly in regulatory domains such as platform governance, it is less effective in explaining outcomes driven primarily by intergovernmental

bargaining. In the case of financial resources, the interdependent nature of the issue and regulatory fragmentation were more difficult to prove. Also, the Commission literally has no established role in this area on which it can build. Therefore, strategic leadership and elite consensus, based on interest-driven negotiations, were also decisive in the fiscal dimension. This provides evidence of important factors beyond neofunctional spillover dynamics. Although neofunctionalist spillovers were particularly evident in digital service regulation, both cases demonstrate empowerment through increased depth (vertical transfer of competences) and breadth (expansion into new digital or fiscal domains).

Table 3. Summary of the study's argument.

Type of Spillover	Digital-Related Financial Resources	Digital Services Regulation
Functional Spillover	The integration of fiscal support with digital and green targets addressed the interdependency between crisis recovery and structural transformation. It supported new EU budget instruments and digital planning at the EU level.	The fragmented nature of national rules and the systemic risks posed by Big Tech led to a need for EU-wide regulatory frameworks, vertical oversight by the Commission, and new areas of intervention.
Political Spillover	Amid national limitations, member states and the public supported EU-level responses. Digital investments were framed as shared strategic aims facilitating supranational budgetary coordination.	Recognising shared risks, such as misinformation and market concentration, shifted political preferences towards EU solutions and empowered the Commission in enforcing regulations on platforms.
Cultivated Spillover	The Commission presented the NGEU as being essential for the EU twin transition and its strategic autonomy. It leveraged the crisis to build support for fiscal innovation and supranational planning.	The Commission used crises such as the Cambridge Analytica scandal, the pandemic, and the war in Ukraine, and strategic framing such as the protection of democracy and digital sovereignty to justify new enforcement powers.

As Table 2 shows, the two cases reveal different yet complementary spillover dynamics. In the case of the RRF, for example, the European Commission played a role in fostering a favourable narrative on digitalisation. Arguably, this narrative not only advanced the Commission's regulatory agenda but also served to justify the need for closer fiscal integration. By overseeing and approving member state recovery plans, which must devote at least 20% of funding to digital investments, the Commission gained considerable leverage over national digital policies. These plans are evaluated against EU-wide priorities, particularly the digital objectives set out in European Semester country-specific recommendations. This creates a conditional framework in which access to funding depends on alignment with EU digital aims which enables the Commission to influence national reforms. In doing so, the influence of the Commission extends beyond standard-setting into fiscal governance and impacts the direction and implementation of digital policies.

By contrast, the case of digital service regulation shows that functional, political, and cultivated spillovers operated more strongly in the traditional regulatory domain of the Commission. The increasing number of fragmented national rules and mounting concerns over the cross-border influence of Big Tech created functional pressures for harmonisation and EU-level enforcement. The DSA and the DMA introduced vertical oversight mechanisms, thus granting the Commission direct supervisory powers over systemic platforms. Politically, high-profile scandals such as the Cambridge Analytica affair and the spread of disinformation reshaped public and government expectations and shifted preferences towards stronger

supranational control. Cultivated spillover was also significant. The Commission strategically presented digital regulation as vital to defend European values, democratic resilience, and digital sovereignty. By presenting itself as the sole entity capable of addressing transnational risks and ensuring accountability, the Commission broadened its remit from agenda-setting to enforcement. These developments further support the neo-neofunctionalist view of crisis-mediated integration with the Commission leveraging functional interdependence and favourable discourse to consolidate regulatory authority.

Writing in mid-2025 and looking ahead, it is unclear whether the recent expansion of the Commission's powers will result in deeper and more lasting European integration. The Commission's recent empowerment was largely shaped by a combination of favourable conditions (which varied in the two cases) based on the high interdependence of the digital dimension, such as transnational data flows coupled with regulatory fragmentation, the Commission's established role in regulatory policies, perceived geopolitical challenges, and low salience coupled with affirmative public discourse related to EU action in the digital domain. All of these conditions can change. For example, a more conflict-prone US government could engage in targeted lobbying efforts, particularly in economically dependent member states such as Ireland. This could reinforce internal divisions and hinder progress towards cohesive EU action. Furthermore, the EU's limited and uneven digital industrial capabilities could further complicate matters. Another issue relates to potentially divergent elite preferences across member states that may also become subject to the political influence of Big Tech. Against this backdrop, EU policymakers would be wise to seek a supranational compromise that enables cohesive EU action. Research could analyse the causes and effects of changes to these conditions, such as how national elites promote national or EU sovereignty, what this means in relation to other digital powers and the reasons behind it.

Acknowledgments

The author would also like to thank the participants of the 2023 UACES Conference in Belfast for their constructive comments on an earlier version of this article. The guest editors of the special issue on *The Geopolitics of Transnational Data Governance*, Xinchuchu Gao and Xuechen Chen, the participants of an online workshop in this context, as well as three anonymous reviewers also provided very useful feedback on earlier versions of this article.

Funding

The author would like to thank the Faculty of Social Sciences for their financial support in proofreading this article.

Conflict of Interests

The author reports no conflict of interest.

LLMs Disclosure

This article was the author's first attempt at using LLMs. Specifically, these models were used to review the language and grammar of the article's initial drafts. For this purpose, the authors used a combination of ChatGPT, DeepL, and Grammarly, also to gain an understanding of their usability for academic purposes. The authors also occasionally asked the LLMs for suggestions regarding topic sentences and rephrasing of paragraphs out of curiosity. While some of these suggestions proved useful (for example, when writing at late hours) and were interesting, they basically always required substantial human adjustment and

verification. The quality of the final version of this text was, afterwards and in addition to the author, substantially improved by a human proofreader (I would like to thank David Barnes for his help). I remain responsible for all errors.

References

Bauer, M. W., & Becker, S. (2014). The unexpected winner of the crisis: The European Commission's strengthened role in economic governance. *Journal of European Integration*, *36*(3), 213–229. https://doi.org/10.1080/07036337.2014.885750

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Bertuzzi, L. (2021, November 17). DSA: EU ambassadors reach agreement to start interinstitutional negotiations. *Euractiv*. https://www.euractiv.com/section/tech/news/dsa-eu-ambassadors-reach-agreement-to-start-interinstitutional-negotiations

Bickerton, C. J., Hodson, D., & Puetter, U. (2015). The new intergovernmentalism: European integration in the post-Maastricht era. *JCMS: Journal of Common Market Studies*, *53*(4), 703–722. https://doi.org/10.1111/jcms.12212

Bonnamy, C., & Perarnaud, C. (2023). Introduction: EU digital policies and politics. *Politique européenne*, *81*(3), 8–27.

Börzel, T. A. (2005). Mind the gap! European integration between level and scope. *Journal of European Public Policy*, *12*(2), 217–236. https://doi.org/10.1080/13501760500043860

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*: Oxford University Press.

Breton, T. (2020). *Speech by commissioner Thierry Breton at Hannover Mese digital days* [Speech transcript]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_20_1362

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*, *61*(5), 1261–1280. https://doi.org/10.1111/jcms.13462

Brooks, E., de Ruijter, A., Greer, S. L., & Rozenblum, S. (2023). EU health policy in the aftermath of Covid-19: Neofunctionalism and crisis-driven integration. *Journal of European Public Policy*, *30*(4), 721–739. https://doi.org/10.1080/13501763.2022.2141301

Buti, M., & Fabbrini, S. (2023). Next generation EU and the future of economic governance: towards a paradigm change or just a big one-off? *Journal of European Public Policy*, *30*(4), 676–695. https://doi.org/10.1080/13501763.2022.2141303

Carver, J. (2023). More bark than bite? European digital sovereignty discourse and changes to the European Union's external relations policy. *Journal of European Public Policy*, *31*(8), 2250–2286. https://doi.org/10.1080/13501763.2023.2295523

Cini, M., & Czulno, P. (2022). Digital single market and the EU competition regime: An explanation of policy change. *Journal of European Integration*, *44*(1), 41–57. https://doi.org/10.1080/07036337.2021.2011260

Council of the European Union. (2020). *Berlin declaration on digital society and value-based digital government*. https://ec.europa.eu/newsroom/dae/document.cfm?doc_id=75984

Council of the European Union. (2021). *A green and digital transformation of the EU*. https://ec.europa.eu/newsroom/dae/redirection/document/74940

Council of the European Union. (2022). *Digital Services Act: Council and European Parliament reach deal on a safer online space*. https://www.consilium.europa.eu/en/press/press-releases/2022/04/23/digital-services-act-council-and-european-parliament-reach-deal-on-a-safer-online-space

Council of the European Union. (2022). *Toulouse call for a green and digital transition in the EU*. https://www.economie.gouv.fr/files/files/2022/Call_for_Green_Digital_Transition_EU.PDF

Decision (EU) 2022/2481 of the European Parliament and of the Council of 14 December 2022 establishing the digital decade policy programme 2030. (2022). *Official Journal of the European Union*, L 323/4. https://eur-lex.europa.eu/eli/dec/2022/2481/oj/eng

de la Porte, C., & Jensen, M. D. (2021). The next generation EU: An analysis of the dimensions of conflict behind the deal. *Social Policy & Administration*, *55*(2), 388–402. https://doi.org/10.1111/spol.12709

Deters, H., & Falkner, G. (2021). Remapping the European agenda-setting landscape. *Public Administration*, *99*(2), 290–303. https://doi.org/10.1111/padm.12716

Donnelly, S., Ríos Camacho, E., & Heidebrecht, S. (2024). Digital sovereignty as control: the regulation of digital finance in the European Union. *Journal of European Public Policy*, *31*(8), 2226–2249. https://doi.org/10.1080/13501763.2023.2295520

European Commission. (2016). *Communication on online platforms and the digital single market opportunities and challenges for Europe* (COM(2016) 288 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52016DC0288

European Commission. (2019). *The green deal* (COM(2019) 640 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0640

European Commission. (2020a). *Commission work programme 2020. A Union that strives for more* (COM(2020) 37 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52019DC0640

European Commission. (2020b). *A new industrial strategy for europe* (COM (2020) 102). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52020DC0102

European Commission. (2021a). *2030 Digital compass: The European way for the digital decade* (COM(2021) 118 final). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021DC0118

European Commission. (2021b). *Updating the 2020 new industrial strategy: Building a stronger single market* (COM (2021) 350). https://commission.europa.eu/document/9ab0244c-6ca3-4b11-bef9-422c7eb34f39_en?prefLang=de

European Commission. (2022a). *The Digital Services Act: Ensuring a safe and accountable online environment*. https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-services-act-ensuring-safe-and-accountable-online-environment_en

European Commission. (2022b). *Digitalising the energy system—EU action plan*. (COM(2022) 552 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52022DC0552

European Commission. (2023). *European economic security strategy*. (JOIN(2023) 20 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52023JC0020

European Commission. (2025). *Moving forward together: A bolder, simpler, faster Union* (COM(2025) 45 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52025DC0045

Falkner, G., Heidebrecht, S., Obendiek, A., & Seidl, T. (2024). Digital sovereignty—Rhetoric and reality. *Journal of European Public Policy*, *31*(8), 2099–2120. https://doi.org/10.1080/13501763.2024.2358984

Farrand, B. (2023). The ordoliberal internet? Continuity and change in the EU's approach to the governance of cyberspace. *European Law Open*, *2*(1), 106–127. https://doi.org/10.1017/elo.2023.14v

Farrand, B., & Carrapico, H. (2022). *Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity*. Unpublished manuscript.

Farrell, H. (2012). The consequences of the internet for politics. *Annual Review of Political Science*, *15*(1), 35–52. https://doi.org/10.1146/annurev-polisci-030810-110815

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79. https://doi.org/10.1162/isec_a_00351

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

Gao, X. (2025). The EU's twin transitions towards sustainability and digital leadership: A coherent or fragmented policy field? *Regional Studies*, *59*(1), Article 2360053. https://doi.org/10.1080/00343404.2024.2360053

Geese, A. (2022). *European Parliament votes on constitution for the internet*. [Press release]. https://www.greens-efa.eu/en/article/press/european-parliament-votes-on-constitution-for-the-internet

Gerring, J. (2004). What is a case study and what is it good for? *American Political Science Review*, *98*(2), 341–354. https://doi.org/10.1017/S0003055404001182

Gocaj, L., & Meunier, S. (2013). Time will tell: The EFSF, the ESM, and the euro crisis. *Journal of European Integration*, *35*(3), 239–253. https://doi.org/10.1080/07036337.2013.774778

Goldstein, K. (2002). Getting in the door: Sampling and completing elite interviews. *PS: Political Science & Politics*, *35*(4), 669–672. https://doi.org/10.1017/S1049096502001130

Gorwa, R. (2021). Elections, institutions, and the regulatory politics of platform governance: The case of the German NetzDG. *Telecommunications Policy*, *45*(6), Article 102145. https://doi.org/10.1016/j.telpol.2021.102145

Haas, E. B. (1958). The challenge of regionalism. *International Organization*, *12*(4), 440–458.

Haggart, B., & Keller, C. I. (2021). Democratic legitimacy in global platform governance. *Telecommunications Policy*, *45*(6), Article 102152. https://doi.org/10.1016/j.telpol.2021.102152

Haugen, F. (2021, November 8). *Public hearing on whistle-blower's testimony on the negative impact of tech companies' products on user: Opening statement by Frances Haugen* [Video]. European Parliament. https://multimedia.europarl.europa.eu/it/video/whistleblowers-testimony-on-the-negative-impact-of-big-tech-companies-products-on-user-extracts-from-the-opening-statement-by-frances-haugen-imco-committee_I213404

Heidebrecht, S. (2017). Trying not to be caught in the act: Explaining European Central Bank's bounded role in shaping the European Banking Union. *Journal of Contemporary European Research*, *13*(2), 1125–1143. https://doi.org/10.30950/jcer.v13i2.785

Heidebrecht, S. (2023). Platform accountability in the European Union: The cases of data protection and digital services regulation. *Politique européenne*, *81*, 142–168. https://doi.org/10.3917/poeu.081.0142

Heidebrecht, S. (2024). From market liberalism to public intervention: Digital Sovereignty and changing European Union digital single market governance. *JCMS: Journal of Common Market Studies*, *62*(1), 205–223. https://doi.org/10.1111/jcms.13488

Heidebrecht, S. (2025). *European Central Bank reform after the financial crisis: Technocratic empowerment*. Routledge. https://doi.org/10.4324/9781003363620

Heldt, E. C., & Mueller, T. (2021). The (self-)empowerment of the European Central Bank during the sovereign debt crisis. *Journal of European Integration*, *43*(1), 83–98. https://doi.org/10.1080/07036337.2020.1729145

Herranz-Surrallés, A., Damro, C., & Eckert, S. (2024). The geoeconomic turn of the single European market? Conceptual challenges and empirical trends. *JCMS: Journal of Common Market Studies*, *62*(4), 919–937. https://doi.org/10.1111/jcms.13591

Hodson, D., & Howarth, D. (2024). The EU's recovery and resilience facility: An exceptional borrowing instrument? *Journal of European Integration*, *46*(1), 69–87. https://doi.org/10.1080/07036337.2023.2243378

Hoeffler, C., & Mérand, F. (2023). Digital sovereignty, economic ideas, and the struggle over the digital markets

act: A political-cultural approach. *Journal of European Public Policy*, *31*(8), 2121–2146. https://doi.org/10.1080/13501763.2023.2294144

Howard, P. N. (2020). *Lie machines: How to save democracy from troll armies, deceitful robots, junk news operations, and political operatives*. Yale University Press.

Howarth, D., & Quaglia, L. (2021). Failing forward in economic and monetary union: explaining weak Eurozone financial support mechanisms. *Journal of European Public Policy*, *28*(10), 1555–1572. https://doi.org/10.1080/13501763.2021.1954060

Howarth, D., & Schild, J. (2021). Nein to 'transfer union': the German brake on the construction of a European Union fiscal capacity. *Journal of European Integration*, *43*(2), 209–226. https://doi.org/10.1080/07036337.2021.1877690

Ioannou, D., Leblond, P., & Niemann, A. (2015). European integration and the crisis: Practice and theory. *Journal of European Public Policy*, *22*(2), 155–176. https://doi.org/10.1080/13501763.2014.994979

Kaletsky, A. (2020, May 21). Europe's Hamiltonian Moment. *Project Syndicate*. https://www.project-syndicate.org/commentary/french-german-european-recovery-plan-proposal-by-anatole-kaletsky-2020-05

Kausche, K., & Weiss, M. (2024). Platform power and regulatory capture in digital governance. *Business and Politics*, *27*(2), 284–308. https://doi.org/10.1017/bap.2024.33

Kayali, L. (2021, May 27). France's plan to rein in Big Tech (and Ireland and Luxembourg) *Politico*. https://www.politico.eu/article/france-ireland-luxembourg-big-tech-regulation-apple-amazon-facebook-google-digital-services-act-digital-markets

Khan, L. M. (2017). Amazon's antitrust paradox. *Yale Law Journal*, *126*(710), 712–805.

Lambach, D., & Oppermann, K. (2022). Narratives of digital sovereignty in German political discourse. *Governance*, *36*(3), 693–709. https://doi.org/10.1111/gove.12690

Laurer, M., & Seidl, T. (2021). Regulating the European data-driven economy: A case study on the general data protection regulation. *Policy & Internet*, *13*(2), 257–277. https://doi.org/10.1002/poi3.246

Majone, G. (1994). The rise of the regulatory state in Europe. *West European Politics*, *17*(3), 77–101. https://doi.org/10.1080/01402389408425031

Matthijs, M., & McNamara, K. (2015). The euro crisis' theory effect: Northern saints, southern sinners, and the demise of the eurobond. *Journal of European Integration*, *37*(2), 229–245. https://doi.org/10.1080/07036337.2014.990137

Mazur, V., & Ramiro Troitiño, D. (2024). Digitalization, neofunctionalism, and integration in the European Union. In D. Ramiro Troitiño (Ed.), *E-Governance in the European Union: Strategies, tools, and implementation* (pp. 7–22). Springer.

McNamara, K. R. (2024). Transforming Europe? The EU's industrial policy and geopolitical turn. *Journal of European Public Policy*, *31*(9), 2371–2396. https://doi.org/10.1080/13501763.2023.2230247

Meunier, S., & Mickus, J. (2020). Sizing up the competition: explaining reform of European Union competition policy in the Covid-19 era. *Journal of European Integration*, *42*(8), 1077–1094. https://doi.org/10.1080/07036337.2020.1852232

Nicoli, F. (2020). Neofunctionalism revisited: Integration theory and varieties of outcomes in the Eurocrisis. *Journal of European Integration*, *42*(7), 897–916.

Niemann, A., & Ioannou, D. (2015). European economic integration in times of crisis: a case of neofunctionalism? *Journal of European Public Policy*, *22*(2), 196–218. https://doi.org/10.1080/13501763.2014.994021

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

Quaglia, L., & Verdun, A. (2023). The Covid-19 pandemic and the European Union: politics, policies and institutions. *Journal of European Public Policy*, *30*(4), 599–611. https://doi.org/10.1080/13501763.2022.2141305

Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828 (Digital Markets Act). *Official Journal of the European Union*, L 265/1. http://data.europa.eu/eli/reg/2022/1925/oj

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). *Official Journal of the European Union*, L 277/1. http://data.europa.eu/eli/reg/2022/2065/oj

Rittberger, B. (2014). Integration without representation? The European parliament and the reform of economic governance in the EU. *JCMS: Journal of Common Market Studies*, *52*(6), 1174–1183. https://doi.org/10.1111/jcms.12185

Roberts, H., Cowls, J., Casolari, F., Morley, J., Taddeo, M., & Floridi, L. (2021). Safeguarding European values with digital sovereignty: An analysis of statements and policies. *Internet Policy Review*, *10*(3). https://doi.org/10.14763/2021.3.1575

Ryan, J., & Toner, A. (2021). *Europe's enforcement paralysis ICCL's 2021 report on the enforcement capacity of data protection authorities*. Irish Council for Civil Liberties. https://www.iccl.ie/digital-data/2021-gdpr-report

Schimmelfennig, F. (2015). Liberal intergovernmentalism and the euro area crisis. *Journal of European Public Policy*, *22*(2), 177–195. https://doi.org/10.1080/13501763.2014.994020

Schmidt, S. K. (2000). Only an agenda setter? The European Commission's power over the council of ministers. *European Union Politics*, *1*(1), 37–61.

Schmitter, P. C. (1970). A revised theory of regional integration. *International Organization*, *24*(4), 836–868.

Schmitter, P. C. (2013). Ernst B. Haas and the legacy of neofunctionalism. In T. Börzel (Ed.), *The disparity of European integration* (pp. 39–56). Routledge.

Schmitz, L., & Seidl, T. (2023). As open as possible, as autonomous as necessary: Understanding the rise of open strategic autonomy in EU trade policy. *JCMS: Journal of Common Market Studies*, *61*(3), 834–852. https://doi.org/10.1111/jcms.13428

Schmitz, L., Seidl, T., & Wuttke, T. (2025). The costs of conditionality. IPCEIs and the constrained politics of EU industrial policy. *Competition & Change*. Advance online publication. https://doi.org/10.1177/10245294251320675

Schoeller, M. G., & Heidebrecht, S. (2024). Continuity despite crises: Germany's euro policy in the light of the pandemic, war and inflation. *Journal of European Public Policy*, *31*(9), 2509–2533. https://doi.org/10.1080/13501763.2023.2218883

Schramm, L., Krotz, U., & De Witte, B. (2022). Building 'next generation' after the pandemic: The implementation and implications of the EU Covid Recovery Plan. *JCMS: Journal of Common Market Studies*, *60*(S1), 114–124. https://doi.org/10.1111/jcms.13375

Seawright, J., & Gerring, J. (2008). Case selection techniques in case study research: A menu of qualitative and quantitative options. *Political Research Quarterly*, *61*(2), 294–308. https://doi.org/10.1177/1065912907313077

Seidl, T., & Schmitz, L. (2023). Moving on to not fall behind? Technological sovereignty and the 'geo-dirigiste' turn in EU industrial policy. *Journal of European Public Policy*, *31*(8), 2147–2174. https://doi.org/10.1080/13501763.2023.2248204

Srnicek, N. (2017). *Platform capitalism*. Polity Press.

Stalton, S. (2020, December 18). Digital brief, powered by Google: DSA and DMA—member states respond. *Euractiv*. https://www.euractiv.com/section/digital/news/digital-brief-powered-by-google-dsa-and-dma-member-states-respond

Stone Sweet, A., & Sandholtz, W. (1997). European integration and supranational governance. *Journal of European Public Policy*, *4*(3), 297–317. https://doi.org/10.1080/13501769780000011

Tansey, O. (2007). Process tracing and elite interviewing: a case for non-probability sampling. *PS: Political Science & Politics*, *40*(4), 765–772.

Van Evera, S. (1997). *Guide to methods for students of political science*: Cornell University Press.

Vanhercke, B., & Verdun, A. (2022). The European semester as goldilocks: Macroeconomic policy coordination and the recovery and resilience facility. *JCMS: Journal of Common Market Studies*, *60*(1), 204–223. https://doi.org/10.1111/jcms.13267

von der Leyen, U. (2019). *Speech by President-elect von der Leyen in the European Parliament Plenary on the occasion of the presentation of her College of Commissioners and their programme, 27 September 2019* [Speech transcript]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/speech_19_6408

von der Leyen, U. (2021). *State of the Union address by President von der Leyen* [Speech transcript]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_21_4701

von Soest, C. (2023). Why do we speak to experts? Reviving the strength of the expert interview method. *Perspectives on Politics*, *21*(1), 277–287. https://doi.org/10.1017/S1537592722001116

Xuechen, C., & Gao, X. (2025). Geopolitics and transnational data governance. *Politics and Governance*, *13*, Article 11428.

Ziegler, C. E. (2018). International dimensions of electoral processes: Russia, the USA, and the 2016 elections. *International Politics*, *55*(5), 557–574. https://doi.org/10.1057/s41311-017-0113-1

Zuboff, S. (2019). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. Hachette Book Group.

About the Author

Sebastian Heidebrecht (PhD, Duisburg-Essen) is an assistant professor at the Centre for European Integration Research (EIF), housed in the University of Vienna's Department of Political Science.

Politics and Governance
2025 • Volume 13 • Article 10422
https://doi.org/10.17645/pag.10422

cogitatio

ARTICLE

Open Access Journal

The EU's Digital Footprint: Shaping Data Governance in Japan and Singapore

Danni Zhang [1,2]

[1] Faculty of Politics and International Relations, Northeastern University London, UK
[2] Institute of Cyber Security for Society, University of Kent, UK

Correspondence: Danni Zhang (dz3501phd@nulondon.ac.uk)

Submitted: 28 March 2025 **Accepted:** 8 May 2025 **Published:** 16 July 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

The rapid development of the internet and information and communication technologies over the past few decades has led to the emergence of a new digital order, attracting significant attention from both academia and policymakers. In the global digital domain, the EU has assumed a distinctive role in shaping and influencing digital norms and standards. This status stems from the EU's pioneering efforts, ranging from the Council of Europe's Convention 108 (1981) to the more recent General Data Protection Regulation, which has exerted far-reaching extraterritorial effects, influencing data laws and regulatory practices beyond the EU's borders. However, there remains a lack of sufficient research on how these actors have progressively enacted and revised their data regulations in response to evolving EU standards. To address this gap, this article adopts a qualitative approach to examine how the EU's evolving data regulations have diffused to and been adopted by two Asian countries—Japan and Singapore. By categorising diffusion mechanisms into incentive, socialisation, learning, competition, and emulation, this research further explores the operative mechanisms underpinning the diffusion process. This research argues that the EU's diffuse-ability in Japan has demonstrated a gradual strengthening trend, with socialisation functioning as the primary mechanism driving this process. In contrast, the EU's diffuse-ability in Singapore has remained relatively weak, with competition serving as the dominant mechanism.

Keywords

data governance; diffuse-ability; EU; Japan; Singapore

1. Introduction

In the digital era, data has emerged as a key geopolitical and economic asset, influencing everything from global trade to national security. More specifically, since data is often referred to as "the new oil" (Humby, 2006, as cited in Palmer, 2006), governments have embraced this metaphor to emphasise its transformative power in the modern economy (Kuneva, 2009; World Economic Forum, 2011). This analogy underscores the strategic value of data, which, much like oil, has become a vital resource central to geopolitical competition. While traditional geopolitics has historically focused on physical geography, the rapid development of information and communication technologies (ICTs) and the internet has introduced cyberspace as an increasingly salient dimension (Brunn, 2000; Deibert, 2008). This expansion has extended the scope of geopolitics to the virtual sphere, making data governance—including its collection, storage, transfer, and protection—a critical issue in shaping international relations and geopolitical dynamics. Moreover, governments advocate divergent models of data governance, thereby creating barriers to global data flow and complicating international cooperation and trade (O'Hara & Hall, 2021). As a key player in both global geopolitical competition and the digital economy, the EU, alongside the US and China, supports a model of data governance that is widely regarded as rights-based, emphasising privacy and data protection (Bradford, 2023; O'Hara & Hall, 2021).

The EU has historically been recognised as a normative power (Manners, 2002), with its strategies often characterised as the "soft version of geopolitics" (Edwards, 2008), extending the norms, values, and standards developed within its geographic space to other countries (Christou, 2010). As the EU strives to promote its norms, values, and standards globally, its role in diffusing these principles provides valuable insights for diffusion research. Specifically, in existing policy diffusion research, two main perspectives explain why external actors selectively adopt EU standards or policies. First, the EU's substantial economic market acts as a powerful incentive, a phenomenon known as the "Brussels effect," where external actors align with EU standards to gain access to its lucrative market (Bradford, 2020). Hopkins and McNeill (2015) illustrate this phenomenon through the case of New Zealand's wine regulations. To gain access to the EU market—accounting for approximately 70% of the global wine market—New Zealand largely adopted the EU model for its wine regulations (Hopkins & McNeill, 2015). Second, geographic proximity is often associated with a higher likelihood of adopting EU laws and standards (Schimmelfennig & Sedelmeier, 2004). During the EU's Eastern enlargement, countries such as Ukraine and Morocco adopted EU-aligned policies through instruments such as the European Neighbourhood Policy and associated agreements (Schimmelfennig & Sedelmeier, 2004). Russia's adoption of antitrust law further demonstrates the influence of geographic proximity (Bradford et al., 2024).

In the context of diffusion research on data laws and regulations, despite an extensive body of scholarship on the global diffusion of EU data policies, several limitations persist. First, some scholars have extended the concept of the Brussels effect and geographic proximity as the two primary factors explaining why external actors selectively adopt the EU's standards or policies in the context of data regulation diffusion. However, this perspective tends to overemphasise EU-driven factors, placing excessive focus on the EU's influence while overlooking the local context and agency recipient actors, including their domestic priorities and strategic adaptations. For instance, Cervi (2022) underscores the appeal of the EU's internal market as a key factor contributing to the GDPR's global reach. Similarly, Akcali Gur (2020), through a case study of Turkey's data protection legislation, highlights the EU's normative power in shaping regulatory frameworks beyond its

jurisdiction, particularly in neighbouring states. By contrast, Corning (2024) challenges this EU-driven perspective, arguing that the prevailing explanation for GDPR diffusion—the Brussels effects—fails to account for how local contexts, including political, institutional, and socio-economic conditions within affected countries, shape both the adoption and implementation of data protection policies.

Second, although recent scholars have increasingly extended their focus beyond the EU's immediate neighbourhood to examine the global diffusion of EU data regulations, much of the research remains centred on the influence of the General Data Protection Regulation (GDPR) in prompting other international actors to formulate or amend their data legislation, while overlooking the impact of earlier EU data regimes. Asia has become a focal point of scholarly attention, given its strategic importance in the EU's digital agenda and its growing role in global data governance. As a result, a growing body of literature examines how EU data regulations have shaped the development and reform of data laws in Asian countries (Bentotahewa et al., 2022; Corning, 2024; Creemers, 2022). Based on case studies of data privacy law reforms in four ASEAN countries—the Philippines, Singapore, Thailand, and Indonesia—Corning (2024) highlights how internal regulatory demands, driven by the accelerating digitalisation of these societies, intersect with the role of the GDPR as a legal template. Similarly, Bentotahewa et al. (2022) demonstrate the influence of the GDPR on South Asian countries, showing how the EU's regulatory framework has informed legislative developments in the region. Additionally, Creemers (2022), through a systematic analysis of China's data protection framework, argues that China's personal information protection model has been significantly influenced by the GDPR. Although China largely adopted the GDPR's consumer protection components, it has explicitly rejected the EU's foundational principle of privacy as a fundamental right. While existing research widely acknowledges the GDPR's influence on the development of data legislation in Asia, it often overstates its role as a global gold standard and neglects the EU's longer-standing regulatory influence in this field. The EU's external regulatory power did not emerge solely with the GDPR, rather, it evolved gradually through earlier instruments such as the Council of Europe's Convention 108 (Convention 108; Council of Europe, 1981) and the 1995 EU Data Protection Directive (1995 Directive; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, 1995). These earlier frameworks laid critical normative and legal foundations for global data governance, influencing legislative developments across various regions well before the GDPR's adoption.

To address these gaps, this article conducts a case study analysis of the development of data regulations in Japan and Singapore, guided by two research questions:

1. To what extent have the data governance frameworks of Japan and Singapore been influenced by the evolution of EU data regulations?
2. What mechanisms contributed to Japan and Singapore's regulatory convergence with EU data regulations, and under what conditions did this convergence occur?

The first question assesses the EU's diffuse-ability in the digital governance domain within Japan and Singapore. The second question further explores the mechanisms that contributed to regulatory convergence, focusing specifically on key periods of convergence to interpret how and under what conditions EU influence took effect.

This article is structured as follows: Section 2 reviews the literature on diffusion theory, including policy diffusion and diffusion mechanisms within the field of international relations (IR), and outlines the

theoretical framework. Section 3 discusses the methodology and case selection. Section 4 presents detailed case studies of Japan and Singapore. Each case study sheds light on the diffusion mechanisms that played significant roles in enabling these countries to adopt EU-inspired regulatory elements and to establish or amend their data laws. Section 5 summarises the key findings and presents the conclusion.

2. A Theoretical Framework Based on Diffusion Literature

To develop a more nuanced understanding of the EU's diffuse-ability and the means through which it transmits regulations to Asian countries, this study employs a theoretical framework grounded in existing diffusion literature. Specifically, in IR scholarship, policy diffusion research focuses on how specific policies spread across different jurisdictions including countries, states, cities, and organisations (Bradford et al., 2024; Graham et al., 2013; Shipan & Volden, 2008). Scholars regard the term "diffusion" as a process of spreading ideational frameworks, instruments, and institutional settings at national, regional, and international levels (Elkins & Simmons, 2005; Simmons et al., 2008). In this study, diffusion is understood as the process through which data regulations are transmitted from the EU to the two Asian countries.

Moreover, "diffusion items" refer to the ideational frameworks, instruments, and institutional settings that are transmitted in the diffusion process. Scholars categorise these items into three levels of specificity: (a) overarching ideas and norms, (b) policy instruments, and (c) precise institutional settings (Klingler-Vidra & Schleifer, 2014). Since legal provisions constitute binding commitments that operationalise regulatory standards within domestic systems, offering codified evidence of convergence or divergence vis-à-vis EU data governance standards, this study relies on formal legal documents, including official policy documents and cooperation agreements, as primary data sources for diffusion analysis. In this research, these diffusion items—referred to as "EU elements" (detailed in Section 3)—are derived from the EU's data regulatory frameworks, including Convention 108, the 1995 Directive, and the GDPR.

To evaluate diffusion outcomes, scholars have used measures such as varying degrees of convergence (Klingler-Vidra & Schleifer, 2014; Solingen, 2012) or a conceptual framework distinguishing between adoption, adaptation, resistance, and rejection (Björkdahl et al., 2015) to capture differing degrees of recipient acceptance. Accordingly, this study adopts diffusion outcomes as analytical tools to assess both the extent and effectiveness of the EU's diffuse-ability in Asian countries over the past three decades (see Table 1).

Scholars acknowledge multiple mechanisms underpinning the spread of diffusion items to varying degrees (Gilardi & Wasserfallen, 2019; Meseguer & Gilardi, 2009; Risse, 2016). To analyse the diffusion mechanisms

Table 1. Conceptual tools of evaluating EU's diffuse-ability.

Conceptual tool	Type and definition	EU's diffuse-ability
Diffusion outcomes	Adoption: Local practices have complied with the EU's diffusion items	Strong
	Adaptation: Local practices have integrated EU's diffusion items but have localised them to fit the local demands and context	Mid-strong
	Resistance: Few local practices imported EU's diffusion items	Weak
	Rejection: Local practices rejected any EU's diffusion item	No

Source: Adapted from Björkdahl et al. (2015).

driving the transmission of EU data regulations to Asian countries, this study adopts five commonly cited mechanisms: (a) incentive, (b) socialisation, (c) learning, (d) competition, and (e) emulation. Building on Risse's (2016) research, this study advances the conceptualisation of interactive diffusion by categorising the five mechanisms according to the identity of the initiator: (a) sender-driven (direct mechanisms) and (b) adopter-driven (indirect mechanisms). Given this study's focus on how the EU induces the adoption of its regulatory frameworks, direct mechanisms are defined as EU-driven, while indirect mechanisms are shaped by recipient actors. Specifically, the incentive is a direct mechanism that includes both positive instruments (e.g., financial support or technical assistance) and negative pressures (e.g., penalties or sanctions) imposed by the senders to promote the uptake of diffusion items (Chen & Gao, 2024; Risse, 2016). The second direct mechanism is socialisation, commonly understood as the process by which actors internalise such items through sustained interaction with external agents or institutions (Risse, 2016; Strang & Meyer, 1993). Given that this study focuses on the EU's effort to actively induce the adoption of its regulatory frameworks in external jurisdictions, it deliberately adopts a more sender-driven interpretation of socialisation, consistent with Risse's (2016) definition. Accordingly, socialisation is conceptualised in this research as a sender-driven, one-way process.

The remaining three mechanisms—competition, learning, and emulation—are classified as indirect mechanisms. Competition refers to the process by which actors adopt the diffusion items to gain advantages or avoid falling behind rivals in the competitive environment (e.g., economic competition, technological innovation, or security threats; Meseguer & Gilardi, 2009). While learning and emulation share conceptual similarities, they differ in the degree of reflexivity. Learning involves a reflective process in which actors selectively adopt or localise diffusion items perceived as effective or contextually appropriate (Shipan & Volden, 2008). In contrast, emulation is a more superficial process in which actors replicate diffusion items with minimal adaptation, motivated by the perceived legitimacy or success of prior adopters (Simmons & Elkins, 2004). Table 2 outlines the five diffusion mechanisms and the indicators used to identify them in the case studies.

Table 2. Diffusion mechanisms and indicators.

Diffusion mechanisms		Indicators
EU-driven mechanisms	Incentive	Positive: • Foreign direct investment (FDI) • Development aid and technical assistance Negative: • Trade restrictions targeting non-compliant countries • Threats of fines or financial penalties
	Socialisation	• Membership in international organisations and forums • Diplomatic engagements and bilateral dialogues
Recipient-driven mechanisms	Competition	• Regional rivalries and competitive adaptation • Legal convergence to enhance the business environment
	Learning	• Explicit references to foreign models in policy debates • Government-sponsored comparative studies
	Emulation	• Replication of foreign legal texts without domestic adaptation

Note: Mechanisms and indicators are summarised from key studies in diffusion literature (see references cited in the theoretical framework).

3. Methodology

This article employs a case-study approach to analyse the evolution of the EU's diffuse-ability in two Asian countries—Japan and Singapore—over the past three decades (1990s–2020s). It further investigates the diffusion mechanisms underlying this process. This research is based on a combination of open-source primary materials, including official policy documents, cooperation agreements, and declarations, complemented by secondary sources such as policy analysis, white papers, and academic journal articles published between the 1980s and the 2020s.

This section explains how the core analytical units—referred to as "EU elements"—were extracted from EU legal instruments and categorised into six provision types. It then outlines the case selection strategy and comparative logic, using Mill's (1843) method of difference and the most similar systems design (MSSD).

3.1. The Categories of Provision Type and EU Elements

To facilitate a systematic comparison of data protection regimes across jurisdictions, this study categorises legal provisions into six functional types, reflecting widely recognised building blocks of data protection frameworks. These include: (a) scope and definitions; (b) data processing; (c) data subject rights; (d) obligations of data controllers/processors; (e) cross-border data transfers; and (f) supervisory authorities and enforcement. This typology is informed by the regulative profile approach to legal analysis, which focuses on the structural and functional roles of legal provisions within a broader regulatory architecture (Francesconi & Passerini, 2007).

Based on this categorisation, the study identifies a set of "EU elements"—previously introduced as the diffusion items in this research—as the core analytical indicators for assessing regulatory convergence. These elements refer to specific concepts and legal requirements that were first introduced or uniquely developed within the EU's data protection instruments, ranging from Convention 108 and the 1995 Directive to the GDPR. Following Greenleaf's (2012) methodology of identifying "European elements" as benchmarks for convergence assessment, this study draws on a close reading of EU legal texts and existing diffusion literature to extract key elements. These are then organised under the six provision types described above and serve as the primary criteria for evaluating the extent of EU influence in the domestic data regulations of Japan and Singapore. Table 3 provides an overview of these provision types, including their definitions and corresponding EU elements.

3.2. Case Selection: Japan and Singapore

This study adopts a comparative case-study design, specifically employing an MSSD grounded in the logic of Mill's (1843) method of difference. MSSD has been widely used in IR research, particularly in small-n comparative case studies that aim to identify causal mechanisms under conditions of limited variation (Lai, 2024). The method of difference involves comparing cases that are similar in most respects but differ in both outcomes and at least one potential causal factor (Mills et al., 2010, pp. 558–559). It enables researchers to isolate explanatory variables by holding background conditions constant. Furthermore, the method of difference can be applied not only across cases but also within a single case over time, thereby enabling a dynamic analysis of policy evolution under otherwise stable structural conditions.

Table 3. Provision types and EU elements.

Provision types	Definitions	EU elements
Scope and definitions	Defines the jurisdictional scope of the regulation and clarifies key legal terms	• Protection of fundamental rights and freedoms, particularly the right to personal data protection • Geographic applicability of data regulations • Concept of sensitive data • Concept of anonymised data • Concept of pseudonymised data
Data processing	Covers principles and rules governing the collection, use, storage, and sharing of personal data	• General requirement of "fair and lawful processing" • Data collection must be limited to what is necessary for the stated purpose • Obligation to destroy or anonymise personal data after a retention period • Restrictions on automated decision-making
Data subject rights	Defines the ability of individuals to exercise control over their personal data	• Right to opt-out of direct marketing uses of personal data • Right to understand the logic behind automated data processing • Requirements to inform the DPA within 72 hours of a data breach and notify individuals if their rights are at risk
Obligations of controllers/processors	Specifies the responsibilities of data controllers and processors, including their roles in managing and executing data processing	• Additional safeguards required for processing sensitive data • Obligation to notify, and in some cases conduct prior checking of, certain types of data processing
Cross-border data transfers	Covers the rules governing the transfer of personal data to third countries or international organisations	• Restrictions on data transfers to countries lacking adequate privacy protection standards
Supervisory authorities and enforcement	Outlines the structure and powers of regulatory bodies and the mechanisms for enforcement	• Requirement of an independent Data Protection Authority • Access to judicial remedies for the enforcement of data privacy rights

Accordingly, Japan and Singapore are selected as two high-exposure, economically advanced Asian states with mature data governance systems and strong relations with the EU. Despite these similarities, they display divergent levels of regulatory convergence with the EU data standards. To trace the mechanisms underlying these divergent trajectories, the study further employs a process tracing approach. Process tracing is a qualitative method used to identify and test causal mechanisms within individual cases (Collier, 2011). It helps establish a temporal link between cause and outcome through detailed within-case analysis (Beach & Pedersen, 2016). In this study, process tracing is applied separately to Japan and Singapore to examine how their domestic data protection regimes evolved from the 1990s to the 2020s, and how EU elements were selectively adopted or resisted over time.

3.3. Case Contexts of Japan and Singapore

In the 1990s, the EU recognised the growing strategic importance of Asia and sought to strengthen ties with Asian countries and regional organisations. The 1994 policy paper Towards a New Asia Strategy and its subsequent updates emphasised expanding bilateral and multilateral cooperation in areas such as trade, technology, and rule-based global governance (European Commission, 2001). As a result, the EU established multiple dialogue mechanisms and signed cooperation agreements with key Asian actors, including Japan, South Korea, and ASEAN. This study selects Japan and Singapore as two geographically diverse, economically advanced Asian states with extensive relations with the EU, to assess the diffusion of EU data protection regulations. The following section provides a brief overview of their data governance trajectories, EU relations, and the temporal benchmarks used in the analysis.

Japan, the world's fourth-largest economy by nominal GDP, maintains strong cooperation with the EU across various domains. The EU is Japan's third-largest trading partner, while Japan ranks as the EU's second-largest in Asia (European Commission, 2024a). Japan was the first country in Asia to enact a privacy law in the late 1990s, initially focused on protecting personal data held by public agencies (Suda, 2020), followed by the adoption of the Act on the Protection of Personal Information (APPI) in the early 2000s to cover the private sector (Adams et al., 2009). As a key EU strategic partner, Japan offers a valuable case for examining the EU's diffuse-ability in data governance. This study divides Japan's regulatory evolution into three periods—2005, 2016, and 2022—each corresponding to major EU developments. It systematically assesses the extent of convergence, identifying specific provisions that incorporate EU elements, and explores the mechanisms that enabled such diffusion.

Singapore, a leading city-state in Southeast Asia, ranks second globally in GDP per capita as of 2023 (WorldData.info, 2024). It is the EU's top trading partner in ASEAN and a major investment destination (European Commission, 2024b). While its engagement with data governance dates back nearly three decades, early efforts focused on voluntary codes such as the Model Data Protection Code for the Private Sector (2002 Model Code; Wong, 2017). Comprehensive legislation was not introduced until 2012, with the Personal Data Protection Act (PDPA) covering both public and private sectors (Singapore Attorney-General's Chambers, 2012). As the EU's most important ASEAN partner, Singapore presents a contrasting case for examining EU regulatory diffusion. The study identifies 2002, 2013, and 2022 as key reform milestones and evaluates the extent to which Singapore's regulations incorporated EU elements. It also investigates the mechanisms driving selective adoption and regulatory localisation.

By selecting Japan and Singapore as case studies, this research captures both convergence and variation in EU influence across the Asian region. It finds that Japan pursued deeper alignment, culminating in GDPR adequacy recognition, while Singapore selectively adapted EU elements within a more flexible regulatory framework. Through cross-case comparison and within-case process tracing, the study identifies both outcome variation and the underlying diffusion mechanisms.

4. Case Study: Data Regulations in Japan and Singapore

This section evaluates the EU's diffuse-ability by examining whether, when, and how Japan and Singapore incorporated EU elements into their domestic data protection frameworks. As outlined in Table 1,

diffuse-ability is assessed based on observable diffusion outcomes—adoption, adaptation, resistance, or rejection—which reflect varying degrees of regulatory convergence.

Moreover, the analysis identifies and explains the underlying diffusion mechanisms that contributed to convergence where it occurred. Rather than assigning mechanisms to every stage of legal development, the study focuses on periods of clear convergence, where EU elements were substantially adopted or adapted. This approach allows for a more targeted and meaningful interpretation of how and under what conditions EU elements gain traction in domestic contexts. While a single mechanism may dominate in a given period, this study supports the insight in diffusion theory that multiple mechanisms often operate simultaneously and interact to shape diffusion outcomes.

4.1. Data Regulation in Japan: From the 1990s to the 2020s

This article argues that the EU's diffuse-ability in Japan has progressively increased over time, reaching its peak between 2006 and 2016, when significant regulatory convergence occurred. During this period, socialisation served as the primary diffusion mechanism driving this regulatory alignment.

To evaluate this trajectory, the analysis draws on the diffusion outcomes typology introduced earlier and uses the matrix in Table 4 to compare the adoption of EU elements across three key time points—2005, 2016, and 2022. This table tracks newly incorporated provisions reflecting EU elements and illustrates the cumulative trajectory of regulatory convergence.

Table 4. Convergence of data regulations of Japan's and EU's.

Provision type/year		2005		2016		2022	
		EU	Japan	EU	Japan	EU	Japan
Scope and definitions	Objectives	✓	✓	✓	1	✓	✓
Scope and definitions	Geographic applicability	✓	✓	✓	1	✓	✓
Scope and definitions	Definitions	✓	✓	✓	1	✓	✓
Data processing	Lawfulness, fairness, and transparency	✓		✓		✓	1
Data processing	Purpose limitation	✓	1	✓	✓	✓	✓
Data processing	Data minimisation	✓		✓	1	✓	✓
Data processing	Accuracy	✓	✓	✓	✓	✓	✓
Data processing	Storage limitation	✓		✓	1	✓	✓
Data processing	Integrity and confidentiality	✓	✓	✓	1	✓	✓
Data processing	Accountability	✓		✓	✓	✓	✓
Data subject rights	Consent before collecting	✓	1	✓	✓	✓	✓
Data subject rights	Access	✓	✓	✓	1	✓	✓
Data subject rights	Correction	✓	✓	✓	1	✓	✓
Data subject rights	Erasure			✓		✓	✓
Data subject rights	Restriction			✓		✓	

Table 4. (Cont.) Convergence of data regulations of Japan's and EU's.

Provision type/year		2005		2016		2022	
		EU	Japan	EU	Japan	EU	Japan
Data subject rights	Objection	✓		✓		✓	
Data subject rights	Portability			✓		✓	1
Obligations of data controllers/processors	Security measures	✓	1	✓	✓	✓	✓
Obligations of data controllers/processors	Breach notification	✓		✓	1	✓	✓
Obligations of data controllers/processors	Maintain records			✓	1	✓	✓
Obligations of data controllers/processors	Data Protection Impact Assessments (DPIAs)			✓		✓	
Obligations of data controllers/processors	Data Protection Officers (DPOs)	✓		✓		✓	
Cross-border data transfers	Consent	✓		✓	✓	✓	✓
Cross-border data transfers	Adequacy level of protection	✓		✓	1	✓	✓
Cross-border data transfers	Standard Contractual Clauses (SCCs)	✓		✓		✓	
Cross-border data transfers	Binding Corporate Rules (BCRs)	✓		✓		✓	
Supervisory authorities and enforcement	Independent supervisory authorities	✓		✓	1	✓	✓
Supervisory authorities and enforcement	Sanctions	✓	✓	✓	✓	✓	✓
Total score			3		12		2

Notes: A checkmark (✓) indicates that the provision was already present in the data regulation at each time point; a blank cell signifies the absence of the provision in the respective regulation; in the Japan provision columns, a score of 1 denotes the first instance where a specific EU element was incorporated, which signals a point of regulatory convergence; the cumulative total score reflects the aggregate number of newly adopted EU elements at each time point.

In the period prior to 2005, Japan integrated only three EU elements, each localised to fit domestic priorities—an outcome that corresponds to resistance, suggesting weak diffuse-ability. However, between 2005 and 2016, Japan introduced a significant number of new EU elements into its data regulations. Although adapted to local contexts, the scale and depth of convergence indicate adaptation and reflect mid-strong diffuse-ability. From 2016 to 2022, only two additional EU-aligned provisions were adopted, yet this should not be interpreted as declining EU influence. The matrix reflects only newly incorporated EU elements, allowing the analysis to highlight key regulatory shifts rather than cumulative harmonisation. Moreover, since legal reforms typically emerge from long-term regulatory and policy engagement, Japan's 2016 data protection reforms should not be seen as a direct response to the GDPR. Rather, they reflect a broader and more gradual alignment with the EU's data governance model—one that had already been shaped by earlier instruments such as Convention 108 and the 1995 Directive, which had exerted sustained influence on Japan's regulatory development over the preceding decades.

From the late-1990s to 2005, Japan's data regulations selectively adopted the basic concepts and principles of the EU's data regulations. More specifically, the 2003 APPI introduced three EU elements in its provisions, including "purpose limitation," "consent of the person before collecting and processing personal information,"

and "security controls" (Japan Ministry of Justice, 2003). These provisions were integrated into Japan's data regulations to address early domestic demands for fundamental data protection. During this period, although Japan's data laws were primarily recognised as being influenced by the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980 OECD Guidelines; Suda, 2020), Birnhack (2008) pointed out that Japan regarded the EU directive as a policy target in its 1998 governmental report and modelled the EU directive's basic data protection principles including purpose limitation, security controls, basic data subject rights, and consent before disclosing to third parties. Additionally, Horibe (2013) pointed out that Japan's data laws considered European legislation as early as the 1980s, with particular reference to Convention 108.

Subsequently, Japan's data regulations have demonstrated a high degree of convergence, gradually aligning with the EU's data regulations since 2005. First, in terms of scope and definitions, the amended 2015 APPI, issued by the Personal Information Protection Commission (PPC; 2016), broadened its scope to introduce the concept of "extraterritorial jurisdiction," meaning that certain provisions applied to business operators outside Japan, rather than being limited to domestic application, as stated in Article 75 of the 2015 APPI. The 2020 APPI further expanded its extraterritorial scope to include any business operators processing data related to Japanese residents, regardless of their geographic location (PPC, 2020, p. 45). Japan also incorporated EU elements into the definitions of key terms in its legislation. For instance, the 2015 APPI added the term "sensitive personal information," encompassing key elements such as an individual's "race, creed, social status, medical history, etc." (PPC, 2016, p. 3). This aligns with the concept of "sensitive data" as emphasised in both the EU Directive and Convention 108.

Regarding the provision type of data processing, Japan's data regulations have been revised since 2005 to align more closely with the EU's data processing principles. In addition to the previously adopted principle of "purpose limitation," the amended data regulations introduced the principles of "data minimisation," "storage limitation" and "integrity and confidentiality" in the 2015 APPI (PPC, 2016, pp. 6–9). For instance, under Article 19 of the APPI (Maintenance of the Accuracy of Data), business operators are required to collect personal data "within the scope necessary for achieving the purpose of use" and to "delete such personal data without delay when its use is no longer required" (PPC, 2016, p. 9), thereby incorporating identified EU elements. The 2015 APPI also introduced a new security measure, "de-identified information" (a concept similarly referenced in the 2012 GDPR proposal), to help prevent the leakage, loss, or damage of processed personal data and to enhance data confidentiality (European Commission, 2012; PPC, 2016). Furthermore, the 2020 APPI introduced a new provision to specifically emphasise the principle of "lawfulness and fairness" (PPC, 2020, p. 9).

Additionally, although Japan's data regulations prioritise economic objectives over recognising the right to data privacy as a fundamental human right, as is emphasised in the EU's approach (Wang, 2020), the amended APPI still revised its provision related to the data subject rights to better align with the EU regulations. For instance, the 2015 APPI revised its provisions related to rights to access, correction, and deletions, and required business operators to provide "the name of the business operator handling personal information, the purpose of use of all retained personal data, etc." upon a data subject's request and must "respond without delay" (PPC, 2016, p. 12). In alignment with the GDPR, the 2020 APPI introduced "data portability rights," as outlined in Article 28 (PPC, 2020). In terms of obligations of data controllers/processors, the 2015 and 2020 APPI respectively introduced and revised the requirements for "timely

breach notifications" and mandated that business operators maintain records of data processing activities both domestically and internationally (PPC, 2016, pp. 8–11; 2020, pp. 10–12).

Finally, Japan's amended data regulations introduced specific provisions related to cross-border data transfers, as well as establishing an independent supervisory authority to ensure an adequate level of personal data protection (PPC, 2016, 2020). These changes were also intended to meet the EU's requirements and to address the challenges posed by the globalisation of data flows (Council of Europe, 1981; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995, 1995; Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016, 2016). Specifically, the Act required business operators to obtain the prior consent of individuals before transferring personal data to third parties outside Japan, while stipulating that the receiving country maintain a "level of protection for the rights and interests of individuals" equivalent to that in Japan (PPC, 2016, p. 11, 2020). Meanwhile, the amended regulations also established the PPC to align with the broader trend of strengthening independent supervisory authorities and to fulfil the EU's adequacy criteria under its data protection framework (Horibe, 2013; Ishiara, 2019).

In sum, Japan's convergence with EU data regulations has been gradual but increasingly substantial, particularly between 2005 and 2016. Regulatory alignment is most evident in foundational areas such as the categories of scope and definitions and data processing, where multiple EU elements have been incorporated and localised. These patterns suggest that the EU's diffuse-ability in Japan has strengthened over time. To understand how this process unfolded, the following section turns to the diffusion mechanisms that underpin Japan's regulatory transformation.

As mentioned at the beginning of Section 4, multiple diffusion mechanisms often operate simultaneously and interactively, making it difficult to isolate them with precision. To guide the identification of the primary mechanisms during key stages of convergence, Table 5 presents the key indicators used to identify the mechanisms of learning and socialisation, along with their corresponding behavioural patterns. While learning played a notable role during the early phase of Japan's data governance in the 1990s and 2000s, much of the evidence observed—particularly during the period of regulatory convergence—corresponds more closely to indicators associated with socialisation. Accordingly, the remainder of this section focuses on explaining how socialisation served as the primary mechanism underpinning the diffusion process.

Table 5. The mechanisms behind the diffusion process in Japan.

Diffusion mechanisms	Indicators	Examples of appropriate behaviour
Learning	Explicit references to foreign models in policy debates	• During the drafting of the 2003 APPI, Japanese officials explicitly referenced the EU's Convention 108 and the 1995 Directive
Socialisation	Membership in international organisations and forums	• Japan's accession to the OECD in 1964 enabled its participation in drafting the 1980 Guidelines and laid the groundwork for later cooperation with EU member states
	Diplomatic engagements and bilateral dialogue	• The EU and Japan signed the 1991 Joint Declaration on Relations between the European Community and its Member States and Japan • Negotiations for the EU–Japan Economic Partnership Agreement (EPA)

First, this study argues that Japan's accession to the OECD in 1964 played a foundational role in shaping its long-term engagement with European regulatory models. Through active participation in the drafting of the 1980 OECD Guidelines, Japan became familiar with data protection principles that closely aligned with EU standards. This early exposure contributed not only to the subsequent incorporation of selected EU elements into Japan's data laws but also laid the groundwork for establishing scientific and technological cooperation and trade relations with founding members of the OECD—primarily EU member states. In a 2013 speech marking the establishment of the PPC, Masao Horibe, then Chair of the PPC and a key figure in drafting the APPI, explicitly acknowledged that Japan's data regulations drew upon the EU's data regulations. Notably, Horibe had also served as a member of the OECD expert group responsible for drafting the 1980 Guidelines, which were themselves heavily influenced by European privacy principles (Kirby, 2017). His dual involvement reflects both the learning mechanism, whereby EU elements were selectively incorporated into Japan's legal framework, and the socialisation mechanism, whereby sustained participation in international forums facilitated normative engagement. These expert-level, rule-setting interactions promoted the diffusion of norms and standards not through coercion or conditionality, but through shared participation in the transnational shaping of data governance principles. Moreover, Japan signed bilateral cooperation agreements with EU member states, such as Germany and France, emphasising collaboration in science and technology (Ministry of Foreign Affairs of Japan, 1999, 2023). Japan also engaged in both inward and outward FDI with the UK in 1983 and expanded the activities to include Germany, France, and Italy since 1987 (Japan External Trade Organization, 2024). These longstanding ties with European partners not only laid the foundation for later Japan-EU cooperation but also created a context of increasing economic and normative proximity that eventually facilitated Japan's regulatory convergence with the EU in the digital era.

Second, this study observes that since the 1990s, the EU has primarily leveraged bilateral cooperation to encourage Japan to adopt its diffusion items, reinforcing regulatory alignment in data governance. Building on Japan's collaborations with EU member states, the EU further established a partnership with Japan across various sectors, including trade, policymaking, and technology. For instance, the 1991 Joint Declaration on Relations between the European Community and its Member States and Japan (Ministry of Foreign Affairs of Japan, 1991) was signed by Japan and the EU, serving as a formal framework for cooperation and dialogue between the two parties. Furthermore, the two parties launched the Action Plan for EU–Japan Cooperation, in which the EU further promoted the principles of "respect for human rights," "promotion of democracy," and "good governance" (Ministry of Foreign Affairs of Japan, 2001).

Moreover, Japan and the EU have expanded their cooperation due to the rapid development of ICTs. Under the EU–Japan Science and Technology Agreement (European Commission, 2009), both parties confirmed new cooperation in Future Internet/New Generation Networks research—a key element of the Digital Agenda for Europe—during the 2011 EU–Japan Dialogue (European Commission, 2011). Additionally, since 2013, negotiations for the EU–Japan EPA have been launched, covering a range of issues including cross-border data flows and regulation cooperation (European Parliament, 2019). During the 22nd EU–Japan Summit (European External Action Service, 2014) and the first EU–Japan Cyber Dialogue (Ministry of Foreign Affairs of Japan, 2014), the EU and Japan discussed governmental structures and principles related to cyber regulations to address the increasing challenges of cybersecurity. As Japan–EU cooperation deepened, the European Commission and Japan engaged in negotiations on adequate data protection levels based on the EPA (European Commission, 2018). These collaborations created channels for

sustained normative interaction, progressively familiarising Japanese regulators with European regulatory standards and expectations and facilitating the adaptation of EU elements.

In sum, although diffusion is a highly complex process involving the interaction of multiple diffusion mechanisms, it is undeniable that socialisation has played a predominant role in Japan's gradual adoption of EU elements in the evolution of its domestic data regulations.

4.2. Data Regulations in Singapore: From the 1990s to the 2020s

This study argues that the EU's diffuse-ability in Singapore has remained weak over time, with only limited incorporation of EU elements across three decades of regulatory development. The overall pattern suggests that convergence has been marginal, with competition emerging as the primary diffusion mechanism.

To examine the EU's diffuse-ability in Singapore, this study applies the diffusion outcomes typology to trace the evolution of regulatory convergence. Table 6 compares key developments in EU and Singaporean data regulations from the 1990s to the 2020s. The number of newly adopted EU elements remained low and relatively stable across the three periods examined (2003, 2012, and 2022), with no clear upward trajectory. These findings suggest that the EU's diffuse-ability in Singapore has remained consistently weak, with most diffusion outcomes falling into the category of resistance.

Table 6. Convergence of data regulations of Singapore's and EU's.

Provision type/year		2002		2013		2022	
		EU	Singapore	EU	Singapore	EU	Singapore
Scope and definitions	Objectives	✓	✓	✓	✓	✓	✓
Scope and definitions	Geographic applicability	✓	1	✓	✓	✓	✓
Scope and definitions	Definitions	✓		✓	✓	✓	✓
Data processing	Lawfulness, fairness, and transparency	✓	✓	✓	✓	✓	✓
Data processing	Purpose limitation	✓	1	✓	✓	✓	✓
Data processing	Data minimisation	✓	1	✓	✓	✓	✓
Data processing	Accuracy	✓	✓	✓	✓	✓	✓
Data processing	Storage limitation	✓		✓	✓	✓	✓
Data processing	Integrity and confidentiality	✓		✓	✓	✓	✓
Data processing	Accountability	✓	✓	✓	✓	✓	✓
Data subject rights	Consent before collecting	✓	✓	✓	✓	✓	✓
Data subject rights	Access	✓	✓	✓	✓	✓	✓
Data subject rights	Correction	✓	✓	✓	✓	✓	✓
Data subject rights	Erasure					✓	✓
Data subject rights	Restriction					✓	
Data subject rights	Objection	✓		✓	1	✓	

Table 6. (Cont.) Convergence of data regulations of Singapore's and EU's.

Provision type/year		2002		2013		2022	
		EU	Singapore	EU	Singapore	EU	Singapore
Data subject rights	Portability					✓	1
Obligations of data controllers/processors	Security measures	✓	✓	✓	✓	✓	✓
Obligations of data controllers/processors	Breach notification	✓		✓		✓	1
Obligations of data controllers/processors	Maintain records				✓	✓	✓
Obligations of data controllers/processors	DPIAs					✓	
Obligations of data controllers/processors	DPOs	✓		✓	1	✓	✓
Cross-border data transfers	Consent	✓	✓	✓	✓	✓	✓
Cross-border data transfers	Adequacy level of protection	✓	1	✓	✓	✓	✓
Cross-border data transfers	SCCs	✓		✓		✓	
Cross-border data transfers	BCRs	✓		✓		✓	
Supervisory authorities and enforcement	Independent supervisory authorities	✓		✓	1	✓	✓
Supervisory authorities and enforcement	Sanctions	✓		✓	✓	✓	✓
Total score			4		3		2

Notes: A checkmark (✓) indicates that the provision was already present in the data regulation at each time point; a blank cell signifies the absence of the provision in the respective regulation; in the Singapore provision columns, a score of 1 denotes the first instance where a specific EU element was incorporated, signalling a point of regulatory convergence; the cumulative total score reflects the aggregate number of newly adopted EU elements at each time point.

During the first period, Singapore's data code incorporated four EU elements and adapted them into domestic data regulations. First, in terms of scope and definitions, Singapore's data regulations began to consider the "territorial scope," which aligned with the EU Directive, as the 2002 Model Code specified that it would apply to "any personal data processed in Singapore, whether the data controller is within Singapore" (National Internet Advisory Committee, 2002, pp. 30–31). Second, in relation to data processing provisions, the 2002 Model Code introduced two principles: "identifying purposes" (Clause 4.2) and "limiting collection" (Clause 4.4), which correspond to the EU elements of "purpose limitation" and "data minimisation" (National Internet Advisory Committee, 2002, pp. 61-67). Specifically, the Code stated that organisations should inform individuals of the purpose "at or before the time of collection" and that the data should not be used for a new purpose (National Internet Advisory Committee, 2002, p. 61). The principle of "limiting collection" required organisations to ensure that the data collected "shall be limited to that which is necessary for the identified purposes" (National Internet Advisory Committee, 2002, p. 67). Additionally, the 2002 Model Code introduced provisions for cross-border transfers, aligning with the EU's regulations. The principle of

"transborder data flows" required organisations to ensure "an adequate level of protection" when transferring data to "any recipient outside Singapore" (National Internet Advisory Committee, 2002, p. 31). Although the 2002 Model Code was a voluntary code designed to align with Article 25 under the framework of the EU Directive, its principles were carried forward into subsequent data regulations. Moreover, in the evolution of Singapore's data regulations, the 2002 Model Code has been regarded as a transitional step toward enacting mandatory legislation to keep pace with global digitalisation (Wong YongQuan, 2017).

During the second period, Singapore enacted its formal data protection law, the 2012 PDPA, which incorporated three provisions containing EU elements. More specifically, Singapore introduced the provision of "withdrawal of consent," meaning that individuals can "withdraw any consent given" at any time, while organisations are required to inform them of the "likely consequences" (Singapore Attorney-General's Chambers, 2012, p. 20). This provision is comparable to the "right to object" under the EU data protection framework. Regarding obligations of data controllers/processors, the 2012 PDPA aligned with the EU Directive by requiring organisations to designate one or more "reasonable persons" to ensure that data is collected and processed in compliance with relevant data protection regulations (see Article 11, Singapore Attorney-General's Chambers, 2012). Finally, Singapore established the Personal Data Protection Commission (PDPC) in 2013 as an independent supervisory authority responsible for administering the PDPA and providing advisory guidelines to individuals and organisations (Singapore Attorney-General's Chambers, 2012). As mentioned earlier, the "requirement of an independent data protection authority" is a key regulatory component emphasised by the EU (Greenleaf, 2012, p. 73). Thus, this development reflects an alignment with EU data regulations and the evolving global landscape of data governance.

Finally, during the third period, Singapore incorporated only two EU elements, adapting them to fit its domestic regulatory framework. This limited adoption further reflects the EU's persistently weak diffuse-ability in Singapore. More specifically, the 2020 PDPA introduced the "notification of data breach" requirement, mirroring the GDPR's provision that organisations must notify the PDPC "no later than three calendar days" and inform affected individuals as soon as possible (Personal Data Protection Commission, 2020, p. 35). Additionally, the amended PDPA incorporated the concept of "anonymised information," first introduced in the 2012 GDPR proposal and later adopted in the final regulation. In alignment with EU data regulations, the PDPA provides that "re-identification is not authorised by the organisation or public agency" (Personal Data Protection Commission, 2020, p. 59).

Overall, by tracing the evolution of Singapore's data regulations, this research finds that the EU's diffuse-ability in Singapore has remained persistently weak. Moreover, the EU elements adopted in Singapore's data regulations are primarily concentrated in the provision types of "data processing" and "cross-border data transfer," particularly provisions governing cross-border data flows.

In terms of diffusion mechanisms, this study finds that while multiple mechanisms operated concurrently, their effects were uneven. Some signs of socialisation—such as bilateral cooperation with the EU and participation in ASEAN-led regional initiatives—became more visible after the 2010s, but did not lead to greater regulatory convergence. In fact, most EU elements were adopted between the 1990s and the 2010s, indicating that socialisation had limited influence on the timing of adoption. Instead, the evidence points to competition as the dominant mechanism. Singapore's strategic aim to position itself as a global trade and data hub, along with regulatory competition with regional actors, better explains its selective adoption of EU elements. This strategic logic is elaborated in the following analysis and summarised in Table 7.

Table 7. The mechanism behind the diffusion process in Singapore.

Diffusion mechanisms	Indicators	Examples of appropriate behaviour
Competition	Legal convergence to enhance the business environment	• Singapore aimed to be the international e-commerce hub • Singapore referenced multiple national data protection regimes in its working papers
	Regional rivalries and competitive adaptation	• Hong Kong enacted the Personal Data (Privacy) Ordinance (PDPO) in 1996

First, this study observes that Singapore's establishment and modification of its data governance framework have been primarily driven by its goal to facilitate cross-border business operations and attract foreign investment. In the early 1990s, Singapore recognised the importance of data protection regulations, and the Singapore Academy of Law issued a working paper stating that the primary objective of the legislation was to strike a balance between the "interests of data subjects, data users and the wider community" (Wong, 2017, p. 288). Although this approach was later reflected in Singapore's data protection framework, the government initially opted to develop voluntary codes for the private sector—following a review of the international data protection landscape—rather than enacting formal legislation for both the public and private sectors (National Internet Advisory Committee, 2002; Wong, 2017). In 2002, the National Internet Advisory Committee Legal Subcommittee noted that the 1999 E-Commerce Code had failed to consider EU data regulations, particularly Article 25 of the EU Directive concerning transborder data flows (National Internet Advisory Committee, 2002). This neglect was seen as potentially undermining Singapore's competitive position in the rapidly evolving global e-commerce landscape.

Second, this study argues that the integration of EU elements into Singapore's data provisions is a result of regulatory adjustments in response to regional competition, enabling Singapore to maintain its economic and strategic advantages in an increasingly competitive digital economy. Singapore, one of Asia's major developed economies since the 1960s, has built its growth largely on its strategic geographic location and "entrepôt trade" (Hundt & Uttam, 2017). For instance, driven by proactive government policy initiatives and global technological developments, the ICT manufacturing sector has become a major economic pillar since the late 1980s. However, Singapore's ICT manufacturing remained heavily export-oriented, rendering it highly sensitive to fluctuations in the global ICT market (Vu, 2013). As one of the Asian Four Tigers alongside Singapore, Hong Kong shared a similar development model, leveraging its geographic advantages to foster international trade and economic growth (Paldam, 2003). To maintain its status as an "international trading centre," Hong Kong enacted the PDPO in 1996, drawing on the 1980 OECD Guidelines to ensure an "adequate level of data protection" (Office of the Privacy Commissioner for Personal Data of Hong Kong, 2024). Tang (2003) highlighted that the success of e-commerce depends heavily on "securing the confidence of consumers over the flow of personal data across territorial boundaries" and emphasised that data protection legislation is a "pre-requisite" for ensuring "an adequate level of data privacy protection" and gaining consumers' confidence.

However, Singapore lacked a comparable data protection framework necessary to ensure its position as a "trusted node" and sustain its status as an "international e-commerce hub" (National Internet Advisory Committee, 2002; Parliament of Singapore, 2012). This absence of an adequate data protection regime posed a particular challenge, given that the EU—Singapore's third-largest export market after Malaysia and

the US—could "place Singapore businesses at disadvantage in the global economy" (National Internet Advisory Committee, 2002, p. 13). Therefore, the National Internet Advisory Committee Legal Subcommittee incorporated EU data regulations into the development of Singapore's data protection framework, publishing the 2002 Model Code and the subsequent 2012 PDPA to address domestic economic demands. Although the PDPA formally recognises the "right of individuals to protect their personal data" (Singapore Attorney-General's Chambers, 2012, p. 12), it primarily emphasises two key objectives: "maintaining individuals' trust in organisations that manage data" at the domestic level and "enhancing Singapore's competitiveness and strengthening its position as a trusted business hub" at the international level (Parliament of Singapore, 2012).

Over the past two decades, the EU and Singapore have engaged in multilevel cooperation across political, economic, and digital domains, signing multiple agreements, including the EU-Singapore Free Trade Agreement and the EU–Singapore Digital Trade Agreements (European Commission, 2024b). Additionally, the EU and ASEAN have established longstanding cooperation and dialogue mechanisms across political, security, and economic areas. In particular, during the EU–ASEAN Commemorative Summit, the EU and its member states—acting under the Team Europe initiative—announced the mobilisation of €10 billion as part of the Global Gateway strategy to accelerate digital infrastructure investment in ASEAN countries (European Commission, 2022). These investments are not purely economic, rather, they involve sustained engagement with technical standards, data security framework, and regulatory practices, thereby providing channels for the gradual socialisation of the European data regulatory approach within ASEAN countries, including Singapore. However, there is limited evidence to support that such dynamics have driven the incorporation of additional EU elements into Singapore's data legislation. In other words, Singapore's data regulations do not show a pattern of increasing adoption of EU elements, despite intensified negotiations and cooperation.

In sum, since most EU elements were incorporated during the early stages of Singapore's data policy development, competition emerged as the dominant diffusion mechanism in this process.

5. Conclusion

This research examines the establishment and evolution of data protection regimes in Japan and Singapore over the past three decades, with a focus on how, when, and to what extent their domestic regulations have converged with the EU's data governance framework. By applying a provision-level analytical approach and identifying key EU elements, the analysis evaluated convergence as a diffusion outcome and accounted for variation through the lens of diffusion mechanisms. The findings reveal two distinct patterns: Japan gradually incorporated a large number of EU elements and demonstrated progressive structural alignment with the EU's data governance model, while Singapore adopted only selected EU elements, reflecting minimal convergence.

Theoretically, this research contributes to diffusion research by complementing existing literature that overemphasises EU-driven factors, such as market size, legal externalities, or normative superiority. This study highlights the role of recipient actors, emphasising how domestic context, strategic orientation, and institutional priorities shape the selective adoption—or rejection—of external regulatory models. It particularly draws attention to the normative tensions between the EU's rights-based data governance model and the market-oriented priorities of some recipient countries. While both Japan and Singapore engaged in adaptation rather than direct adoption, their regulatory trajectories diverged significantly. Japan's

reforms have progressively aligned with EU standards, incorporating stronger rights protections and supervisory structures. In contrast, Singapore initially relied on voluntary, non-legislative codes, such as the 2002 Model Code, to regulate data protection. As global regulatory standards evolved, it introduced the PDPA in 2012 to formalise its framework. However, the PDPA retained a business-oriented, flexible approach that prioritised trade facilitation and cross-border data flows. Rather than fully aligning with the EU's rights-based model, Singapore has continued to selectively adapt global standards in ways that support its competitive positioning as an international data hub. This contrast illustrates that regulatory convergence is not merely a function of external pressure, but a negotiated outcome shaped by the domestic logic of strategic regulatory positioning.

Empirically, this comparison reveals that the EU's regulatory power in global data governance is both conditional and uneven. Its influence depends not only on market size or legal sophistication but also on the institutional receptivity and strategic interests of recipient states. In Japan, longstanding institutional ties and economic interdependence created favourable conditions for socialisation and deeper regulatory convergence. In Singapore, by contrast, the need to remain agile and competitive, in a multipolar regulatory environment led to selective and instrumental alignment. These findings suggest that the diffusion of European standards should be understood not as a linear or automatic process, but as one shaped by reciprocal engagement, institutional filtering, and regulatory competition.

The findings also offer broader implications for future research on global diffusion. The mechanisms identified in this study are not exclusive to Japan and Singapore but are likely to influence regulatory outcomes across a wide range of emerging economies. As countries increasingly navigate between competing regulatory models, understanding how external norms and standards are domestically interpreted, adopted, or resisted is critical for capturing variation in convergence outcomes. Future studies could build on this framework by applying it to a broader set of cases and by examining how domestic political coalitions, legal traditions, and global alignments mediate the influence of external normative pressures in shaping data governance trajectories.

Acknowledgments

The author would like to thank the academic editors of this thematic issue, Dr Xuechen Chen and Dr Xinchuchu Gao, for their efforts in organising the issue and for their valuable feedback during the drafting process. Sincere thanks also go to Professor Benjamin Farrand for his insightful comments and to the three anonymous reviewers for their constructive and thoughtful suggestions.

Funding

The author would like to thank Northeastern University London for funding the open access publication of this article.

Conflict of Interests

The author declares no conflict of interests.

References

Adams, A. A., Murata, K., & Orito, Y. (2009). The Japanese sense of information privacy. *AI & Society*, *24*(4), 327–341. https://doi.org/10.1007/s00146-009-0228-z

Akcali Gur, B. (2020). The normative power of the EU: A case study of data protection laws of Turkey. *International Data Privacy Law*, *10*(4), 314–329. https://doi.org/10.1093/idpl/ipaa013

Beach, D., & Pedersen, R. B. (2016). *Causal case study methods: Foundations and guidelines for comparing, matching, and tracing*. University of Michigan Press. https://doi.org/10.3998/mpub.6576809

Bentotahewa, V., Hewage, C., & Williams, J. (2022). The normative power of the GDPR: A case study of data protection laws of South Asian countries. *SN Computer Science*, *3*, Article 183. https://doi.org/10.1007/s42979-022-01079-z

Birnhack, M. D. (2008). The EU Data Protection Directive: An engine of a global regime. *The Computer Law and Security Report*, *24*(6), 508–520. https://doi.org/10.1016/j.clsr.2008.09.001

Björkdahl, A., Chaban, N., Leslie, J., & Masselot, A. (2015). Introduction: To take or not to take EU norms? Adoption, adaptation, resistance, and rejection. In A. Björkdahl, N. Chaban, J. Leslie, & A. Masselot (Eds.), *Importing EU norms* (Vol. 8, pp. 1–9). Springer. https://doi.org/10.1007/978-3-319-13740-7_1

Bradford, A. (2020). *The Brussels effect: How the European Union rules the world*. Oxford University Press.

Bradford, A. (2023). *Digital empires: The global battle to regulate technology*. Oxford University Press.

Bradford, A., Chilton, A., & Linos, K. (2024). Dynamic diffusion. *Journal of International Economic Law*, *27*(3), 538–557. https://doi.org/10.1093/jiel/jgae034

Brunn, S. D. (2000). Towards an understanding of the geopolitics of cyberspace: Learning, re-learning and un-learning. *Geopolitics*, *5*(3), 144–149. https://doi.org/10.1080/14650040008407697

Cervi, G. V. (2022). Why and how does the EU rule global digital policy: An empirical analysis of EU regulatory influence in data protection laws. *Digital Society*, *1*(2), Article 18. https://doi.org/10.1007/s44206-022-00005-3

Chen, X., & Gao, X. (2024). Norm diffusion in cyber governance: China as an emerging norm entrepreneur? *International Affairs*, *100*(6), 2419–2440. https://doi.org/10.1093/ia/iiae237

Christou, G. (2010). European Union security logics to the East: The European neighbourhood policy and the Eastern partnership. *European Security*, *19*(3), 413–430. https://doi.org/10.1080/09662839.2010.526110

Collier, D. (2011). Understanding process tracing. *PS, Political Science & Politics*, *44*(4), 823–830. https://doi.org/10.1017/S1049096511001429

Corning, G. P. (2024). The diffusion of data privacy laws in Southeast Asia: Learning and the extraterritorial reach of the EU's GDPR. *Contemporary Politics*, *30*(5), 656–677. https://doi.org/10.1080/13569775.2024.2310220

Council of Europe. (1981). *Convention for the protection of individuals with regard to automatic processing of personal data* (European Treaty Series No. 108). https://rm.coe.int/1680078b37

Creemers, R. (2022). China's emerging data protection framework. *Journal of Cybersecurity*, *8*(1), Article tyac011. https://doi.org/10.1093/cybsec/tyac011

Deibert, R. J. (2008). The geopolitics of internet control: Censorship, sovereignty, and cyberspace. In A. Chadwick & P. N. Howard (Eds.), *Routledge handbook of internet politics* (pp. 323–336). Routledge. https://doi.org/10.4324/9780203962541

Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. (1995). *Official Journal of the European Union*, L 281. https://eur-lex.europa.eu/eli/dir/1995/46/oj/eng

Edwards, G. (2008). The construction of ambiguity and the limits of attraction: Europe and its neighbourhood policy. *Journal of European Integration*, *30*(1), 45–62. https://doi.org/10.1080/07036330801959465

Elkins, Z., & Simmons, B. (2005). On waves, clusters, and diffusion: A conceptual framework. *The Annals of the American Academy of Political and Social Science*, *598*(1), 33–51. https://doi.org/10.1177/0002716204272516

European Commission. (2001). *Europe and Asia: A strategic framework for enhanced partnerships* (COM(2001) 469 final). https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2001:0469:FIN:EN:PDF

European Commission. (2009, November 30). *European community signs a science & technology cooperation agreement with Japan* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_09_1844

European Commission. (2011). *Digital agenda: EU and Japan agree to strengthen cooperation in future internet research* (MEMO/11/432). https://ec.europa.eu/commission/presscorner/api/files/document/print/en/memo_11_432/MEMO_11_432_EN.pdf

European Commission. (2012). *Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* (COM(2012) 11 final). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52012PC0011

European Commission. (2018, September 5). *International data flows: Commission launches the adoption of its adequacy decision on Japan* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_18_5433

European Commission. (2022, December 14). *Global gateway: EU and its member states to mobilise €10 billion for South-East Asia* [Press release]. https://ec.europa.eu/commission/presscorner/detail/en/ip_22_7678

European Commission. (2024a). *Japan—EU trade relations with Japan: Facts, figures and latest developments*. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/japan_en

European Commission. (2024b). *Singapore: EU trade relations*. https://policy.trade.ec.europa.eu/eu-trade-relationships-country-and-region/countries-and-regions/singapore_en

European External Action Service. (2014, May 7). *22nd EU-Japan Summit joint press statement* [Press release]. https://eeas.europa.eu/archives/delegations/japan/en/resources/news-from-the-eu/news2014/20140507/210016/index.html

European Parliament. (2019). *EU-Japan Economic Partnership Agreement (EPA)*. https://www.europarl.europa.eu/legislative-train/theme-international-trade-inta/file-eu-japan-epa

Francesconi, E., & Passerini, A. (2007). Automatic classification of provisions in legislative texts. *Artificial Intelligence and Law*, *15*(1), 1–17. https://doi.org/10.1007/s10506-007-9038-0

Gilardi, F., & Wasserfallen, F. (2019). The politics of policy diffusion. *European Journal of Political Research*, *58*(4), 1245–1256. https://doi.org/10.1111/1475-6765.12326

Graham, E. R., Shipan, C. R., & Volden, C. (2013). The diffusion of policy diffusion research in political science. *British Journal of Political Science*, *43*(3), 673–701. https://doi.org/10.1017/S0007123412000415

Greenleaf, G. (2012). The influence of European data privacy standards outside Europe: Implications for globalization of Convention 108. *International Data Privacy Law*, *2*(2), 68–92. https://doi.org/10.1093/idpl/ips006

Hopkins, W., & McNeill, H. (2015). Exporting hard law through soft norms: New Zealand's reception of European standards. In A. Björkdahl, N. Chaban, J. Leslie, & A. Masselot (Eds.), *Importing EU norms* (pp. 153–172). Springer. https://doi.org/10.1007/978-3-319-13740-7_8

Horibe, M. (2013). *Privacy culture and data protection laws in Japan* [Speech transcript]. Personal Information Protection Commission. https://www.ppc.go.jp/files/pdf/290928_en_horibespeech.pdf

Hundt, D., & Uttam, J. (2017). *Varieties of capitalism in Asia: Beyond the development state*. Palgrave Macmillan. https://doi.org/10.1057/978-1-349-58974-6_5

Ishiara, T. (2019). Japan. In A. C. Raul (Ed.), *The privacy, data protection and cybersecurity law review* (6th ed.,

pp. 233–250). Law Business Research Ltd. https://datamatters.sidley.com/wp-content/uploads/sites/2/2019/11/The-Privacy-Data-Protection-and-Cybersecurity-Law-Review-Edition-6.pdf

Japan External Trade Organization. (2024). *Japanese trade and investment statistics*. https://www.jetro.go.jp/en/reports/statistics.html

Japan Ministry of Justice. (2003). *Act on the protection of personal information* (Act No. 57 of May 30, 2003). Japanese Law Translation. https://www.japaneselawtranslation.go.jp/en/laws/view/130

Kirby, M. (2017). Privacy today: Something old, something new, something borrowed, something blue. *Journal of Law, Information and Science*, *25*(1), 1–25. https://www.austlii.edu.au/au/journals/JlLawInfoSci/2017/1.html

Klingler-Vidra, R., & Schleifer, P. (2014). Convergence more or less: Why do practices vary as they diffuse? *International Studies Review*, *16*(2), 264–274. https://doi.org/10.1111/misr.12137

Kuneva, M. (2009). *Meglena Kuneva—European Consumer Commissioner—Keynote Speech—Roundtable on online data collection, targeting and profiling* [Speech transcript]. European Commission. https://ec.europa.eu/commission/presscorner/detail/en/SPEECH_09_156

Lai, D. (2024). Reimagining comparisons in international relations through reflexivity. *International Studies Review*, *26*(4), Article viae043. https://doi.org/10.1093/isr/viae043

Manners, I. (2002). Normative power Europe: A contradiction in terms? *Journal of Common Market Studies*, *40*(2), 235–258. https://doi.org/10.1111/1468-5965.00353

Meseguer, C., & Gilardi, F. (2009). What is new in the study of policy diffusion? *Review of International Political Economy*, *16*(3), 527–543. https://doi.org/10.1080/09692290802409236

Mill, J. S. (1843). *A system of logic, ratiocinative and inductive: Being a connected view of the principles of evidence, and methods of scientific investigation*. J. W. Parker. https://doi.org/10.5962/bhl.title.25118

Mills, A. J., Durepos, G., & Wiebe, E. (Eds.). (2010). *Method of difference*. In *Encyclopedia of case study research* (pp. 558–559). Sage. https://doi.org/10.4135/9781412957397.n206

Ministry of Foreign Affairs of Japan. (1991). *Joint declaration on relations between the European Community and its member states and Japan*. https://www.mofa.go.jp/region/europe/eu/overview/declar.html

Ministry of Foreign Affairs of Japan. (1999, December 16). *Japan–France bilateral summit between Prime Ministers Obuchi and Jospin*. https://www.mofa.go.jp/region/europe/france/visit9912/joint/index.html

Ministry of Foreign Affairs of Japan. (2001). *An action plan for EU–Japan cooperation*. https://www.mofa.go.jp/mofaj/area/eu/kodo_k_e.html#1-3

Ministry of Foreign Affairs of Japan. (2014, October 3). *First meeting of Japan–EU cyber dialogue* [Press release]. https://www.mofa.go.jp/press/release/press4e_000447.html

Ministry of Foreign Affairs of Japan. (2023, February 3). *The 24th Japan–Germany joint committee meeting on science and technology cooperation* [Press release]. https://www.mofa.go.jp/press/release/press3e_000540.html

National Internet Advisory Committee. (2002). *Report on a model data protection code for the private sector*. https://www.agc.gov.sg/docs/default-source/publications/law-reform-reports/2002_report-on-a-model-data-protection-code-for-the-private-sector.pdf

O'Hara, K., & Hall, W. (2021). *Four internets: Data, geopolitics, and the governance of cyberspace*. Oxford University Press. https://doi.org/10.1093/oso/9780197523681.001.0001

Office of the Privacy Commissioner for Personal Data of Hong Kong. (2024). *The personal data (privacy) ordinance*. https://www.pcpd.org.hk/english/data_privacy_law/ordinance_at_a_Glance/ordinance.html

Paldam, M. (2003). Economic freedom and the success of the Asian tigers: An essay on controversy. *European Journal of Political Economy*, *19*(3), 453–477. https://doi.org/10.1016/S0176-2680(03)00012-0

Palmer, M. (2006, November 3). Data is the new oil. *ANA Marketing Maestros Blog*. https://ana.blogs.com/maestros/2006/11/data_is_the_new.html

Parliament of Singapore. (2012). *Personal data protection bill*. https://sprs.parl.gov.sg/search/email/link/?id=023_20121015_S0003_T0002&fullContentFlag=false

Personal Data Protection Commission. (2020). *Personal data protection (amendment) act 2020*. Singapore Statutes Online. https://sso.agc.gov.sg/Acts-Supp/40-2020

Personal Information Protection Commission of Japan. (2016). *Act on the Protection of Personal Information (APPI)*. https://www.ppc.go.jp/files/pdf/280222_amendedlaw.pdf

Personal Information Protection Commission of Japan. (2020). *Act on the Protection of Personal Information (APPI)*. https://www.ppc.go.jp/files/pdf/APPI_english.pdf

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 (General Data Protection Regulation). (2016). *Official Journal of the European Union*, L 119/1. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Risse, T. (2016). The diffusion of regionalism. In T. A. Börzel & T. Risse (Eds.), *The Oxford handbook of comparative regionalism* (pp. 87–108). Oxford University Press.

Schimmelfennig, F., & Sedelmeier, U. (2004). Governance by conditionality: EU rule transfer to the candidate countries of Central and Eastern Europe. *Journal of European Public Policy*, *11*(4), 661–679. https://doi.org/10.1080/1350176042000248089

Shipan, C. R., & Volden, C. (2008). The mechanisms of policy diffusion. *American Journal of Political Science*, *52*(4), 840–857. https://doi.org/10.1111/j.1540-5907.2008.00346.x

Simmons, B. A., Dobbin, F., & Garrett, G. (2008). *The global diffusion of markets and democracy*. Cambridge University Press.

Simmons, B. A., & Elkins, Z. (2004). The globalization of liberalization: Policy diffusion in the international political economy. *The American Political Science Review*, *98*(1), 171–189. https://doi.org/10.1017/S0003055404001078

Singapore Attorney-General's Chambers. (2012). *Personal Data Protection Act 2012* (No. 26 of 2012). https://sso.agc.gov.sg/Act/PDPA2012/Historical/20130102?DocDate=20121203&ValidDate=20130102

Solingen, E. (2012). Of dominoes and firewalls: The domestic, regional, and global politics of international diffusion. *International Studies Quarterly*, *56*(4), 631–644. https://doi.org/10.1111/isqu.12034

Strang, D., & Meyer, J. W. (1993). Institutional conditions for diffusion. *Theory and Society*, *22*(4), 487–511. https://doi.org/10.1007/BF00993595

Suda, Y. (2020). Japan's personal information protection policy under pressure: The Japan-EU data transfer dialogue and beyond. *Asian Survey*, *60*(3), 510–533. https://doi.org/10.1525/AS.2020.60.3.510

Tang, R. (2003). *A short paper on implementing data privacy principles: How are governments making it work in the real world?* Office of the Privacy Commissioner for Personal Data, Hong Kong. https://www.pcpd.org.hk/english/news_events/speech/apec_feb03.html

Vu, K. M. (2013). Information and communication technology (ICT) and Singapore's economic growth. *Information Economics and Policy*, *25*(4), 284–300. https://doi.org/10.1016/j.infoecopol.2013.08.002

Wang, F. Y. (2020). Cooperative data privacy: The Japanese model of data privacy and the EU–Japan GDPR adequacy agreement. *Harvard Journal of Law & Technology*, *33*(2), 661–728. https://jolt.law.harvard.edu/assets/articlePDFs/v33/33HarvJLTech661.pdf

Wong YongQuan, B. (2017). Data privacy law in Singapore: The Personal Data Protection Act 2012. *International Data Privacy Law*, *7*(4), 287–302. https://doi.org/10.1093/idpl/ipx016

WorldData.info. (2024). *Economy of Singapore* [Data set]. https://www.worlddata.info/asia/singapore/economy.php

World Economic Forum. (2011). *Personal data: The emergence of a new asset class*. https://www3.weforum.org/docs/WEF_ITTC_PersonalDataNewAsset_Report_2011.pdf

About the Author

Danni Zhang is a joint PhD researcher at Northeastern University London and the University of Kent, affiliated with the Institute of Cyber Security for Society. Her research focuses on digital governance in the EU and China, especially in digital economy, data governance, and AI regulation.

Politics and Governance
2025 • Volume 13 • Article 10575
https://doi.org/10.17645/pag.10575

cogitatio

ARTICLE

Open Access Journal

Digital Sovereignism: A Comparative Analysis of Italian Parties' Positioning on Transnational Data Governance

Marianna Griffini

Department of Politics, International Relations, Sociology and Anthropology, Northeastern University London, UK

Correspondence: Marianna Griffini (m.griffini@northeastern.edu)

Submitted: 22 April 2025 **Accepted:** 22 July 2025 **Published:** 8 October 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

This article examines the positioning of political parties on the issue of transnational data governance, with a special focus on sovereignist parties, through the case study of Italy. With digital policy being increasingly high on Italy's political agenda, the country finds itself in a delicate balancing act between guarding itself from external interference, and opening up to global key players in data governance, including international corporate actors. While the literature on Italy's domestic data governance is relatively well developed, party-specific stances on its external dimension are understudied. Given their sovereignist ideology, it is expected that populist radical right parties prioritise sovereignty-focused stances, with concerns around data security and state control over digital policy. However, the populist radical right government's flirtation with radical right tech entrepreneur Elon Musk poses a significant research puzzle. Through a qualitative analysis of Italy's parliamentary debates covering the 12 months prior to the approval of the Space Law in June 2025, this article investigates how the incumbent sovereignist populist radical right positioned itself on digital sovereignty in the context of cross-border data governance, compared to opposition parties occupying different dimensions on the political spectrum. This case study will especially focus on the most prominent topic in current parliamentary debates on external data governance: Italy's proposed deal with Musk's SpaceX for the acquisition of Starlink technology.

Keywords

data governance; digital sovereignty; party politics; populist radical right

1. Introduction

On 7 November 2024, Italy's populist radical right Prime Minister Giorgia Meloni announced she had spoken to tech tycoon and former Donald Trump supporter Elon Musk about Italy potentially acquiring Starlink technology for telecommunications. On that occasion, Meloni praised Musk for his "commitment and vision [that] can be an important asset to…Italy" ("Meloni sente Musk," 2024). Meloni's announcement should not be dismissed as an occasional interaction between a PM and a tech titan, who, at that time, exerted enormous influence on President Trump. In fact, the publicised economic and political relationship between Meloni and Musk sparked acrimonious political debate over the threat to digital sovereignty and national security that Musk's services could pose. Significantly, Musk, who is the former co-founder of PayPal, and now executive of aerospace company SpaceX, the social network X, and automotive company Tesla, holds ideas close to the radical right MAGA movement. Before their bitter fallout in May 2025, Musk had been appointed by President Trump to lead the newly formed Department of Government Efficiency (DOGE). Regardless of his unstable relationship with Trump, Musk's economic and political sway is massive and carries important implications for the political actors he engages with.

Meloni's negotiations with Musk over Starlink have triggered opposition backlash, which has intensified during debates on the Space bill (that became law in June 2025; Senato della Repubblica, 2025). Despite Defence Minister Guido Crosetto's March 2025 declaration that talks with Musk had stalled ("Italy's talks with Musk's Starlink," 2025), the topic is poised to remain politically relevant, especially given the recent approval of the Space Law. The latter does not explicitly mention Starlink, but Article 25 allows non-Italian operators (like SpaceX) to provide strategic satellite services (like Starlink; Senato della Repubblica, 2025). Party debates over the proposed Starlink deal occur within broader political discussions about the external dimension of data governance, central to Italy's digital policy since Italy's 2021 digitalisation campaign under the EU-funded National Recovery and Resilience Plan (NRRP) worth EUR 194.4 billion. Since then, digitalisation has become a government priority devised to boost an ailing economy after the Covid-19 pandemic and to address economic, infrastructural, environmental, and equality-related challenges (Italia Domani, 2025).

While the NRRP digitalisation pillar has a predominantly domestic focus, discussions of the external dimension of digital policy cannot be overlooked, given their importance to Italy's increasing involvement in transnational data governance. In this realm, Italy strategically engages with digital powers, encompassing states, supranational organisations, and non-state actors, such as private companies. Importantly, Italy's geopolitical strategy needs to be embedded in the EU regulatory framework on the external dimension of digital policy, including the EU Coordinated Plan (European Commission, 2018) and Strategy for Data (European Commission, 2020), which advocate for increasing monitoring over European data.

At the national level, external digital policy is highly politicised by different political parties. While literature on Italy's digitalisation efforts is relatively well developed, little attention is paid to party-specific stances on this issue. We thus respond to this scholarly gap by examining how political parties from across the political spectrum position themselves on the external dimension of digital policy. In particular, this article studies the specific case of the Starlink negotiations, which hold utmost prominence in parliamentary debates. This perspective allows us to capture party dynamics articulated on two axes: (a) government vs. opposition; and (b) populist radical right vs. parties differently located on the ideological spectrum.

We are particularly interested in the populist radical right's positioning, due to their sovereignist ideology (Basile & Mazzoleni, 2020). Digital sovereignism consists of "political ideas characterized by the primacy of the national-level politics over the international one" (Pizzul & Veneziano, 2024, p. 1009). Hence, we expect these parties to prioritise the protection of digital sovereignty, connected to national security, to protect "decision-making authority of the nation-states and people's empowerment against the elites" (Basile & Borri, 2022, p. 366). Indeed, we also expect these parties to express scepticism towards corporate actors and foreign states' interference in national digital governance. Corporate actors are especially interesting, given their expanding political ambitions, making them global power brokers (Ibled, 2025). As Bellanova et al. (2022, p. 340) suggest, European digital sovereignty attempts "may be hampered by the actual, and ever increasing, role of private actors and IT companies, in particular Big Tech."

In the Italian context, populist radical right parties Fratelli d'Italia (FdI) and Lega (now in a coalition government) are anticipated to express sovereignist concerns around data security cooperation with third countries and non-state actors outside the EU, in line with their trademark ideological sovereignism. Evidence of Musk's closeness with Meloni (FdI's leader), though, suggests a potential change in the populist radical right's sovereignism regarding cross-border data governance. To tackle this puzzle, this article uses a qualitative analysis of parliamentary debates in the Chamber of Deputies (henceforth, the Chamber) and in the Senate, covering the year prior to the Space Law approval. The aim is to investigate whether sovereignist populist radical right parties in government have enacted a shift on digital sovereignty and security compared to opposition parties when dealing with ideologically aligned tech actors.

Italy provides an interesting case study to develop new insights on whether the populist radical right embraces digital sovereignty, in the context of the ongoing interlocutions between Meloni and Musk. Italy is the first Western European EU member state to have a coalition government entirely led by the populist radical right, which typically adopts sovereignty-centred stances (Basile & Mazzoleni, 2020). Meloni's coalition government, sworn in in October 2022, brings together FdI, Lega (populist radical right), and Forza Italia (FI; populist right-wing without radical elements). Additionally, Meloni's government has been particularly close to Musk, known for his patently radical right beliefs, which, in most of the period analysed, were also markedly pro-Trump (Ibled, 2025).

Therefore, the argument advanced by this article unfolds against the background of the populist radical right's dealings with Musk, who shares ideological alignment and personal friendship with Italy's PM Meloni. Importantly, from this case study, broader lessons can be learnt about how populist radical right parties position themselves on transnational data governance at a time when these parties are gaining influence and consolidating connections with tech tycoons.

The article is organised as follows. After establishing the theoretical framework centred on transnational data governance and digital sovereignty, the article will review the relevant literature on the populist radical right's sovereignism. Indeed, this party family is expected to significantly vocalise concerns for digital sovereignty compared to competing parties. The contextualisation of the case study is followed by methodological notes on the analysis of parliamentary debates. Subsequently, the analysis of parties' positioning on the external dimension of data governance is articulated around two main themes: digital security and digital sovereignty. Finally, the article offers concluding thoughts.

2. The Framework of Transnational Data Governance and Sovereignty

To examine how incumbent populist radical right parties, when engaging with ideologically aligned tech actors, position themselves on digital sovereignty and security compared to the opposition, we combine insights from comparative politics and international relations. First, this article draws on the normative understanding of transnational data governance in international relations as the set of legislation regulating the relationships between different stakeholders involved in the collection, processing, storing, access, control, sharing, and use of data (Micheli et al., 2020).

Extensive literature has studied transnational data governance in the fields of IT, legal regimes, geopolitics (Farrand & Carrapico, 2022; Gao & Chen, 2022), power inequalities, and citizens' governmentality (Bigo et al., 2019; Juverdeanu, 2024). Comparatively less extensive is the literature on the relationship between political parties and the digital. Within this emerging strand of literature, König and Wenzelburger (2018) draw attention to the increasing salience of the issue of digitisation in party manifestos in eight Western European countries. In a similar vein, König's (2019) comparative analysis of party policy on digital technologies finds that the growing relevance of digital policies pressures parties to shape their own policy preferences, making digital policy a terrain for party competition. Guglielmo (2024) provides an innovative typology of how parties' stances on digital economy and digital politics are moulded by ideology.

Transnational data governance, implying compromises between international actors, hinges upon states' willingness to negotiate national sovereignty, and to loosen policies on data access, processing, and use, which may affect national security. Indeed, national security and sovereignty drive geopolitical competition between the major digital powers. This geopolitical competition sees two main approaches to transnational data governance (included in the broader category of cyber governance): (a) Beijing's approach, driven by Chinese telecommunication and e-commerce companies that provide services across the globe, prizing the Chinese government's involvement in cyber governance; and (b) the Western-centric approach, embraced by Washington and Brussels, dominated by multi-stakeholderism, openness, and the commitment to democracy, human rights, and the free exchange of ideas (DeNardis, 2014; Gao, 2022).

As Gao and Chen (2022) notice, though, these two approaches are not dichotomous blocks. For instance, the EU combines multi-stakeholderism with increasing involvement in transnational data governance. This becomes apparent in the European Strategy for Data (European Commission, 2020), where the European Commission warns that "the way in which the data are collected and used must place the interests of the individual first, in accordance with European values, fundamental rights and rules," and it is essential that personal data sharing in the EU complies with the General Data Protection Regulation (GDPR).

Through the establishment of strict data protection rules, the EU attempts to become "a global regulatory hegemon unmatched by its geopolitical rivals" (Christakis, 2020, p. i). In doing so, the EU bolsters digital sovereignty and defensive measures against the US-American and Chinese technological behemoths, while endeavouring to contest US supremacy in the West (Chen & Yang, 2022). Indeed, the European Strategy for Data (European Commission, 2020) vocally affirms that "if the EU is to acquire a leading role in the data economy, it has to act now and tackle, in a concerted manner, issues ranging from connectivity to processing and storage of data, computing power and cybersecurity." In the attempt to assert itself as an increasingly important data governance player without relinquishing digital sovereignty claims, in the 2020 *Digital*

Sovereignty for Europe report, the EU codified digital sovereignty as "Europe's ability to act independently in the digital world" through protective mechanisms to foster digital innovation (including in cooperation with non-EU companies; European Parliament, 2020, as cited in Gao, 2022).

The desire to set the standard for digital innovation and to ensure independence from non-EU tech companies underpin the EU strategic goal of strengthening its digital sovereignty (Floridi, 2021). As Velliet (2023, p. 6) suggests, "[Digital sovereignty] justifies a large number of 'protective' and 'offensive' policies…protecting the data of Europeans, securing communication infrastructures, stimulating technological innovation." Notably, Italy's Starlink negotiations may conflict with the EU regulatory framework, since they would induce dependence on a non-European corporate actor. In fact, Italian MEPs submitted a parliamentary question expressing reservations about the potential Starlink deal and asking whether it would not be wiser if member states relied on European satellite projects such as IRIS^2 (European Parliament, 2025).

Broadly speaking, digital sovereignty is situated at the nexus of bordering practices, data management, and securitisation (Thumfart, 2025). In EU member states, the concept of digital sovereignty gained circulation in the 2000s when France and Germany vocalised concerns about the US's access to and processing of personal data (Bellanger, 2014). For instance, France warned against the risk that the EU would turn into a "colony of the digital world" (Morin-Desailly, 2013), and Germany underlined the priority of concentrating, through the EU, on national security, economic strategy, and digital sovereignty (Steiger et al., 2017). Germany also voiced security concerns around the protection of national IT infrastructure from external interference (Pohle & Thiel, 2020). Between 2019 and 2022, under the Von der Leyen Commission, digital sovereignty concerns became high on the EU agenda (Bellanova et al., 2022) and were understood as a way to further deepen European integration (European Commission, 2020) and reduce dependence on other states. As Farrand and Carrapico (2022) argue, through digital sovereignty the EU aims to achieve technological independence and the protection of its digital borders from international competition.

3. Populist Radical Right Parties and the External Dimension of Digital Policy

Due to the primacy of sovereignty on the populist radical right's agenda, this article focuses its attention on how these parties compete against their opponents on transnational data governance. Among the broad range of definitional attempts, here we adopt Mudde's seminal characterisation of populist radical right parties as advocating strict law and order, pitting themselves as the "pure" people against multifarious elites, and embracing nativism (i.e., the nationalist and xenophobic belief that the nation should be inhabited only by natives; Mudde, 2007).

Because of this domestic anti-elitism, the foreign policy of populist parties (not necessarily located on the right end of the political spectrum) may be confrontational towards international elites, i.e., international political actors including states and international institutions (Chryssogelos, 2017). Nevertheless, it is worth noting that often populist leaders become part of the political establishment elite.

The populist radical right adds a sovereignist dimension to the international anti-elitism manifested by populism at large, through a nationalist emphasis on national sovereignty (Basile & Borri, 2022; Meijen, 2024) vis-à-vis international actors. Sovereignty, understood as "mutually exclusive territories" (Basile &

Borri, 2022, p. 367), faces challenges from a multiplicity of stakeholders, such as transnational movements, corporate actors, and civil society, to name a few. The solution proposed by sovereignist parties is to solidify state borders both physically and figuratively to firmly ground authority in the state (Bickerton et al., 2022). Notably, recent scholarship shows a tension between the populist radical right's flirtations with the "tech oligarchs" elite, such as Musk, and its typical anti-elitism and sovereignism (Farkas & Mondon, 2025).

4. Methodology

In order to examine parties' stances on the external dimension of data governance, this article draws on a thematic analysis of 98 parliamentary debates delivered in the Chamber and in the Senate in the 12 months prior to the 11 June 2025 approval of the so-called Space Law. The latter represents a critical point in Italy's policy-making on transnational data governance, and was preceded by the increasing salience in political debates of Musk's Starlink provision of encrypted telecommunication services for the Italian government and the management of sensitive diplomatic and military data. Concurrently, Musk has been progressively politicising his persona, aligning with Trump for most of the period under consideration through shared hostility against immigration, the so-called "deep state," and "woke ideology" (Galasso, 2024). However, their relationship became strained due to a recent disagreement over tariffs and the "Big Beautiful Bill," and culminated with Musk's announcing the formation of his own America Party in July 2025 (Clun & Sommerlad, 2025; Price, 2025).

The selected debates were retrieved from the digital archives of the two parliamentary houses. A pilot keyword search was performed using the Italian translation of the stem word "digital*," and the words "data," "informatics," and "cyber." Given the overwhelming salience of "Starlink" and "(Elon) Musk" in the results of the pilot search, the data collection then proceeded based on these two terms. The analysis proceeded through the deductive coding of the individual speeches, by drawing on the established themes in the literature on the external dimensions of digital policy, comprising transnational data governance, and on sovereignism. This qualitative text analysis approach has the merit of capturing both the nuances and the complexity of the data.

A potential drawback of the study is that its focus is circumscribed to the debate on digital policy centred on Starlink and Musk. However, this limited focus is justified by the fact that Starlink and Musk emerged as the absolutely predominant themes in parliamentary speeches on the transnational dimension of digital policy.

5. The External Dimension of the Digital: The Case of Starlink

The analysis of parliamentary debates reveals that digitalisation is frequently mentioned within the context of the NRRP. This is relevant, since it entails that political parties tend to focus on the domestic dimension of digital policy, related to the "digital transition" that is one of the priorities of the NRRP, established by the EU during the Covid-19 pandemic to stimulate economic recovery in different EU member states (Italia Domani, 2025). In 2021, Italy became the beneficiary of EUR 194.4 billion to be disbursed in 10 tranches by 2026, conditional upon the implementation of reforms on the digital and green transitions. The appeal of digitalisation spans across Italian major parties hailing from different ideologies, such as the populist catch-all party Movimento Cinque Stelle (M5S), the populist radical right FdI and Lega, and the centre-left Partito Democratico (PD; Senate 2024/ 216). However, as common wisdom would suggest, the PD, playing

the role of the opposition in parliamentary debates, used the acceleration of the green and digital transitions to attack the alleged underperformance of the government (Senate 2024/229).

Digitalisation efforts go beyond the domestic sphere and inevitably invoke the discussion of Italy's rumoured deal with Musk for the installation of Starlink to boost connectivity across the peninsula ("Financial Times: «Musk cerca Mattarella," 2025). The populist radical right immediately emerges as favourable to the deal, by championing the use of Musk's innovative tools of data governance. This may be partly explained by the previous findings by Guglielmo (2024), which show that FdI and Lega put a premium on innovation as a driver of national economic competitiveness. Instead, the M5S rebuked the FdI-led government for "gifting Elon Musk an exceptionally advantageous deal through the purchase of the satellite network Starlink" (Conte, in Chamber 2024/402). Also Francesco Boccia (from the centre-left PD) berated the government for "shamefully" gifting private companies, like Musk's, the incredibly profitable development of broadband infrastructure as part of the NRRP (Senate 2024/258). This throws into sharp relief the coalescing of the opposition against the Starlink deal, with the centre-left PD attacking the negotiations in a not dissimilar way from how the catch-all populist M5S does.

The analysis of the parliamentary debates shows how the Starlink deal, i.e., the acquisition of Starlink telecommunications security technological infrastructure, and its extortionate price, doubtlessly overshadow other themes related to the external dimension of the digital in the period under consideration. As we will see in the next two sections of the analysis, the meddling of Musk in Italy's data governance polarises political parties in two main respects: security and sovereignty. The parties that are traditionally ideologically sovereignist have been relenting on digital sovereignty in the context of Musk's ventures. This apparent paradox is not trivial, and illuminates the tensions between ideological sovereignty and pragmatic openness to international corporate partnerships on digital infrastructures.

5.1. Security and the Digital

In debates over the external dimension of transnational data governance, reflections on security occupy a paramount and polarising role when parties discuss Italy's proposed purchase of Musk's Starlink infrastructure for telecommunications security.

Predictably, security preoccupations play a salient role in parties' stances across the political spectrum. Particular emphasis on the matter is expected to come from the populist radical right. Based on the literature on the populist radical right unpacked earlier, we anticipate that their priorities, dictated by nationalism, will be: (a) the primacy of national security; and (b) guardedness vis-à-vis potential foreign involvement in transnational data governance that could interfere with national security. In our specific case study, foreign actors are embodied by international corporate entities linked to foreign states, such as Musk as the leader of his aerospace company SpaceX and as former President Trump's aide.

Our first expectation is met: The populist radical right promotes national economic and security interests, through the development of the digital sphere. The Brussels data governance model discussed previously prizes a multilateral approach, while putting cybersecurity high on the agenda (Gao & Chen, 2022). Adolfo Urso, FdI Minister of Industry and Made in Italy, emphasised the importance of the development and consolidation of digital resources, in which government investments have been concentrated (Senate

2025/260). Nicola Calandrini, FdI representative, praised Italy's 2024 budget for its focus on green and digital transitions, which enables Italy and the EU to pursue their strategic interests (Senate 2024/229). In a similar fashion, FdI former Ambassador and former Minister of Foreign Affairs Giulio Terzi di Sant'Agata pressed for digital innovation and the increase in digital connections between Italy and Europe (Senate 2024/229) as a way to promote national interests.

Our second expectation, instead, is not met: In our case study, while populist radical right parties are typically sovereignist, their incumbent status and ideological alignment with tech actors appear to override digital sovereignty concerns. These specific dynamics, with resistance to foreign involvement in transnational data governance coming from the opposition rather than the sovereignist populist radical right, should be interpreted in the light of the close relationship between Meloni and the tech mogul Musk. Indeed, it would be politically damaging for incumbent parties not to support the government-led Starlink negotiations, whereas it would be predictable that resistance comes from the parties in opposition. Moreover, the ideological leanings of the tech entrepreneur, close to the radical right galaxy, may explain the populist radical right's tension between ideological sovereignism and pragmatism.

Diving into the specifics of the criticism levelled by political opponents, Andrea Casu, from centre-left PD, demanded from PM Meloni clarity over the contentious question of her negotiations with tech tycoon and Trump's buddy Musk, which would imply a "waste of 1.5 billion EUR" for strategic services (Chamber 2025/404). Casu continued: "We are risking handing over the reins of our security and defence to an external power" (Chamber 2025/404). "External power" in this quotation refers to the private company SpaceX, embodied by Musk with his enormous economic and political power, and firm radical right leanings.

Worries about security threats from this external power led to a group of PD MPs presenting on 8 January 2025 a formal written question to the minister of defence on the potential agreement between Italy's government and SpaceX on telecommunication security. The written question defined the existence of a negotiation between Italy's government and Musk as "disquieting," since it would entail entrusting military security data to a private company owned by one of the wealthiest men on earth and, simultaneously, then close adviser of President Trump, and still a supporter of the radical right in Europe (Chamber 2025/Allegato A [08/01/2025]). The main concern voiced in this written question is the security menace that an agreement with Musk stipulating the adoption of Starlink would pose to Italy. Such a threat would blatantly conflict with the NRRP strategic goal of embedding national development in the EU milieu (Chamber 2025/Allegato A [08/01/2025]). Among the opposition, we identify rampant suspicions that the government overlooks national security in favour of technological innovation led by radical right tech tycoons. The political affinity between Musk and the radical right may be an explanatory factor of the opposition's politicisation of the issue of digital innovation and of the strong feelings elicited about the perceived surrendering of national security to Musk through the adoption of Starlink.

Distrustful positions preoccupied with national security emerge also from the left-wing party Alleanza Verdi e Sinistra (AVS), which sits on the left of the centre-left PD, and from the catch-all populist M5S. Riccardo Ricciardi (M5S) and Chiara Braga (PD) fretted about the unlawful handing over of sensitive data security to Musk and summoned Meloni to appear in parliament to justify her dealings with Musk (Chamber 2025/405). Moreover, Giuseppe Conte (M5S; Chamber 2025/450), Francesca Ghirra (AVS; Chamber 2025/440), and Filiberto Zaratti (AVS; Chamber 2025/404) attacked the governing parties for contracting out national

security, citizens' privacy, and Italy's defence, despite their self-projection as patriots and protectors of national autonomy. The perception of digital technologies as potential risks to privacy is not new. As König (2019) noticed in the context of party competition in Germany and Ireland on the issue of digital policy, parties grapple with a trade-off between harnessing the economic value of digital technology and concerns with the granular and extensive collection of personal data. According to Zaratti (AVS), "It seems that this meeting [between Meloni and Musk] is based more on the subservient relationship Italy has with the US, than on the protection of our national interests" (Chamber 2025/404). In this case, Musk has become the personification of the US (under the second term of President Trump). The fallout between Trump and Musk did not allay the fears of the opposition: While discussing the Space Law, M5S MP Gisella Naturale denounced the risks to national interest and security posed by Starlink, and cited the breakup between Musk and Trump as evidence that the US realised the national security issue caused by entrusting transnational data governance to an individual holding a monopoly over satellite telecommunications (Chamber 2025/314).

Overall, the opposition shares a critical stance towards the potential security threat posed by the installation of Musk's Starlink telecommunications infrastructure to manage diplomatic and military data. By contrast, the populist radical right relaxes its typical guardedness vis-à-vis foreign interference in security affairs when it deals with corporate actors close to radical right views. Indeed, Musk's close relationship with Italian PM Meloni has gone from strength to strength, after being propelled by Musk's participation at FdI's national Atreju Convention in December 2023. Consequently, on the party competition chessboard, the parties in opposition perform their assigned role and push back the government's proposals.

5.2. Sovereignty and the Digital

Musk's Starlink is perceived not just as a security threat to Italy, but, more prominently, as an infringement of sovereignty. Meloni's visit to then-US president-elect Trump in early January 2025 prompted strong reactions from the opposition due to rumours about a reported agreement between Meloni and Musk for the installation of Starlink platforms in Italy. On 6 January 2025, *Bloomberg* (Mancini, 2025) announced that Meloni met Musk at Trump's residence in Mar-a-Lago, where they progressed on negotiations for Italy's purchase of Musk's telecommunications security system. Meloni immediately denied signing any agreement, without disproving the existence of negotiations. On this occasion, worries over national security became intertwined with worries over Italy's digital sovereignty, arguably threatened by Musk's interference.

As with party positioning on the issue of Starlink's implications for national security, stances on its potential geopolitical threats to national (digital) sovereignty also follow the government-opposition dividing line. This is unsurprising, since the populist radical right in government has entertained dense diplomatic relations with Musk. Hence, it would be contradictory to show guardedness vis-à-vis foreign actors. According to the party competition playbook, the opposition instead frames Musk as the archenemy of Italy's (digital) sovereignty, fearing possible repercussions in several aspects of national economy and politics. Nevertheless, these observed dynamics, where opposition parties rather than the populist radical right express concerns about Musk's Starlink infrastructure threatening digital sovereignty, do not invalidate the prevailing argument in the literature. The foreign policy of populist parties in the digital sphere remains primarily driven by sovereignty concerns, but being in government versus being in opposition appears to influence the degree to which these concerns manifest. Indeed, it is logical that the incumbent status of

populist radical right parties may unsettle their traditional sovereignism when they discuss a deal proposed and supported by the US-American radical right tycoon Musk. Yet, the aforementioned dynamics call for the problematisation of the populist radical right's stance on the external dimension of digital policy, showing how being in power and ideological affinity with corporate actors may twist expectations on parties' adherence to digital sovereignty.

Taking a step back in time, we notice that concerns over Musk's penetration in Italy's sovereignty as a foreign corporate power were already circulating before his controversial encounter with Meloni in January 2025. Remarkably, on 14 November 2024, PD MP Casu reproached Transport Minister Matteo Salvini, leader of FdI's coalition partner Lega, for "opening up the doors of our country to Elon Musk" and ignoring national sovereignty as well as the existence of a EU satellite strategy (Chamber 2024/383). The latter represents a crucial node in the debates, where the opposition repeatedly and vocally called for the adoption of the EU satellite project IRIS^2.

Anxiety about Musk's potential threat to digital sovereignty did not subside. On 11 December 2024, the opposition attacked Meloni for her talks with Musk, citing Starlink's potential infiltration in Italy's data governance. Senator Antonio Nicita (from the centre-left PD), implicitly accusing Starlink, emphasised the importance that "big digital platforms do not cause conflicts of interest in the domain of services for connectivity, [and] data governance" (Senate 2024/252). Furthermore, considering that NRRP funds had previously been allocated to two Italian companies involved in digital innovation, Nicita harshly denounced as unlawful the diversion of these funds (distributed by the EU) into Italy's investment in Starlink (Senate 2024/252). Apprehensions over Musk's incursion into Italy's digital sovereignty peaked during the discussion of the Space Law. Elena Pavanelli (M5S) and Elly Schlein (PD) resented the rejection of the amendments proposed by the opposition to block foreign access to Italian data, in order to sustain national data governance enterprises (Chamber 2025/438; Chamber 2025/440; Chamber 2025/450). In a similar fashion, Luigi Manca (PD) deprecated the handover of sovereignty to Musk, with the related national security implications (Senate 2025/285).

Interestingly, the parties invoking sovereignism do not belong to the populist radical right, which has traditionally been distinguished by sovereignism (Taggart & Pirro, 2021). This paradox is obvious in Nicita's further criticism of the government's inconsistency: On one hand, in the past, the populist radical right had opposed the use of foreign-owned clouds to host Italians' data on grounds of sovereignty protection; on the other hand, today they have betrayed their digital sovereignism under the spell cast by Musk (Senate 2024/252). In this regard, Nicita stated emphatically: "Where did the government's sovereignism go?" thus provoking the governing parties and hinting at their trademark sovereignist ideology (Senate 2024/252).

Criticism of the government's potential engagement with Musk through his provision of Starlink is spread across the opposition. Centre-left Italia Viva's (IV) Enrico Borghi urged the parliament to keep up with digital evolutions without surrendering sovereignty to big techs: "AI and, more broadly, the digital, do not mean surrendering a grazing ground [i.e., authority over resources] to Musk or anyone like him" (Senate 2024/257). On a more critical note, IV MP Silvia Fregolent provoked the government by taunting the populist radical right's typical slogan "Italians first," and suggesting, instead, that the populist radical right now prioritises Musk to Italians (Senate 2024/257). Hesitation over Musk's provision of data services is grounded in apprehensions about the economic and political influence the tech tycoon may exert, particularly his galvanising influence

over European radical right parties (Robertson, 2025). External influence in data governance, therefore, is feared to spill over into the domestic economic and political domains.

Zaratti, from AVS (firmly located on the left-hand side of the political spectrum), shared pressing concerns about the news (later revealed to be unfounded) that Meloni had discussed with Musk about a EUR 1.5 billion contract between Italy and Starlink. Such concerns are due to the alarms over the impact that Musk could have on telecommunications in the military, the government, and emergency satellite services (Chamber 2025/404), which are crucial to Italy's national interest. By extension, Zaratti (AVS) labelled the (falsely) reported contract between Italy's government and Musk as yet another instance of Italy's externalisation of border control (Chamber 2025/404).

The opposition's accusations also pertain to the realm of the protection of democracy, in response to Musk's meddling with Italian institutions. In reaction to the Italian court's decision to block, on the grounds of lack of legitimacy, the deal devised by Meloni on Italy's externalisation of migration to Albania, Musk publicly expressed his outrage at the ruling (Winfield, 2024). This prompted the Italian head of state Sergio Mattarella to rebuke, indirectly but resolutely, Musk for interfering with Italy's sovereignty (Winfield, 2024). MP Simona Bonafé (PD; Chamber 2024/386), Andrea Casu (PD; Chamber 2024/380), and Angelo Bonelli (AVS; Chamber 2024/380) concurred in resenting Musk's boldness in attacking the Italian judges. More broadly, PD's Nicita questioned the influence that "tycoons of digital and global capitalism" may have on public debates and on the public sphere, posing a serious risk to democracy through non-transparent data management and the manipulation of public opinion (Senate 2024/252). Sarcastically, Nicita quipped, "We have transitioned from national-sovereignism to an extreme provincialism, where we just need a billionaire tycoon to sell out our country" (Senate 2024/252). This scepticism was also echoed by MP Federico Giannassi from the centre-left IV (Chamber 2025/408).

Therefore, extensive emphasis on concerns around digital sovereignty spans multiple opposition parties, while the incumbent populist radical right remains open to foreign corporate actors' involvement in Italy's external dimension of data governance. Across the sample, the incumbent populist radical right ministers and MPs very rarely intervened in the Musk's Starlink debate, and only in response to written questions coming from the opposition (see Table 1). For instance, FdI Minister of Industry and Made in Italy Urso appeared in the Chamber to defensively state that the government is working on a national satellite system to offer a competitive alternative to Starlink (Chamber 2025/431). Minister of Relationships with Parliament Edmondo Ciriani (FdI) similarly appeared in the Senate to respond to a written question and reiterated what had already been declared by Minister of Defence Guido Crosetto (FdI; Chamber 2025/405), i.e., the government had not signed any agreement for Starlink and was mindful of the protection of national security and national sovereignty (Senate 2025/285).

Hence, FdI ministers intervened in parliamentary debates in order to support the government's stance on Musk, which had been clarified by PM Meloni in her 2025 new-year press conference. On that occasion, Meloni reassured that the Starlink question was being explored by involving the relevant institutional branches, thus hinting at the fact that no deal had been signed up to then (Meloni, 2025). Meloni also underlined that both national security and digital innovation would underpin any consideration about Starlink, thus attempting to prove unfounded the concerns of the opposition (Meloni, 2025). Incidentally, it is noteworthy that Lega and FI, despite being government coalition partners, only rarely intervened and retained a purely supportive role for FdI.

Table 1. Summary of interventions in the Musk's Starlink debate cited according to party, party status (incumbent/opposition), and intervention type.

Party	Total number of MPs'/ministers' interventions in the cited sample	Status	Response to written question?
PD (Partito Democratico)	12	Opposition	No
M5S (Movimento Cinque Stelle)	5	Opposition	No
AVS (Alleanza Verdi e Sinistra)	3	Opposition	No
IV (Italia Viva)	3	Opposition	No
FdI (Fratelli d'Italia)	3	Incumbent	Yes

Therefore, the Italian populist radical right appears to be shaping a digital foreign policy leaning towards the pragmatic use of foreign provision of satellite services and the consequent loosening of its traditional sovereignism. Pragmatism in populist foreign policy is not new (Giurlando, 2021) and allows these parties to flexibly pursue their own interests without being bent to their ideological sovereignism. In our case study, pragmatism is attributable to two main reasons. First, the government needs to meet the EU digital challenges and act as a credible actor in the EU. In fact, status-seeking has been recognised as a goal of populist foreign policy, which outweighs the risks inherent to trade-offs between sovereignty and economic opportunities in the international sphere (Destradi et al., 2021). Second, the government needs to maintain and intensify the relationship with tech billionaire Musk because of ideological proximity and the economic and political support that Musk could provide. The ideological affinity between Meloni and Musk strengthens their links on transnational data governance, but is not dictated by the sovereignism that usually characterises the radical right's ideology.

As a concluding note, it is interesting to observe that the parliamentary debates analysed scarcely mention AI, which would have been useful to examine, in order to gain a broad and profound understanding of party positioning in the context of transnational data governance. In fact, calls for AI regulation are usually a major manifestation of digital sovereignty related to AI. The scarce attention to AI matters is striking if one considers the EU's insistence on regulating AI according to international competitiveness and EU values (Roberts et al., 2022). The near absence of this topic in the debates speaks volumes to the primacy given to the proposed Starlink deal between Meloni and Musk, which eclipses other related topics.

6. Conclusion

To conclude, this article offers a currently pertinent examination of the evolving dynamics of party positioning on the external dimension of data governance during increasing involvement of foreign corporate actors. Indeed, this article has analysed the critical case study of Italy, to investigate how political parties situate themselves on the external dimension of digital policy, with a specific focus on the positioning of the incumbent populist radical right in Italy vis-à-vis the opposition. In this context, parliamentary debates were dominated by the proposed deal between Meloni and Musk on Italy's acquisition of Starlink for connectivity and telecommunication purposes. This trending theme inevitably invokes the examination of whether the populist radical right, now in government and led by PM Meloni, maintains its typical sovereignism when it comes to digital sovereignty, compared to opposition parties.

Extensive literature has unpacked populist and populist radical right foreign policy on one hand, and, on the other hand, the issue of digital sovereignty within the ambit of transnational data governance. Instead, the intersection of these two themes, precisely how political parties across the political spectrum position themselves regarding transnational data governance, is still underexamined. This article aims to fill this gap, while also responding to the call for a multidisciplinary approach to the global challenge of digital data governance (Löfflmann, 2022; Savona, 2024). Hence, this article bridges comparative politics approaches to the study of party politics, with the international relations conceptual toolkit on digital sovereignty.

Qualitative discourse analysis of parliamentary debates reveals that party ideological positioning does not significantly shape party stances about digital sovereignty. Instead, being in power versus being in opposition preponderantly influences party positioning vis-à-vis the specific question of the proposed deal between Italy and Musk related to transnational data governance. Overall, pragmatism predominates over ideological sovereignism: The Italian government, ruled by the populist radical right, aims at achieving digital innovation, being reputable at the EU level, and leveraging Musk's immense economic and political sway in radical right circles.

This finding is not unexpected, since it is logical that governing parties leading negotiations with Musk would not frame the prospective deal as threatening national sovereignty. At the same time, this finding is interesting, because it indicates that populist radical right parties defy expectations over their ideological sovereignism, by supporting foreign involvement, especially Musk's, in transnational data governance. Instead, opposition parties belonging to the centre-left PD and IV, the left AVS, and the catch-all populist M5S express scepticism or utter hostility about the Starlink negotiations on the grounds of security and sovereignty-related preoccupations.

These findings have important implications for our understanding of domestic digital policy in an EU member state ruled by the populist radical right, indicating potential for further research on how political parties rise to the challenge of transnational data governance, mapped against the backdrop of the rising influence of radical right tech barons. While attempting to fill the gap in the literature and enrich the underexplored scholarship on party positioning on transnational data governance, this article does not offer a full account of the plethora of aspects composing the external dimension of Italy's digital policy and of the entire spectrum of stakeholders. Instead, this research, based on the analysis of parliamentary debates, focuses on a timely but understudied topic currently animating political debate in the Italian parliament.

Additionally, this article hopes to stimulate a new research agenda, focusing on the pressing issues dictated by corporate actors' infiltration of states' digital sovereignty. This agenda presents further opportunities to research this ever-evolving topic by extending the geographical, temporal, and thematic reach of the article through a comparison of different parties across a range of countries and time periods, and through consideration of additional topics related to transnational data governance, such as policies on 5G technology, cloud storage, and AI. This exemplar case study leaves some interesting questions unanswered: How does the Italian populist radical right government reconcile compliance with EU digital policies on one side, and the politicised attraction to US tech entrepreneurs on the other side? Particularly, is Italy aligning itself with tech entrepreneurs linked to the radical right?

Acknowledgments

The author would like to thank the academic editors, Dr. Xuechen Chen and Dr. Xinchuchu Gao, for organising this thematic issue, and for their insightful comments; all the participants in the thematic issue workshop in January 2025, especially Professor Helena Carrapico and Professor Benjamin Farrand, for their very thorough comments; and the three anonymous reviewers for their constructive suggestions. Sincere thanks go also to Dr. Matilde Rosina for the helpful advice.

Conflict of Interests

The author declares no conflict of interests.

Data Availability

Research data are available online in the parliamentary archives of the Italian Senate (https://www.senato.it/ric/generale/nuovaricerca.do?params.legislatura=19) and Chamber of Deputies (https://banchedati.camera.it/tiap_19/ctrStartPage.asp).

References

Basile, L., & Borri, R. (2022). Sovereignty of what and for whom? The political mobilisation of sovereignty claims by the Italian Lega and Fratelli d'Italia. *Comparative European Politics*, *20*, 365–389. https://doi.org/10.1057/s41295-022-00273-w

Basile, L., & Mazzoleni, O. (2020). Sovereignist wine in populist bottles? An introduction. *European Politics and Society*, *21*(2), 151–162. https://doi.org/10.1080/23745118.2019.1632576

Bellanger, P. (2014). *La souveraineté numérique*. Stock.

Bellanova, R., Carrapico, H., & Duez, D. (2022). Digital/sovereignty and European security integration: An introduction. *European Security*, *31*(3), 337–355. https://doi.org/10.1080/09662839.2022.2101887

Bickerton, C., Brack, N., Coman, R., & Crespy, A. (2022). Conflicts of sovereignty in contemporary Europe: A framework of analysis. *Comparative European Politics*, *20*, 257–274.

Bigo, D., Isin, E., & Ruppert, E. (2019). Data politics. In D. Bigo, E. Isin, & E. Ruppert E. (Eds), *Data politics: Worlds, subjects, rights* (pp. 1–18). Routledge.

Chen, X., & Yang, Y. (2022). Different shades of norms: Comparing the approaches of the EU and ASEAN to cyber governance. *The International Spectator*, *57*(3), 48–65. https://doi.org/10.1080/03932729.2022.2066841

Christakis, T. (2020). *'European Digital Sovereignty': Successfully navigating between the 'Brussels Effect' and Europe's quest for strategic autonomy*. SSRN. https://doi.org/10.2139/ssrn.3748098

Chryssogelos, A. (2017). Populism in foreign policy. In *Oxford research encyclopedia of politics*. Oxford University Press.

Clun, R., & Sommerlad, J. (2025, July 1). Trump and Musk's feud timeline: From Epstein allegations to clash over the Big, Beautiful Bill. *The Independent*. https://www.independent.co.uk/news/world/americas/us-politics/trump-musk-feud-timeline-twitter-truth-social-b2780187.html

DeNardis, L. (2014). *The global war for internet governance*. Yale University Press.

Destradi, S., Cadier, D., & Plagemann, J. (2021). Populism and foreign policy: A research agenda (Introduction). *Comparative European Politics*, *19*(6), 663–682.

European Commission. (2018). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—"Coordinated Plan on Artificial Intelligence"* (COM(2018)795 Final). Publications Office of the EU.

European Commission. (2020). *Communication from the Commission to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions—"A European Strategy for Data"* (COM (2020) 66 Final). Publications Office of the EU.

European Parliament. (2025). *The impact of Starlink on the European satellite internet service market* (EU Parliamentary question E-000092/2025). https://www.europarl.europa.eu/doceo/document/E-10-2025-000092_EN.html

Farkas, J., & Mondon, A. (2025). The roots of reactionary tech oligarchy and the need for radical democratic alternatives. *Communication Culture & Critique*, *18*(2), 123–126. https://doi.org/10.1093/ccc/tcaf011

Farrand, B., & Carrapico, H. (2022). Digital sovereignty and taking back control: From regulatory capitalism to regulatory mercantilism in EU cybersecurity. *European Security*, *31*(3), 435–453.

Financial Times: «Musk cerca Mattarella per salvare l'accordo di Starlink in Italia». Salvini: sarebbe un incontro stimolante. (2025, March 10). *Sole 24 Ore*. https://www.ilsole24ore.com/art/financial-times-musk-cerca-mattarella-salvare-l-accordo-starlink-italia-AGUcXPRD

Floridi, L. (2021). The fight for digital sovereignty: What it is, and why it matters, especially for the EU. *Philosophy & Technology*, *33*, 369–378. https://doi.org/10.1007/s13347-020-00423-6

Galasso, V. (2024, December 11). Elon Musk and Giorgia Meloni: A burgeoning friendship the world should keep an eye on. *The Conversation*. https://theconversation.com/elon-musk-and-giorgia-meloni-a-burgeoning-friendship-the-world-should-keep-an-eye-on-245593

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, *57*(3), 15–30.

Gao, X., & Chen, X. (2022). Role enactment and the contestation of global cybersecurity governance. *Defence Studies*, *22*(4), 689–708. https://doi.org/10.1080/14702436.2022.2110485

Giurlando, P. (2021). Populist foreign policy: The case of Italy. *Canadian Foreign Policy Journal*, *27*(2), 251–267. https://doi.org/10.1080/11926422.2020.1819357

Guglielmo, M. (2024). Going digital…but what for? Parties' ideological positions and divides on platform societies in Western Europe. *Government and Opposition*, *60*(3), 703–728. https://doi.org/10.1017/gov.2024.24

Ibled, C. (2025). 'Founder as victim, founder as God': Peter Thiel, Elon Musk and the two bodies of the entrepreneur. *Journal of Cultural Economy*. Advance online publication. https://doi.org/10.1080/17530350.2025.2471602

Italia Domani. (2025). *The national recovery and resilience plan*. https://www.italiadomani.gov.it/content/sogei-ng/it/en/home.html

Italy's talks with Musk's Starlink have stalled, minister says. (2025, March 22). *Reuters*. https://www.reuters.com/business/aerospace-defense/italys-deal-with-starlink-has-stalled-defence-minister-says-2025-03-22

Juverdeanu, C. (2024). The EU settlement scheme: Footprints in quicksand. *Big Data & Society*, *11*(2). https://doi.org/10.1177/20539517241242537

König, P. D. (2019). Signs of convergence in party policies on digital technologies. A comparative analysis of party policy stances in Ireland and Germany. *Journal of Information Technology & Politics*, *16*(2), 137–153. https://doi.org/10.1080/19331681.2019.1613280

König, P. D., & Wenzelburger, G. (2018). Why parties take up digitization in their manifestos: An empirical analysis of eight Western European economies. *Journal of European Public Policy*, *26*(11), 1678–1695. https://doi.org/10.1080/13501763.2018.1544268

Löfflmann, G. (2022). Introduction to special issue: The study of populism in international relations.

The British Journal of Politics and International Relations, *24*(3), 403–415. https://doi.org/10.1177/13691481221103116

Mancini, D. P. (2025, January 6). Meloni's closeness to Musk and Trump is a win-win—And a big risk. *Bloomberg*. https://www.bloomberg.com/news/articles/2025-01-06/meloni-s-closeness-to-musk-and-trump-is-a-win-win-and-a-big-risk?srnd=homepage-europe&sref=P9eL2p16

Meijen, J. (2024). Future-proofing the people? A comparative analysis of data sovereignty as a discursive practice in Western European right-wing populism's digital policies. *Information Polity*, *29*(1), 73–91. https://doi.org/10.3233/IP-220023

Meloni, G. (2025). *Conferenza stampa di inizio anno del Presidente Meloni* [Speech transcript]. Governo Italiano. https://www.governo.it/it/articolo/conferenza-stampa-di-inizio-anno-del-presidente-meloni/27435

Meloni sente Musk: 'La sua visione è una risorsa per Usa e Italia.' (2024, November 7). *Ansa*. https://www.ansa.it/usa_2024/notizie/2024/11/07/meloni-sente-musk-la-sua-visione-e-una-risorsa-per-usa-e-italia_5ebcb00b-2f34-48ad-a1b4-f6d8308f28f9.html

Micheli, M., Ponti, M., Craglia, M., & Berti Suman, A. (2020). Emerging models of data governance in the age of datafication. *Big Data & Society*, *7*(2). https://doi.org/10.1177/2053951720948087

Morin-Desailly, C. (2013). *L'Union européenne, colonie du monde numérique?* Senat.

Mudde, C. (2007). *Populist radical right parties in Europe*. Cambridge University Press. https://doi.org/10.1017/CBO9780511492037

Pizzul, D., & Veneziano, M. (2024). Digital sovereignty or sovereignism? Investigating the political discourse on digital contact tracing apps in France. *Information, Communication & Society*, *27*(5), 1008–1024. https://doi.org/10.1080/1369118X.2023.2232840

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

Price, M. (2025, July 7). Musk says he's forming a new political party after split with Trump over tax cuts law. *Associated Press*. https://apnews.com/article/elon-musk-political-party-92353942308fee929a937b17113e077e

Roberts, H., Cowls, J., Hine, E., Morley, J., Wang, V., Taddeo, M., & Floridi, L. (2022). Governing artificial intelligence in China and the European Union: Comparing aims and promoting ethical outcomes. *The Information Society*, *39*(2), 79–97. https://doi.org/10.1080/01972243.2022.2124565

Robertson, D. (2025, January 6). Musk takes governance-by-X to Europe. *POLITICO*. https://www.politico.com/newsletters/digital-future-daily/2025/01/06/musk-takes-governance-by-x-to-europe-00196723

Savona, M. (2024). Data governance: Main challenges. *EconPol Forum*, *25*(3), 28–31.

Senato della Repubblica. (2025). *Disegno di legge n.1415. Disposizioni in materia di economia dello spazio*. https://www.senato.it/show-doc?leg=19&tipodoc=DDLMESS&id=1459686&idoggetto=0

Steiger, S., Schünemann, W. J., & Dimmroth, K. (2017). Outrage without consequences? Post-snowden discourses and governmental practice in Germany. *Media and Communication*, *5*(1), 7–16. https://doi.org/10.17645/mac.v5i1.814

Taggart, P., & Pirro, A. L. P. (2021). European populism before the pandemic: Ideology, Euroscepticism, electoral performance, and government participation of 63 parties in 30 countries. *Italian Political Science Review*, *51*(3), 281–304. https://doi.org/10.1017/ipo.2021.13

Thumfart, J. (2025). Digital sovereignty in China, Russia, and India: From NWICO to SCO and BRICS. In M. Jiang & L. Belli (Eds.), *Digital sovereignty in the BRICS countries: How the Global South and emerging power alliances are reshaping digital governance* (pp. 41–62). Cambridge University Press.

Velliet, M. (2023). *Digital sovereignty: European policies, American dilemmas*. Institut français des relations

internationales. https://www.ifri.org/en/papers/digital-sovereignty-european-policies-american-dilemmas

Winfield, N. (2024, November 13). Italy's president sharply rebukes Elon Musk over comments on X about migration court rulings. *Associated Press*. https://apnews.com/article/musk-italy-albania-migration-8a3cad24845a86f7ae5a11fc00ce4931

About the Author

Marianna Griffini is an assistant professor in the Department of Politics and International Relations at Northeastern University London, and an affiliate at the College of Social Sciences and Humanities at Northeastern University Boston. Marianna holds a PhD in European and international studies from King's College London. Her research focuses on party politics.

Politics and Governance
2025 • Volume 13 • Article 10437
https://doi.org/10.17645/pag.10437

cogitatio

ARTICLE

Open Access Journal

Offshore Embeddedness Beyond the Wall: Chinese Cloud Providers in Southeast Asia's Data Governance Landscape

Binyi Yang and Mingjiang Li

S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore

Correspondence: Binyi Yang (binyi001@e.ntu.edu.sg)

Submitted: 30 March 2025 **Accepted:** 10 July 2025 **Published:** 19 August 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

Why do middle power states permit companies from institutionally controversial jurisdictions to build and run critical cloud infrastructure on their soil, despite pronounced data governance concerns? How do such firms convert deep suspicion into durable market legitimacy amid intensifying geopolitical competition? Drawing on case studies of Alibaba Cloud and Tencent Cloud across five ASEAN countries (2015–2024), this article proposes the concept of offshore embeddedness: a legitimacy strategy that combines demonstrable separation from home-state control with deep integration into host-state governance structures. Three mechanisms underpin this strategy: regulatory-infrastructure convergence through exhaustive certification and sovereign cloud builds, network integration via stakeholder coalitions that fuse firm survival to domestic political interests, and organizational decoupling accomplished through verifiable legal separation from home-country governance. ASEAN governments shape these outcomes by acting as gatekeeper-regulators (imposing localization and audit preconditions), infrastructure brokers (exchanging market access for domestic data center investment and skills transfer), and coalition orchestrators (embedding foreign clouds within host-led political-economic networks). Through these roles, domestic data governance frameworks shift from exclusionary shields to leverage tools, recalibrating digital governance and binary US–China narratives.

Keywords

ASEAN; Chinese cloud providers; data governance; offshore embeddedness; US–China technological competition

1. Introduction

Data now functions less like a raw production factor and more like a strategic asset, whose custody defines the boundaries of sovereignty, much as the control of sea lanes once did (Chander & Lê, 2014; Ding & Dafoe, 2021). This revaluation has turned rules over storage, processing, and cross-border transfer into prime instruments of statecraft, situating data governance at the center of contemporary great-power competition (X. Chen & Gao, 2024; Christophe et al., 2023; Tang, 2020). Washington and Beijing each leverage export-control lists, security reviews, and market-access vetoes to constrain the other's cloud champions, framing foreign platforms as vectors of surveillance or coercion. Yet, multinational enterprises continue to thread operations through this tightening lattice of restrictions, and—critically—Southeast Asian governments do more than passively watch the contest unfold. How can firms whose home jurisdictions are framed as security risks secure legitimacy abroad, and must ASEAN states merely choose sides, or can they wield domestic data governance clauses to extract investment, technology transfer, and political leverage from competing cloud providers? The rapid ascent of Alibaba Cloud and Tencent Cloud across major ASEAN markets offers a revealing vantage point for answering these questions.

Despite entering the ASEAN market later than Western counterparts, Chinese cloud providers have rapidly expanded their data centers across the region, now outpacing American competitors in physical presence (K. Xu, 2023). Alibaba Cloud and Tencent Cloud currently operate data centers in Thailand, Malaysia, Singapore, and Indonesia, with Alibaba additionally maintaining facilities in the Philippines—a country with ongoing maritime disputes with Beijing and a historically US-aligned stance. In contrast, Amazon Web Services (AWS) operates data centers in Singapore and Indonesia, while its Thailand and Malaysia facilities remain under development. Microsoft Azure maintains a presence in Singapore, with locations in Indonesia and Malaysia pending deployment. Alibaba Cloud's market share in Southeast Asia increased substantially from 3.7% in 2018 to 15.2% in 2023 (Chai, 2024).

These gains were achieved in jurisdictions that explicitly invoke data sovereignty principles to justify localization mandates, licensing requirements, and security audits. While ASEAN governments have not established a shared definition of "data sovereignty," this article uses the term to refer to the assertion of national jurisdiction over data generated within territorial borders, typically implemented through local storage mandates, cross-border transfer restrictions, and national security exemptions that enable governments to control the cross-border movement of data. Indonesian officials have characterized digital sovereignty as essential to preventing digital colonization ("Minister calls for protection," 2022). Vietnam's Cybersecurity Decree 53/2022 mandates in-country storage of regulated data, establishing data localization as a government enforcement mechanism (The Government of Vietnam, 2022). Malaysia's MyDIGITAL blueprint prioritizes building a trusted and secure digital environment, linking cybersecurity to domestic capacity development (Ministry of Communications and Digital, 2021). Thailand requires cross-border data transfers only to destinations with adequate protection standards (Herbert Smith Freehills, 2024), while Singapore mandates comparable protection standards for overseas transfers (Minister for Communications and Information, 2021). These frameworks reflect a regional approach where data governance serves multiple policy objectives beyond privacy protection, creating complex compliance environments for foreign cloud providers. This prompts us to consider the following question: How do Chinese cloud providers achieve market success in ASEAN jurisdictions that have adopted data localization and sovereignty measures often used to curb foreign digital influence?

Three pieces of literature address the presented question but leave it unresolved. International business scholarship explains foreign success through dual embeddedness—cultivating host ties while leveraging home networks (Kostova & Zaheer, 1999; Sun et al., 2012)—yet assumes that institutional distance is bridgeable through firm adaptation, not that home-state laws like China's 2017 Intelligence Law create ongoing sovereignty concerns no conventional strategy can offset. Weaponized interdependence theory shows how hub states exploit network centralities to coerce others (Farrell & Newman, 2019), but it treats firms as passive conduits rather than strategic actors. Polycentric governance research maps how authority disperses across overlapping institutions (Aguerre, 2024; Han, 2024; Kausche & Weiss, 2024), yet it assumes already-legitimate actors and leaves unanswered how controversial-origin firms can convert institutional liabilities into host-state legitimacy.

This article introduces offshore embeddedness: a legitimacy strategy combining demonstrable separation from home-state control with deep integration into host-state governance structures. Through an analysis of Chinese cloud providers across ASEAN's regulatory landscape, we identify three mechanisms that enable firms of controversial origin to transform regulatory scrutiny into a competitive positioning in cloud markets.

2. Controversial Origins and Regulatory Complexity: Chinese Cloud Providers in ASEAN

2.1. Positioning Controversial Origins of Chinese Cloud Providers in its Overseas Expansions

Chinese cloud providers originate from institutional contexts that generate legitimacy deficits in host markets. Three interconnected factors explain why these firms encounter heightened scrutiny that Western competitors avoid.

State-centric data governance conflicts with liberal privacy norms. China's cyber sovereignty framework treats information flows as state territory, subject to party-state oversight, which fundamentally diverges from liberal governance models that emphasize individual rights and consent-based processing (Arner et al., 2022; Gao, 2022). The 2017 Cybersecurity Law operationalized this doctrine through mandatory local storage requirements, creating tensions when Chinese providers enter markets governed by liberal privacy frameworks.

Blurred state-business boundaries raise corporate independence questions. Communist Party committees embedded within nominally private firms create organizational forms where commercial independence and political guidance coexist, challenging traditional public-private distinctions (Pearson et al., 2022). Recent Chinese legal frameworks establish broad expectations that enterprises assist with intelligence work and comply with cross-border data restrictions, making credible demonstrations of state separation difficult in foreign markets that prize corporate autonomy.

Geopolitical competition amplifies technological suspicion. US–China competition has transformed cloud services from commercial offerings into national security considerations, as manifested through initiatives like the Clean Network program, which targets Chinese firms across over 50 countries (Rithmire & Han, 2021). This competitive dynamic means Chinese providers must navigate not only regulatory requirements but broader questions about technological alignment in an increasingly polarized environment.

2.2. ASEAN's Data Governance Landscape

ASEAN's cloud market has expanded significantly in recent years, with public cloud revenues rising by 31.63% since 2019—surpassing the global average of 26.43% (Suruga, 2023). Yet, this surge in market opportunity coexists with a complex regulatory mosaic across member states, which creates substantial legitimacy challenges for foreign cloud providers, particularly those from controversial institutional contexts.

While ASEAN represents a coherent regional economic space with shared digitization goals, the data governance landscape remains highly diversified across member states, creating both challenges and strategic opportunities for multinational cloud providers. Figure 1 highlights substantial variation in both digital trade and data governance metrics, using composite indicators from the Global Data Barometer and Digital Trade Provisions Index. These indicators measure data governance readiness through a weighted aggregation of privacy safeguards, enforcement capabilities, and transparency provisions. The scores range from Singapore's comparatively high overall rating (60%) to Vietnam's more restrictive design (32%), illustrating the regulatory heterogeneity that characterizes the region.

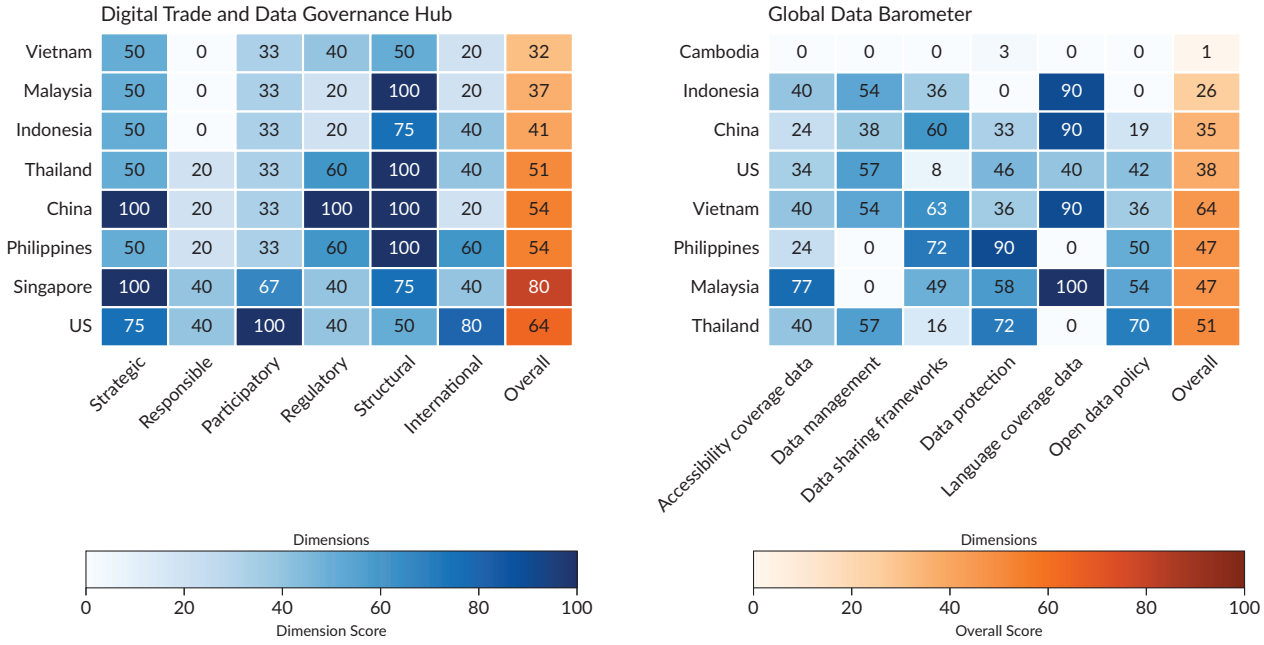


Figure 1. Comparative data governance scores in ASEAN and benchmark countries. Note: Data drawn from the first edition of the Global Data Barometer (2021) and the Digital Trade and Data Governance Hub (2024), selected for their comprehensive ASEAN coverage.

ASEAN's regulatory architecture reveals three characteristics that shape foreign cloud provider operations. Western-influenced governance standards remain deeply embedded across ASEAN, evident in General Data Protection Regulation (GDPR) derived consent-based models and breach-notification requirements in countries such as Malaysia, Singapore, and Thailand (see Supplementary File, Table 1). These frameworks reflect liberal governance philosophies emphasizing individual privacy rights and data subject control. Jurisdictional fragmentation creates complex compliance matrices through regulatory heterogeneity—Indonesia's targeted localization mandates in finance, Vietnam's comprehensive requirements for in-country storage of personal data, and Singapore's permissive approach to cross-border transfers secured by binding

corporate rules. Credible enforcement capacity demonstrates real consequences, as ASEAN regulators possess both legal authority and technical capacity to impose meaningful compliance requirements. Recent enforcement actions demonstrate regulatory capacity: Indonesia blocked major platforms, including Steam and PayPal, for license violations in 2022; Singapore's Personal Data Protection Commission imposed multiple fines on telecommunications providers; and Vietnam conducted comprehensive inspections of TikTok operations in 2023, demanding structural changes.

The intersection of controversial origins with ASEAN's regulatory characteristics creates verification requirements extending beyond routine compliance. Western-influenced standards intensify doctrinal conflicts, requiring Chinese providers to demonstrate credible separation from home-country governance approaches. Jurisdictional fragmentation multiplies verification points, as each jurisdiction applies distinct standards for evaluating independence claims regarding National Intelligence Law obligations and party committee presence. Enforcement capacity creates heightened scrutiny risks where regulatory concerns intersect with geopolitical competition dynamics, precisely targeting the institutional characteristics that define Chinese providers' controversial origins.

3. Literature Review

International business research has long recognized that institutional distance between home and host countries creates systematic barriers for multinational enterprises expanding overseas. Institutional distance encompasses regulatory compliance costs, normative misalignment, and cognitive difficulties in navigating unfamiliar business environments, creating what Kostova and Zaheer (1999) term the "liability of foreignness"—disadvantages faced by foreign firms compared to domestic competitors. These barriers manifest through increased transaction costs, reduced legitimacy with local stakeholders, and difficulties accessing critical resources and information networks (D. Xu & Shenkar, 2002; Zaheer, 1995).

The dominant theoretical solution involves embeddedness and localization strategies that simultaneously cultivate dense ties to host institutions while retaining strong intra-multinational enterprise and home-government linkages to neutralize foreignness penalties. Host-side political and social ties buffer institutional risk by providing access to local knowledge, regulatory influence, and stakeholder networks (Sun et al., 2012). Internal-external embeddedness enhances subsidiary influence and innovation performance through knowledge transfer and resource access (Ciabuschi et al., 2014). This strategic approach assumes that institutional distance represents a bridgeable gap requiring appropriate firm-level responses rather than insurmountable structural barriers.

Research on Chinese firms specifically demonstrates how political connections can facilitate international expansion through multiple channels. Muellner et al. (2017) show that foreign subsidiaries can compensate for institutional disadvantages by integrating deeply into host-country political and social networks, gaining access to local decision-makers, and reducing regulatory uncertainty. Li et al. (2018) demonstrate that Chinese firms with stronger political ties to home governments can better access and leverage intergovernmental diplomatic connections, thereby gaining enhanced access to information, reduced political risks, and increased legitimacy in host countries. These connections operate through formal diplomatic channels, business associations, and informal networks that span public and private sectors.

However, recent research challenges the assumption that political connections provide universal benefits across all institutional contexts. L. Chen et al. (2018) reveal that the efficacy of political networking depends critically on complementary conditions, including firm resources, industry dynamics, and the specific level of institutional distance involved. Their configurational analysis of Chinese high-tech firms demonstrates that different combinations of home political connections, host political connections, research and development capabilities, and internationalization experience are required to overcome high versus low institutional distance. They find that political connections can switch from valuable assets to dispensable strategies—or even liabilities—depending on the institutional context, challenging linear assumptions about distance effects.

This configurational logic suggests that successful international expansion requires a combination of political strategies and firm capabilities, rather than relying on individual solutions. Yet even this sophisticated understanding still presumes that origin represents a manageable handicap once appropriate strategic combinations are deployed—an assumption that breaks down when home-state laws create ongoing sovereignty concerns that no conventional localization strategy can offset.

Weaponized interdependence theory offers a different explanation for multinational enterprise success that shifts the focus from firm-level adaptation to structural network positions under the current geopolitical competition. Farrell and Newman (2019) demonstrate that digital networks exhibit highly centralized structures where states with jurisdiction over central nodes can leverage their positions for strategic advantage through surveillance capabilities and access denial mechanisms. This framework predicts that power flows from hub states, which control network infrastructure, to spoke-states that are dependent on hub-controlled services, suggesting that firm success in international markets depends fundamentally on the strategic positioning of their home states within global networks, rather than on individual firm capabilities.

The theory has been extended to address bipolar competition between US and Chinese digital networks while maintaining core assumptions about hub-state dominance. Lehdonvirta et al. (2025) show that bipolar competition enables spoke-states to exercise choices unavailable in unipolar structures, yet their analysis suggests these choices primarily reflect great-power competition dynamics rather than independent spoke-state agency. China's digital expansion through initiatives like the Digital Silk Road represents hub-state competition for network control rather than empowerment of third countries, with Chinese technology firms serving as instruments of broader geopolitical strategy (Cheney, 2019; Shen, 2018). From this perspective, Chinese technology firms' international success would be explained by China's growing position as a network hub competing with established US dominance rather than firm-level strategic adaptation.

Recent theoretical developments acknowledge significant complications arising from private infrastructure ownership and corporate autonomy that complicate state weaponization capabilities. Gjesvik (2023) demonstrates that ownership-concentrated networks create inherent tensions between commercial interests and strategic objectives that can limit state weaponization capabilities, as private firms resist directives that conflict with profit maximization. Broeders et al. (2025) show that technology companies exercise considerable autonomy in geopolitical contexts, including active resistance to government pressure when it conflicts with business objectives, challenging assumptions about firms as passive conduits of state power.

This perspective receives further support from research on state-firm coordination variations in Chinese corporate internationalization. Oh and No (2020) provide a nuanced framework for understanding the varied patterns of state-firm coordination in China's corporate internationalization, arguing that outcomes depend on complex interactions between firms' foreign direct investment motives and the technology intensity of target industries. Their research on Chinese mergers and acquisitions in Southeast Asia demonstrates that while some transactions involve strong state partnership with elaborate policies and financing, others show more limited alignment or even minimal engagement, supporting the view that Chinese private firms operate as hybrid entities leveraging home-country backing while navigating local sovereignty expectations rather than simply implementing state directives.

He (2024) finds that Chinese technology firms in Indonesia primarily respond to local market conditions rather than implementing state directives, suggesting that commercial adaptation continues to drive firm behavior even in politically sensitive contexts. Yet this framework's emphasis on network topology and hub-state capabilities provides inadequate attention to spoke-state regulatory resources and how these might be leveraged to influence firm behavior. When spoke-states possess significant market opportunities, regulatory authority, or strategic positioning, they may exercise influence that exceeds what network centrality alone would predict, revealing fundamental limitations in both firm-centric international business approaches and state-centric network theories.

Recognizing these limitations, polycentric data governance theory emerged to explain how firms navigate governance authority that is distributed across multiple levels and institutional actors rather than flowing simply from network position or firm adaptation. In polycentric systems, multiple rule-making centers enjoy partial autonomy, adapt to one another, and resolve disputes through shared forums, with no single entity capable of exercising complete control over data flows (McGinnis, 2011; Ostrom, 2010). Aguerre (2024) demonstrates how authority becomes diffused across multiple institutions and jurisdictions in data governance, with overlapping mandates creating institutional complexity where multiple agencies can claim regulatory competence over the same issues.

Firm-level applications reveal dramatically varying outcomes across different jurisdictions and regulatory contexts. Kausche and Weiss (2024) demonstrate how established platforms like Google and Meta successfully captured the EU's Digital Services Act regulatory process through their structural power as digital intermediaries, despite widespread initial demands for strict regulation. Using process-tracing analysis of lobbying activities from 2020 to 2022, they show how these companies leveraged their entrenched position as providers of essential digital infrastructure and employed ideational strategies to shape policy outcomes in their favor, successfully shifting regulatory discourse away from legal accountability toward voluntary responsibility frameworks and preserving technological flexibility by positioning themselves as neutral technical experts.

By contrast, Han (2024) shows how Southeast Asian states exercise strategic agency through selective data localization as economic statecraft, with governments strategically deploying data governance as an economic instrument to achieve political objectives rather than merely responding to security or economic pressures in isolation. Through comparative analysis of Vietnam, Singapore, and Indonesia, Han demonstrates that data localization occurs when states simultaneously experience negative network perception and negative security externalities, with Vietnam's localization reflecting the Communist Party information

control concerns, Singapore's rejection prioritizing its digital hub status, and Indonesia's 2012–2019 policy reversals illustrating evolving state perceptions of technological dependency and security risks.

This framework reveals that state capacity to resist platform power varies significantly based on domestic political calculations within the same global governance system, complicating narratives of either state sovereignty or platform dominance. However, polycentric governance research assumes an arena populated by already-legitimate actors—established Western multinational enterprises in European regulatory processes and long-embedded telecommunications providers in Southeast Asian markets—while treating controversial-origin entrants as analytical afterthoughts rather than central actors requiring theoretical attention.

3.1. Research Gap

None of these explanations fully addresses the empirical puzzle. International business scholarship assumes that institutional distance is bridgeable through conventional adaptation strategies, yet cannot account for cases where home-state laws—such as China's 2017 Intelligence Law—render origin itself a persistent threat that no amount of localization offsets (Kostova & Zaheer, 1999; Sun et al., 2012). Weaponized interdependence theory foregrounds hub-state coercion but reduces firms to passive conduits, underplaying spoke-state regulatory leverage and corporate counter-strategies despite evidence that middle powers and profit-seeking firms continually reshape outcomes (Farrell & Newman, 2019; Gjesvik, 2023).

Polycentric governance research maps distributed authority across multiple actors but assumes an arena populated by already-legitimate incumbents—established Western counterparts and long-embedded telecoms—while treating controversial-origin entrants as analytical afterthoughts (Aguerre, 2024; Han, 2024; Kausche & Weiss, 2024). Consequently, it cannot explain the legitimacy conversion mechanisms we observe in Chinese cloud providers: front-loaded certification, coalition-building with host elites, and multi-tier organizational decoupling that enables data governance screenings and market success across diverse regulatory regimes. Without addressing these gaps, existing frameworks cannot predict why controversial-origin firms succeed where incumbents merely adapt.

4. Methodology

This research employs qualitative comparative case studies with process tracing to examine how Chinese cloud providers operationalize offshore embeddedness across ASEAN's data governance landscape. That, in turn, enables systematic analysis of mechanisms through which controversial-origin firms achieve legitimacy conversion from original liabilities into competitive advantages.

The selection of Alibaba Cloud and Tencent Cloud follows Yin's (2018) theoretical replication logic, testing whether the same framework operates across different organizational contexts. Both share controversial Chinese origins while varying strategically—Alibaba focuses on enterprise digitization through government partnerships, while Tencent emphasizes content services through gaming and entertainment. This variation tests whether offshore embeddedness represents systematic responses to controversial origins rather than firm-specific adaptations. Single-case designs would conflate firm strategies with theoretical mechanisms, limiting generalizability (Eisenhardt & Graebner, 2007).

The five-country design maximizes variation on regulatory stringency while controlling for regional context. Singapore and Malaysia represent mature regulatory environments, Indonesia and Thailand operate as middle-tier regimes, and Vietnam exemplifies restrictive approaches. This systematic variation tests whether mechanisms operate consistently across different regulatory intensities or require specific institutional conditions (Gerring, 2007). Five countries provide sufficient cases to identify patterns while maintaining analytical depth (Ragin, 2014).

Western providers (AWS, Microsoft Azure, and Google Cloud) serve as shadow cases. These firms face identical market opportunities but lack controversial origins, necessitating offshore embeddedness strategies. Shadow case analysis enables identification of which elements represent industry-standard practices versus distinctive responses to legitimacy deficits.

Process tracing examines causal pathways linking institutional challenges to strategic responses to legitimacy outcomes, moving beyond correlation to trace how specific mechanisms generate results (Beach & Pedersen, 2019). Mechanism identification followed iterative analysis across cases and regulatory environments. Initial pattern-matching revealed systematic differences between Chinese and Western approaches. Subsequent analysis clustered these into three coherent strategic responses consistently appearing across firms and markets, then analytically refined these through engagement with our proposed framework.

Analysis draws on corporate documentation (annual reports and regulatory filings), regulatory documentation (national laws and policy announcements), and third-party data (market research and international organizations). The 2015–2024 timeframe captures when Chinese cloud providers started their ASEAN expansions.

5. Analytical Framework: Offshore Embeddedness

5.1. Analytical Foundation: Suchman's Organizational Legitimacy Framework

Suchman's (1995) framework conceptualizes legitimacy as a generalized perception that organizational actions are desirable, proper, or appropriate within socially constructed systems of norms, values, beliefs, and definitions. His framework identifies three legitimacy types: pragmatic legitimacy rests on audience self-interest calculations, moral legitimacy reflects positive normative evaluation of organizational activities, and cognitive legitimacy emerges from comprehensibility and taken-for-grantedness. Suchman addresses legitimacy management through three temporal challenges—gaining, maintaining, and repairing legitimacy through strategic organizational responses.

Building on Suchman's strategic management framework, we identified three core stakeholder questions that controversial-origin firms must address: Can ASEAN regulators believe a Chinese provider will respect their rules? Even if ASEAN regulators trust you technically, who will defend you when politics get rough? And what if Beijing issues an order ASEAN regulators consider incompatible with local requirements? These questions guided our empirical investigation through process-tracing of Alibaba Cloud and Tencent Cloud across five ASEAN markets, producing empirical regularities that pattern-matched into three recurring strategic tasks corresponding to our theoretical questions.

5.2. The Offshore Embeddedness Framework

Offshore embeddedness refers to how controversial-origin firms systematically convert controversial home-country associations into host-state legitimacy assets through simultaneous processes of demonstrable separation from home-country institutional control and deep integration with host-state governance structures and stakeholder networks.

This framework applies when three conditions intersect: institutional controversy, where home-country frameworks may create legal obligations that conflict with host-state sovereignty preferences; business operations involve ongoing access to sensitive data or control over critical digital infrastructure; and host-state regulators possess both the legal authority and technical capacity to monitor and verify organizational separation claims. The framework addresses a security-sensitive legitimacy domain where conventional international business strategies prove insufficient due to heightened suspicion thresholds, persistent security vulnerabilities, and verification imperatives requiring demonstrable rather than communicative evidence of institutional separation.

Guided by three questions inspired by Suchman's (1995) legitimacy theory, the framework rests on three interlocking mechanisms:

1. Compliance signaling through regulatory-infrastructure convergence addresses fundamental credibility deficits by simultaneously pursuing comprehensive certifications and constructing physical infrastructure before revenue justifies such capital expenditure, signaling genuine commitment rather than market opportunism.
2. Network integration via stakeholder coalitions responds to political vulnerability by systematically cultivating financial and reputational stakes among key domestic actors, creating webs of mutual dependence that transform potential adversaries into stakeholders with material interests in continued Chinese presence.
3. Organizational decoupling for jurisdictional assurance addresses core data governance concerns by establishing locally registered entities with genuine legal autonomy, enabling host governments to regulate and enforce against local assets without engaging Chinese parent companies directly.

5.3. Mechanism Analysis

Compliance signaling through regulatory-infrastructure convergence addresses the fundamental credibility deficit facing Chinese technology providers in ASEAN markets. Chinese cloud providers systematically exceed their Western counterparts' regulatory compliance by front-loading both comprehensive certification portfolios and physical data center construction. This strategy diverges from Western incumbents, who typically pursue sequential development—certifying first, then localizing hardware when demand materializes. The simultaneous approach communicates substantial sunk cost commitments to anchor operations under local legal frameworks.

Network integration via stakeholder coalitions manufactures protective coalitions within host countries through direct financial and reputational stakes among government ministries, state-owned enterprises, telecommunications providers, and national champion platforms. Arrangements like Tencent's equity

partnerships with Indonesia's GoTo platform or Alibaba's revenue-sharing agreements in Malaysia's City Brain initiatives create webs of mutual dependence that are costly to unwind, generating Indigenous political protection that transcends formal diplomatic relations.

Organizational decoupling for jurisdictional assurance establishes locally registered entities with genuine legal autonomy, often incorporating local board representation or partnerships with state-linked domestic firms. This structural innovation provides host governments with tangible enforcement mechanisms rather than technical assurances, offering jurisdictional clarity that contrasts with Western providers' reliance on encryption protocols and contractual commitments.

These mechanisms function as complementary layers addressing distinct dimensions of trust and control problems (technical credibility, political backing, and sovereign authority). None alone proves sufficient, but their combination systematically converts Chinese origin from competitive liability into a managed and potentially advantageous market position within ASEAN data governance frameworks.

6. Case Analysis: Offshore Embeddedness in ASEAN's Data Governance Landscape

6.1. Compliance Signaling Through Regulatory-Infrastructure Convergence

Chinese cloud providers neutralize origin-based suspicion in ASEAN by pairing Western-derived compliance with territorially fixed hardware, and by doing so at a greater breadth and speed than their Western counterparts. The mechanism works because it gives regulators a double lock: global best-practice paperwork that they already recognize, plus domestic infrastructure that they can physically police. Drawing on regulation theory (Aglietta, 1979; Lipietz, 1987), capitalist accumulation requires institutional coherence between sectoral strategies and the broader mode of regulation—the ensemble of institutional forms that stabilizes inherently contradictory accumulation processes (Boyer, 2005). When the dominant rulebook for cloud services in ASEAN is a Euro-American compliance assemblage, Chinese providers seek legitimacy by integrating into the status quo. By combining Western-authored certifications with territorially embedded infrastructure, Alibaba Cloud and Tencent Cloud align their operations with the prevailing mode of regulation and thereby neutralize the liability of authoritarian origin.

Procedural convergence comes first. Alibaba became the world's inaugural cloud provider to hold all three Singapore Infocomm Media Development Authority data-protection marks (Data Protection Trustmark, APEC Cross-Border Privacy Rules, and APEC Privacy Recognition for Processors) in June 2021, only four years after setting up shop in the city-state (Alibaba Cloud, 2021). Table 1 shows that by 2024, both Alibaba and Tencent have displayed the full package, including International Organization for Standardization/ International Electrotechnical Commission (ISO/IEC) 27001, 27017, and 27018 standards for information security management, the Payment Card Industry Data Security Standard (PCI-DSS) Level 1 for payments, the Cloud Security Alliance Security, Trust & Assurance Registry (CSA STAR) certification for cloud security, and the Health Insurance Portability and Accountability Act (HIPAA) controls for health data—bringing them to parity with AWS on every audit ASEAN regulators routinely reference, bringing them to parity with AWS on every audit ASEAN regulators routinely reference. Because each badge is issued by an independent European or US assessor, the audits externalize trust: host officials need not take Beijing's word, only the regulator's.

Table 1. Comparative certifications of major cloud service providers in information security, privacy, and compliance (June 2025 data).

Certification category	AWS	Alibaba Cloud	Tencent Cloud	Standard origin	Governing body/authority
Information security	ISO/IEC 27001, 27017, 27018, and 27701	ISO/IEC 27001, 27017, 27018, 27701	ISO/ IEC 27001, 27017, 27018, 27701	Switzerland/ EU-led international collaboration	ISO (Geneva) and IEC
Privacy and data protection	General Data Protection Regulation(GDPR) and California Consumer Privacy Act(CCPA)	GDPR	GDPR	EU	European Data Protection Board
Financial services	PCI DSS Level 1, SOC 1/2/3	PCI DSS, SOC 1/2	PCI DSS, SOC 1/2	US-based global financial institutions	Payment Card Industry Security Standards Council (US) and American Institute of Certified Public Accountants (US)
Cloud security	CSA STAR Level 2	CSA STAR	CSA STAR	US-based global alliance	Cloud Security Alliance (US)
Industry-specific	Federal Risk and Authorization Management Program (FedRAMP), HIPAA, and MTCS	HIPAA and Multi-Tier Cloud Security (MTCS)	HIPAA and MTCS	US (HIPAA) and Singapore (MTCS)	US Department of Health and Infocomm Media Development Authority (IMDA) Singapore

Note: Data was compiled from corporate disclosures as of June 2025 and verified with certification authorities.

The breadth of that portfolio matters because the majority standard is Western in origin. Far from advancing a "China model," the firms prove they can inhabit the status quo ante more completely—and, crucially, more rapidly—than their US counterparts. Alibaba and Tencent attach sovereign plug-ins such as Singapore's MTCS Level-3 and OSPAR banking mark at launch, whereas AWS obtained MTCS earlier (in 2014) but added the financial-sector OSPAR mark only after it had already captured most regional workloads. Swift, full-stack adoption turns regulatory screening into a formality, demonstrating that controversial provenance need not predict divergent practice.

Compliance on paper becomes credible only when the servers themselves stay inside national borders. Alibaba opened its first overseas region and global cloud headquarters in Singapore in August 2015, then rolled out Kuala Lumpur (2017), Jakarta (2018), Bangkok (2022), and Ho Chi Minh City (2024), amassing nine availability

zones across the five study markets. Each launch embeds hyperscale hardware worth roughly $50 million (Swinhoe, 2023). Those nodes give regulators what the audits cannot: physical jurisdiction, inspection rights, and an emergency switch.

Tencent launched its first Indonesian data-center region in Jakarta in April 2021 and declared the facility fully operational the day it opened. The plant sits in the capital's central business district, runs dual utility feeds plus N+1 diesel capacity, and already hosts Bank Neo Commerce and JOOX streaming workloads (Swinhoe, 2021a). Tencent has since added second availability zones in Bangkok and pledged $500 million for a third Jakarta site by 2030 in collaboration with Telkomsel—a joint-venture structure that ties foreign capital to domestic political patrons (Swinhoe, 2021b).

Western incumbents, with first-mover advantages, act more slowly. AWS, Microsoft, and Google long served most ASEAN traffic from a 2010 Singapore hub; only in May 2024 did AWS announce a further $12 billion build-out through 2028 (Amazon, 2024). The contrast is not mere chronology but sequencing: Chinese firms saturate every major jurisdiction once they commit, pre-empting sovereignty objections, while US competitors add sovereign capacity reactively as market pressure intensifies.

Certifications externalize trust through third-party audits; bricks and mortar turn that symbolic assurance into an enforceable reality. Maintaining overlapping audits and sovereign-grade regions is costly, yet that very expense makes the signal credible: revocation would strand capital and invalidate certifications, aligning the providers' incentives with state demands. ASEAN governments reward the double lock with cloud-first procurement, national AI sandboxes, and flagship smart-city contracts, turning gatekeepers into stakeholders and demonstrating how spoke-states can weaponize interdependence from below.

Regulatory-infrastructure convergence, therefore, supplies the institutional "permission to operate" on which offshore embeddedness rests. It shows that when controversial-origin firms fully internalize the dominant rule system—procedurally and materially—they not only defuse geopolitical suspicion but also embed themselves so deeply that expulsion becomes costlier for host states than disciplined inclusion. The next section traces how Alibaba and Tencent leverage that granted legitimacy to assemble durable political-economic coalitions across Southeast Asia's fragmented data-governance landscape.

6.2. Network Integration via Stakeholder Coalitions

Controversial-origin cloud providers convert provisional regulatory approval into durable legitimacy by embedding themselves in host-country political and economic circuits. They form stakeholder coalitions—ministries, state-owned enterprises, and national-champion platforms—that acquire direct financial or reputational stakes in uninterrupted service provision, thereby transforming sovereignty anxieties into incentives for protection.

Indonesia furnishes a national-scale illustration. On 10 November 2024, GoTo Group, Tencent Cloud, and Alibaba Cloud concluded a tripartite pact—witnessed by President Prabowo Subianto—to expand domestic infrastructure and train Indonesian engineers ("Indonesia's GoTo, China's Tencent," 2024). Because GoTo underpins e-commerce, ride-hailing, and digital payments for millions of citizens, its dependence on Chinese clouds renders service continuity a quasi-public good; any disruption would entail immediate political costs

for the presidency and for GoTo's sovereign-wealth shareholders in Abu Dhabi and Singapore. Presidential endorsement thus elevates a commercial contract into a broad coalition linking executive authority, capital markets, and everyday users.

In Malaysia, the same outcome emerges through divergent templates. The Kuala Lumpur City Brain initiative, launched in 2018 by Alibaba Cloud and the Malaysia Digital Economy Corporation, required extensive algorithmic tailoring to local traffic regulations and infrastructural particularities (Farhan, 2018; Tan, 2018). The pilot phase reduced travel times by 12% (Azhar, 2019) while simultaneously developing Malaysian AI expertise and embedding Alibaba engineers in municipal routines. Tencent adopted a locally owned operator model: in August 2024, it partnered with Global Resources Management to create Alto Cloud, an internet-data-center campus in Cyberjaya that delivers more than 400 Tencent Cloud services through a Cloud Dedicated Zone architecture (Tencent Cloud, 2024). Because Malaysian capital retains equity control and front-end customer relationships, any sweeping restrictions on Tencent would inflict losses on domestic investors as well as the foreign entrant, dampening enthusiasm for exclusionary measures.

Vietnam underscores the value of coalition-based embedding under restrictive regulation. Alibaba leases capacity from Viettel and VNPT—state telcos that supply the bulk of national data-centre space—thereby situating foreign infrastructure within entities already entrusted with defence and public-security workloads (Nguyen, 2024). Tencent is negotiating a similar telecom-anchored entry. Embedding within incumbents that carry sovereign mandates provides an additional layer of political cover that greenfield builds would lack.

Western incumbents follow a different trajectory. AWS's $12 billion Singapore expansion and its $5 billion Jakarta investment are financed entirely from its Seattle headquarters, offering no equity shares to domestic state-owned enterprises (Amazon, 2024; Spencer, 2021). Microsoft's $2.2 billion Malaysia West region is likewise wholly owned, with local participation limited to skill memoranda of understanding (Microsoft, 2024). Even where AWS involves local firms, it relies on reseller tiers rather than joint-equity vehicles. This arm's-length posture contrasts with the equity joint ventures, smart-city pilots, and telecom co-location strategies that enable Chinese providers to cultivate mutual dependence.

Stakeholder coalitions thus reclassify Chinese clouds from potential political threats to development partners whose success is intertwined with influential domestic constituencies. Once ride-hailing dispatch, instant payment systems, or urban-mobility algorithms run on a Chinese platform, any interruption would impose immediate economic pain—and likely electoral repercussions—on host governments. The upfront costs borne by Alibaba and Tencent (e.g., seeding city Brain capabilities before revenue, accepting equity dilution, and pledging US$500 million for a third Jakarta availability zone) signal long-horizon commitment and solidify elite support. Network integration, therefore, deepens offshore embeddedness beyond rule compliance: audited certifications and onshore hardware secure the initial "permission to operate," while mutually dependent coalitions convert that permission into a political shield against future nationalist backlash.

6.3. Organizational Decoupling for Jurisdictional Assurance

Organizational decoupling secures host-state trust by embedding legal authority and day-to-day decision-making within the jurisdiction that grants market access. Rather than asking regulators to rely on

contractual promises, Chinese cloud providers create legally distinct regional units, whose boards, bank accounts, and compliance functions are governed by local law. This structural separation provides a concrete guarantee that Beijing cannot unilaterally override ASEAN statutes, completing the legitimation work begun by regulatory-infrastructure convergence and coalition building.

Alibaba Cloud pursues a headquarters-relocation model that recenters control in Singapore. In August 2015, the company registered Alibaba Cloud (Singapore) Pte Ltd as an independent holding company with its own directors and data-protection officers, thereby shifting oversight of all Southeast-Asian activities from Hangzhou to Singapore. Subsequent ventures, such as Indonesia's data-center cluster, which opened in February 2018, and the Fusionex partnership, which was signed in Malaysia in September 2017, report to this entity—not to the Chinese parent. By bringing corporate governance under Singaporean company law and the Personal Data Protection Act, Alibaba supplies regulators with a single, locally accountable node to which fines, audits, or suspension orders can be directed.

Tencent Cloud deploys a partner-anchored model that assigns contractual liability to domestic firms. In Thailand, the company signed a memorandum of understanding with Bangkok-listed systems integrator MFEC, stipulating that MFEC—not Tencent—acts as the counterparty for all public-sector and regulated-industry customers (MFEC, 2024). A parallel agreement in March 2025 designated state-affiliated Telkomsel as the front-end operator for a third Jakarta availability zone, while Tencent remains the platform licensor (Telkomsel, n.d.). These arrangements locate service-level guarantees, data-handling obligations, and tax reporting within entities answerable to Thai and Indonesian courts, leaving Tencent one step removed from coercive jurisdiction without relinquishing technical control.

ASEAN regulators value these structures because they convert abstract assurances into enforceable rights. Duplicate boards, autonomous compliance teams, and locally held assets allow officials to inspect shareholder registers, subpoena records, or revoke licenses without engaging Chinese authorities. Should geopolitical tensions escalate, ministries can compel the regional subsidiary or joint-venture partner to sever cross-border links or migrate sensitive workloads—actions that would be politically and technically costlier if the cloud were managed directly from China. Organizational decoupling thus realigns bargaining power, giving middle power states a credible "off switch" that is consistent with their sovereignty claims.

For Alibaba and Tencent, the additional administrative layers represent a calculated investment in political insurance. The expense of parallel governance structures is offset by access to government contracts, finance, healthcare, and other data-sensitive sectors that would remain out of reach without a demonstrable local accountability mechanism. By institutionalizing a locally enforceable chain of accountability, the providers turn what would otherwise be a unilateral compliance cost into a market differentiator, signaling to risk-averse corporate and public clients that their data will remain unequivocally subject to domestic law.

The absence of comparable measures among US and European competitors underscores that decoupling is a context-specific response to contested institutional origins rather than an industry-wide norm. Providers domiciled in GDPR or Cloud-Act jurisdictions already enjoy presumptive equivalence in ASEAN law; regulators address residual concerns through existing treaties and audit regimes rather than demanding local reincorporation. The contrast highlights why organizational decoupling is central to the offshore embeddedness of Chinese clouds: it addresses a credibility gap that arises only when the

provider's home legal system is treated as politically or juridically incompatible with the host state's data governance requirements.

7. Conclusion

This article challenges prevailing narratives of US–China technological competition by demonstrating how middle powers and non-state actors reshape data governance outcomes through strategic bargaining rather than passive alignment. The puzzle of Chinese cloud providers' success in ASEAN markets reveals that firms of controversial origin can convert institutional liabilities into competitive advantages, while middle powers exercise agency that transcends binary great power choices.

Offshore embeddedness explains this transformation through three complementary mechanisms. Regulatory-infrastructure convergence establishes technical credibility by exceeding Western competitors' compliance standards while embedding territorially fixed assets. Network integration via stakeholder coalitions manufactures domestic political protection by creating webs of mutual dependence among government ministries, state enterprises, and national platforms. Organizational decoupling provides jurisdictional assurance through locally accountable legal structures that give host governments enforceable control mechanisms. Together, these mechanisms enable firms of controversial origin to systematically convert data skepticism into managed market positions.

This framework advances understanding of technological competition in three ways. First, it reveals that firm legitimacy in contested domains depends less on home-country advantages than on strategic adaptation to host-state governance preferences. Chinese cloud providers have succeeded not by leveraging Beijing's network position but by demonstrating credible separation from it—challenging both international business assumptions about bridgeable institutional distance and weaponized interdependence theories treating firms as passive state conduits.

Second, the analysis exposes how middle powers exercise structural agency through sophisticated regulatory strategies. ASEAN governments do not merely choose between US and Chinese technological ecosystems; they actively recalibrate these choices by demanding simultaneous satisfaction of technical, political, and legal conditions. As gatekeeper-regulators, they control market entry through calibrated licensing; as infrastructure brokers, they convert regulatory consent into tangible national assets; and as coalition orchestrators, they embed foreign providers within domestic networks that align commercial success with development objectives.

Third, data governance frameworks function as leverage tools rather than defensive barriers. Rather than excluding controversial providers, sophisticated regulatory regimes enable selective inclusion on terms that maximize host-state benefits while minimizing sovereignty risks. This contradicts assumptions that middle powers must simply adapt to great power competition and demonstrates how they extract strategic value from technological rivalry.

The research illuminates the critical role of non-state actors in mediating competition outcomes. Chinese providers' success depends fundamentally on cultivating stakeholder coalitions in host countries with direct financial stakes in continued service provision. When ride-hailing platforms, payment systems, and smart

cities depend on Chinese infrastructure, disruption becomes politically costly regardless of geopolitical tensions. Indonesian President Prabowo's endorsement of the GoTo–Tencent–Alibaba partnership, Malaysia's integration of Alibaba's City Brain, and Vietnam's embedding of Chinese clouds within state telecoms all demonstrate how non-state stakeholders create constituencies for technological cooperation transcending formal government relations.

Future research should examine whether offshore embeddedness operates across different technological domains and regional contexts, track how intensifying competition affects middle power agency, and quantitatively analyze the marginal effects of individual mechanisms across institutional conditions.

The broader significance extends beyond Southeast Asia to challenge assumptions about technological competition in a multipolar world. Rather than bipolar division into competing technological spheres, we observe complex landscapes where middle powers leverage regulatory authority to extract benefits while maintaining flexibility, and Chinese firms succeed through offshore embedding within host data governance landscapes—operating beyond Beijing's direct control rather than implementing its preferences. This suggests future data and technology governance will be characterized by polycentric authority structures where middle powers and non-state actors exercise significant influence. Understanding these complex bargaining relationships, rather than focusing solely on great power competition, will be essential for predicting how critical technologies are governed. The politics of digital infrastructure are not predetermined by Washington or Beijing but emerge from strategic interactions across diverse stakeholders and contexts.

Acknowledgments

We are grateful for the constructive comments from external reviewers and from participants of the thematic issue workshop, which have substantially improved this article.

Funding

This research is supported by the Ministry of Education, Singapore, under its Academic Research Fund Tier 1 (RG50/23).

Conflict of Interests

The authors declare no conflict of interests.

LLMs Disclosure

We used OpenAI's ChatGPT-01 and Anthropic's Claude Sonnet 4 to assist with polishing the language in the final draft.

Supplementary Material

Supplementary material for this article is available online in the format provided by the authors (unedited).

References

Aglietta, M. (1979). *A theory of capitalist regulation: The U.S. experience*. Schocken Books.

Aguerre, C. (2024). Internet interoperability and polycentric attributes in global digital data ordering. In C. Aguerre, M. Campbell-Verduyn, & J. A. Scholte (Eds.), *Global digital data governance: Polycentric perspectives* (pp. 34–50). Routledge. https://doi.org/10.4324/9781003388418-4

Alibaba Cloud. (2021). *Alibaba Cloud secures all three data protection certifications in Singapore*. https://www.alibabacloud.com/en/press-room/alibaba-cloud-secure-all-three-data-protection-certifications-in-singapore

Amazon. (2024). *AWS deepens commitment to Singapore with additional S$12 billion investment by 2028 and new flagship AI programme*. https://www.aboutamazon.sg/news/aws/aws-deepens-commitment-to-singapore-with-additional-sg-12-billion-investment-by-2028-and-new-flagship-ai-programme

Arner, D. W., Castellano, G. G., & Selga, E. K. (2022). The transnational data governance problem. *Berkeley Technology Law Journal*, *37*, Article 623.

Azhar, K. (2019, October 30). Tech: Alibaba Cloud's City Brain could reduce KL travel time by 12%. *The Edge Malaysia*. https://www.theedgemarkets.com/article/tech-alibaba-clouds-city-brain-could-reduce-kl-travel-time-12

Beach, D., & Pedersen, R. B. (2019). *Process-tracing methods: Foundations and guidelines* (2nd ed.). University of Michigan Press.

Boyer, R. (2005). How and why capitalisms differ. *Economy and Society*, *34*(4), 509–557.

Broeders, D., Sukumar, A., Kello, M., & Andersen, L. H. (2025). Digital corporate autonomy: Geo-economics and corporate agency in conflict and competition. *Review of International Political Economy*, *32*(4), 1189–1213. https://doi.org/10.1080/09692290.2025.2468308

Chai, X. (2024, February 13). Alibaba Cloud has pressed the acceleration button for external expansion. *Moomoo*. https://www.moomoo.com/news/post/49172740/alibaba-cloud-has-pressed-the-acceleration-button-for-external-expansion?level=2&data_ticket=1753874376318849

Chander, A., & Lê, U. P. (2014). Data nationalism. *Emory Law Journal*, *64*, 677–739.

Chen, L., Li, Y., & Fan, D. (2018). How do emerging multinationals configure political connections across institutional contexts? *Global Strategy Journal*, *8*(3), 447–470. https://doi.org/10.1002/gsj.1187

Chen, X., & Gao, X. (2024). The regime complex for digital trade in Asia and China's engagement. *Asia Europe Journal*. Advance online publication. https://doi.org/10.1007/s10308-024-00705-0

Cheney, C. (2019). *China's Digital Silk Road: Strategic technological competition and exporting political illiberalism*. Council on Foreign Relations. https://www.cfr.org/blog/chinas-digital-silk-road-strategic-technological-competition-and-exporting-political

Christophe, B., Giron, A., & Verin, G. (2023). A comparative analysis with machine learning of public data governance and AI policies in the European Union, United States, and China. *Journal of Intelligence Studies in Business*, *13*(2), 61–74.

Ciabuschi, F., Holm, U., & Martín, O. M. (2014). Dual embeddedness, influence and performance of innovating subsidiaries in the multinational corporation. *International Business Review*, *23*(5), 897–909. https://doi.org/10.1016/j.ibusrev.2014.02.002

Digital Trade and Data Governance Hub. (2024). *Global data governance mapping project*. https://globaldatagovernancemapping.org

Ding, J., & Dafoe, A. (2021). The logic of strategic assets: From oil to AI. *Security Studies*, *30*(2), 182–212. https://doi.org/10.1080/09636412.2021.1915583

Eisenhardt, K. M., & Graebner, M. E. (2007). Theory building from cases: Opportunities and challenges. *Academy of Management Journal*, *50*(1), 25–32.

Farhan. (2018, January 29). MDEC and DBKL partner with Alibaba to deploy traffic management AI platform. *Lowyat.NET*. https://www.lowyat.net/2018/153685/mdec-dbkl-partner-alibaba-deploy-traffic-management-ai-platform

Farrell, H., & Newman, A. L. (2019). Weaponized interdependence: How global economic networks shape state coercion. *International Security*, *44*(1), 42–79.

Gao, X. (2022). An attractive alternative? China's approach to cyber governance and its implications for the Western model. *The International Spectator*, *57*(3), 15–30.

Gerring, J. (2007). *Case study research: Principles and practices*. Cambridge University Press.

Gjesvik, L. (2023). Digital choke-points and the limits of state power. *Survival*, *65*(2), 85–108.

Global Data Barometer. (2021). *Global Data Barometer: First edition*. https://firstedition.globaldatabarometer.org

Han, S. (2024). Data and statecraft: Why and how states localize data. *Business and Politics*, *26*(2), 263–288. https://doi.org/10.1017/bap.2023.41

He, Y. (2024). Chinese digital platform companies' expansion in the Belt and Road countries. *The Information Society*, *40*(2), 96–119. https://doi.org/10.1080/01972243.2024.2317058

Herbert Smith Freehills. (2024). *Thailand's new legislation on cross-border transfer of personal data*. https://www.herbertsmithfreehills.com/notes/data/2024-01/thailands-new-legislation-on-cross-border-transfer-of-personal-data

Indonesia's GoTo, China's Tencent, Alibaba agree on cloud infrastructure development. (2024, November 10). *The Business Times*. https://www.businesstimes.com.sg/international/asean/indonesias-goto-chinas-tencent-alibaba-agree-cloud-infrastructure-development

Kausche, K., & Weiss, M. (2024). Platform power and regulatory capture in digital governance. *Business and Politics*, *27*(2), 284–308. https://doi.org/10.1017/bap.2024.33

Kostova, T., & Zaheer, S. (1999). Organizational legitimacy under conditions of complexity: The case of the multinational enterprise. *Academy of Management Review*, *24*(1), 64–81.

Lehdonvirta, V., Wú, B., & Hawkins, Z. (2025). Weaponised interdependence in a bipolar world: How economic forces and security interests shape the global reach of US and Chinese cloud data centres. *Review of International Political Economy*. Advance online publication. https://doi.org/10.1080/09692290.2025.2489077

Li, J., Meyer, K. E., Zhang, H., & Ding, Y. (2018). Diplomatic and corporate networks: Bridges to foreign locations. *Journal of International Business Studies*, *49*(6), 659–683.

Lipietz, A. (1987). *Mirages and miracles: The crises of global Fordism*. Verso.

McGinnis, M. D. (2011). An introduction to IAD and the language of the Ostrom workshop: A simple guide to a complex framework. *Policy Studies Journal*, *39*(1), 169–183.

MFEC. (2024). *MFEC signed MoU with Tencent Cloud to drive technological innovation in Thailand and globally*. https://www.mfec.co.th/en/success-stories/mfec-mou-tencent-cloud

Microsoft. (2024). *Microsoft announces US$2.2 billion investment to fuel Malaysia's cloud and AI transformation*. https://news.microsoft.com/apac/2024/05/02/microsoft-announces-us2-2-billion-investment-to-fuel-malaysias-cloud-and-ai-transformation

Minister calls for protection of Indonesia's digital sovereignty. (2022, August 17). *Antara*. https://en.antaranews.com/news/246946/minister-calls-for-protection-of-indonesias-digital-sovereignty

Minister for Communications and Information. (2021). *Personal data protection (notification of data breaches) regulations 2021*. Singapore Statutes Online. https://sso.agc.gov.sg/SL/PDPA2012-S64-2021

Ministry of Communications and Digital. (2021). *Malaysia digital economy blueprint (MyDIGITAL)*. Government of Malaysia.

Muellner, J., Klopf, P., & Nell, P. C. (2017). Trojan horses or local allies: Host-country national managers in developing-market subsidiaries. *Journal of International Management*, *23*(3), 306–325. https://doi.org/10.1016/j.intman.2016.12.001

Nguyen, K. (2024, May 2). Alibaba plans $1 billion data centre in Vietnam. *Vietnam Investment Review*. https://vir.com.vn/alibaba-plans-1-billion-data-centre-in-vietnam-110812.html

Oh, Y. A., & No, S. (2020). The patterns of state-firm coordination in China's private sector internationalization: China's mergers and acquisitions in Southeast Asia. *The Pacific Review*, *33*(6), 873–899.

Ostrom, E. (2010). Beyond markets and states: Polycentric governance of complex economic systems. *American Economic Review*, *100*(3), 641–672.

Pearson, M. M., Rithmire, M., & Tsai, K. S. (2022). China's party-state capitalism and international backlash: From interdependence to insecurity. *International Security*, *47*(2), 135–176.

Ragin, C. C. (2014). *The comparative method: Moving beyond qualitative and quantitative strategies*. University of California Press.

Rithmire, M., & Han, C. (2021). *The clean network and the future of global technology* competition. Harvard Business School Case.

Shen, H. (2018). Building a Digital Silk Road? Situating the internet in China's Belt and Road Initiative. *International Journal of Communication*, *12*, 2683–2701.

Spencer, L. (2021, December 13). AWS launches Indonesia cloud region, pledges $5B investment. *Channel Asia*. https://www.channelasia.tech/article/1266775/aws-launches-indonesia-cloud-region-pledges-5b-investment.html

Suchman, M. C. (1995). Managing legitimacy: Strategic and institutional approaches. *Academy of Management Review*, *20*(3), 571–610.

Sun, P., Mellahi, K., & Wright, M. (2012). The contingent value of corporate political ties. *Academy of Management Perspectives*, *26*(3), 35–52. https://doi.org/10.5465/amp.2011.0164

Suruga, T. (2023, November 15). Southeast Asia's digital battle: Chinese and U.S. big tech face off over $1tn market. *Nikkei Asia*. https://asia.nikkei.com/Spotlight/The-Big-Story/Southeast-Asia-s-digital-battle-Chinese-and-U.S.-Big-Tech-face-off-over-1tn-market

Swinhoe, D. (2021a, April 12). Tencent Cloud launches first data center in Jakarta, Indonesia. *Data Centre Dynamics*. https://www.datacenterdynamics.com/en/news/tencent-cloud-launches-first-data-center-in-jakarta-indonesia

Swinhoe, D. (2021b, June 3). Tencent opens four new availability zones in Asia and Europe. *Data Centre Dynamics*. https://www.datacenterdynamics.com/en/news/tencent-opens-four-new-availability-zones-in-asia-and-europe

Swinhoe, D. (2023, October 11). NTT launches data center in Cyberjaya, Malaysia. *Data Centre Dynamics*. https://www.datacenterdynamics.com/en/news/ntt-launches-data-center-in-cyberjaya-malaysia

Tan, D. (2018). *Alibaba brings 'City Brain' traffic control system to KL*. Paul Tan. https://paultan.org/2018/01/30/alibaba-to-set-up-ai-traffic-control-system-for-kl-traffic

Tang, M. (2020). Huawei versus the United States? The geopolitics of exterritorial internet infrastructure. *International Journal of Communication*, *14*, 4556–4577.

Telkomsel. (n.d.). *Telkomsel and Tencent Cloud develop AI and cloud solutions to enhance customer experience*. https://www.telkomsel.com/en/about-us/news/telkomsel-and-tencent-cloud-develop-ai-and-cloud-solutions-enhance-customer

Tencent Cloud. (2024). *Alto Cloud grand launching 2024—Powered by Tencent Cloud, Alto Cloud joins the Malaysian market as a full-service cloud solutions provider*. https://www.tencentcloud.com/dynamic/news-details/100594

The Government of Vietnam. (2022). *Elaborating a number of articles of the law on cybersecurity of Vietnam* (Decree No. 53/2022/ND-CP). https://thuvienphapluat.vn/van-ban/EN/Cong-nghe-thong-tin/Decree-53-2022-ND-CP-elaborating-the-Law-on-cybersecurity-of-Vietnam/527750/tieng-anh.aspx

Xu, D., & Shenkar, O. (2002). Institutional distance and the multinational enterprise. *Academy of Management Review*, *27*(4), 608–618.

Xu, K. (2023). *US vs China: A cloud proxy war*. Interconnected. https://interconnected.blog/us-vs-china-a-cloud-proxy-war

Yin, R. K. (2018). *Case study research: Design and methods* (6th ed.). Sage.

Zaheer, S. (1995). Overcoming the liability of foreignness. *Academy of Management Journal*, *38*(2), 341–363.

About the Authors

Binyi Yang is a PhD candidate at the S. Rajaratnam School of International Studies, Nanyang Technological University, Singapore. Her research explores state-business relationships in China's technological development, with a focus on clean-tech sectors, subnational dynamics, and the global expansion strategies of Chinese firms.

Mingjiang Li is an associate professor and Provost's Chair in international relations at S. Rajaratnam School of International Studies (RSIS), Nanyang Technological University, Singapore. His main research interests include Chinese foreign policy, China–ASEAN relations, Sino–US relations, and Asia-Pacific security.

Politics and Governance
2025 • Volume 13 • Article 10429
https://doi.org/10.17645/pag.10429

cogitatio

ARTICLE

Open Access Journal

Data Governance in the Geopolitics of Energy Transition: Comparing Regional Energy Cooperation in ASEAN and the EU

Kaho Yu [1], Jinseok Sung [2], and Yunheng Zhou [3]

[1] Asia Carbon Institute, Singapore
[2] Energy Studies Institute, National University of Singapore, Singapore
[3] School of Public Affairs, Zhejiang University, China

Correspondence: Yunheng Zhou (yunhengzhou@zju.edu.cn)

Submitted: 29 March 2025 **Accepted:** 14 May 2025 **Published:** 20 August 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

Data governance has become a critical enabler in the geopolitics of energy transition, influencing regional cooperation, energy security, and climate leadership. This article compares the contrasting approaches of the European Union and ASEAN to data governance in the context of energy transition and examines their geopolitical implications. The EU's centralised model is underpinned by strong institutional capacity, policy alignment, interdependence among member states, and political will. These conditions support robust data governance across regional power grids, critical raw material supply chains, and carbon markets, enhancing the EU's energy resilience and influence in global climate standard-setting. In contrast, despite advancing regional energy initiatives, ASEAN's decentralised and informal approach to data governance presents both opportunities and challenges for deepening regional data integration. Through comparative case studies, this article investigates how energy data governance is both shaped and reshapes the geopolitics of energy transition.

Keywords

carbon market; critical raw materials; data governance; energy transition; power grid

1. Introduction

Energy and geopolitics are deeply intertwined and the global energy transition is reshaping these geopolitical dynamics, with data governance taking on an increasingly critical role (Ansari et al., 2025; Ashford, 2024). While energy geopolitics has traditionally focused on fossil fuel access, supply security, and chokepoints, the Ukraine war has prompted many countries, especially in Europe, to reduce reliance on Russian energy and

accelerate their energy transitions. This shift reflects the growing significance of the geopolitics of the energy transition, centred on regional decarbonisation efforts such as power grids, critical raw material (CRM) supply chains, and carbon markets. As these efforts become increasingly transboundary and interconnected, data governance is emerging as a key enabler underpinning regional cooperation in the energy transition (Beltramo et al., 2024; Garske et al., 2024; Wang et al., 2023). Robust data governance ensures cross-border data sharing in regional power grids, mineral supply chain coordination, and standardised carbon accounting frameworks. In contrast, the lack of cohesive governance frameworks introduces risks that could undermine progress, such as politically sensitive data sovereignty, limited data availability for strategic resources, and disparities in data standards. These challenges highlight the geopolitical stakes of regional energy cooperation, which this article analyses through the lens of regional integration.

This article addresses an underexplored dimension of the geopolitics of energy transition by examining the role of data governance through a comparative analysis of the EU and ASEAN. These two regions are selected as contrasting cases: the EU operates under a supranational governance model with strong institutional enforcement, whereas ASEAN functions through intergovernmental coordination and non-binding consensus. Their differing governance structures offer a valuable foundation for analysing how data governance shapes regional cooperation and the geopolitics of energy transition. This article first explores the role of data governance in energy transition, with a focus on cross-border power grids, mineral supply chains, and carbon markets. A comparative analysis of the EU and ASEAN follows, highlighting the institutional and geopolitical factors that define their contrasting data governance models. The article concludes by reflecting on the broader geopolitical implications of data governance in regional energy cooperation.

2. Data Governance in the Geopolitics of Energy Transition

The geopolitics of energy has evolved from traditional concerns over fossil fuel security to new forms of interdependency driven by the rapid development of the energy transition. Geopolitical concerns once centred on fossil fuels—shaping global trade patterns, strategic alliances, and national security strategies—have now extended to energy transition-related technologies, resources, and market standards (Scholten, 2024). As energy systems undergo structural change, three decarbonisation trends are redefining the geopolitical landscape. First, power grids have become the backbone for scaling renewable use and integration (IRENA, 2024; Wang et al., 2023), creating new forms of cross-border interdependency. Second, energy security concerns are shifting from fossil fuels to critical minerals, essential for clean energy technologies (IEA, 2021), intensifying competition for CRMs (Nakano, 2020; Yu, 2023b). Third, tightening environmental regulations are accelerating the development of carbon markets, where competition over market standards between developed and developing countries is shaping global climate governance (Li & Kim, 2024; Lo & Yu, 2024; Wu, 2023). These trends illustrate how the energy transition is transforming not only energy systems but also the foundations of geopolitical strategy.

These emerging energy trends have introduced new forms of interdependence that reshape traditional geopolitical dynamics. As IRENA (2023) highlights, these new interdependencies can not only foster cooperation but also heighten tensions. Scholars such as O'Sullivan (2017, 2023) argue that these shifts have introduced new sources of geopolitical tension—including fragmented cooperation, uneven access to clean technologies, rising resource nationalism, and regulatory divergence—which complicate rather than resolve existing energy security concerns. The geopolitics of the energy transition is increasingly shaped by

state-led industrial policies, regional bloc formation, technological innovation, and market standard competition—all of which influence how the benefits and risks of decarbonisation are distributed.

These geopolitical dynamics have been further intensified by recent crises and uneven regional responses. For example, energy market disruptions during the Ukraine war prompted many countries, especially in Europe, to accelerate energy transition, but this shift has also increased interdependency pressure on CRM supply chains and exposed regional grid limitations amid rapid renewable expansion (Chestney, 2025). In Southeast Asia, while there is also growing pressure to scale up the energy transition, underlying geopolitical frictions—such as intra-regional competition and limited strategic alignment—continue to hinder broader cooperation on cross-border solutions like regional grids and coordinated carbon markets. This shift away from fossil fuels to energy transition efforts introduces new dependencies and vulnerabilities, reshaping the geopolitics of the energy transition through trade dependencies, resource access, and market standards (Ashford, 2024).

Amid this shifting geopolitical landscape, data governance has emerged as a critical enabler of the energy transition, which is becoming increasingly data-reliant. In electricity systems, cross-border grids rely on real-time data and predictive analytics, including weather data, to optimise daily operations, supply stability, and integration of variable energy sources (Wang et al., 2023). In mineral supply chains, transparent and interoperable data platforms help track flows, assess risks, and coordinate responses to disruptions, thereby enhancing supply security (Krol-Sinclair, 2023; Stuermer & Wittenstein, 2023). In carbon markets, consistent and credible data systems are essential for emissions monitoring, verification, and alignment with evolving international standards (Lo & Yu, 2024). Furthermore, risks such as cybersecurity threats, uneven data access, fragmented standards, and data nationalism highlight the growing need for more robust and cooperative data governance frameworks to support an effective and equitable energy transition (H. Gao, 2021; X. Gao & Chen, 2024; KPMG, 2023).

Robust data governance—referring to the rules and institutions that guide how energy data is collected, shared, and used (Wang et al., 2023)—is essential for regional cooperation under rising geopolitical pressures, as the energy transition becomes increasingly data-reliant. The modern concept of data sharing emerged in the 1980s and has evolved across various industries (Beltramo et al., 2024). It refers to the process of making datasets accessible, usable, and reusable under clearly defined terms, often guided by internationally accepted principles (UNESCO, 2021). Advocacy for open science, including the 2001 Budapest Open Access Initiative and the 2015 OECD initiative, has further advanced the adoption of open data and data sharing practices (BOAI, 2021). Foundational initiatives, such as the findable, accessible, interoperable, and reusable (FAIR) principles, have been pivotal in standardising data collection and dissemination practices (GoFair, 2016). These frameworks facilitate cross-border collaboration by ensuring high-quality data is accessible, even in resource-constrained circumstances. They reduce barriers to use through open licensing, data protection laws, and the provision of machine-readable formats (Beltramo et al., 2024).

The international community has also increasingly recognised the importance of data sharing in addressing regional energy challenges (Wang et al., 2023). The UN Conference on Trade and Development (2021) highlights the need for a coordinated governance approach to facilitate the flow of data across borders. This has driven efforts to improve data governance in energy and commodity markets through regional initiatives aimed at enhancing transparency, reliability, and accessibility of critical data. For example, the IEA provides open access to energy datasets for energy policy planning, the EITI ensures transparency in mineral

extraction data, and the World Bank's Open Data Initiative supports carbon market registries (EITI, 2023; IEA, 2025; World Bank, 2025). Such initiatives play a vital role in supporting informed decision-making and fostering market stability within interconnected energy systems across regions, especially in times of geopolitical crisis.

These developments reveal the growing intersection between geopolitics, regional integration, and data governance. Effective management of these interconnected systems and cross-border issues hinges on robust data governance within regional cooperation, a challenge that regional integration theory offers a lens through which to examine. Regional integration refers to a cooperative framework where states within a region promote economic cooperation through established institutions and rules aimed at reducing barriers to free trade, capital flows, and human mobility (Ginsberg, 2007; Sapir, 2011). Its foundation rests on the principle that collective action strengthens capacity, promoting development and security (Chingono & Nakana, 2009). Scholars, notably Schimmelfennig (2018), emphasise that the effectiveness of regional integration depends on four key conditions: institutional capacity, policy alignment, interdependence, and political will. These conditions collectively determine how states coordinate governance, establish binding agreements, and sustain long-term cooperation.

Within energy scholarship, regional integration is widely regarded as a key mechanism for enhancing the energy transition and energy security (ADBI, 2020; Feng et al., 2024; Naeher & Narayanan, 2020; Yu, 2019, 2023a). Its importance stems from the transboundary nature of energy systems, where activities span interconnected networks and require coordinated strategies. The UNDP (2011) highlights that, beyond trade liberalisation, regional integration involves coordinated infrastructure investment, regulatory alignment, unified macroeconomic policies, shared resource governance, and enhanced labour mobility. These characteristics create a governance environment in which data plays a central role in facilitating cooperation and addressing complex geopolitical challenges.

The following sections examine the data governance models of the EU and ASEAN across three key areas—power grids, CRM supply chains, and carbon markets—that underpin the evolving geopolitics of the energy transition.

3. Case Study of Data Governance in the EU's Energy Transition

The EU, a leader in climate policy and regional integration, relies on data governance as a central part of its decarbonisation strategy, strengthening regional energy cooperation to achieve climate goals (van Boven, 2023). Built on transparency, accountability, and teamwork, this approach has driven major progress in the energy transition in Europe, including cross-border power grid integration, CRM management, and carbon market development. Supply disruption during the Ukraine crisis since 2022 has accelerated these efforts as a way to boost the EU's energy security and global position (Kirkegaard, 2023; Patrahau, 2023; Ye et al., 2025).

3.1. The EU's Power Grid Integration

For over two decades, the EU has maintained an efficient and integrated electricity market delivering both supply security and decarbonisation. To reduce reliance on Russia's energy supply and to align with its 2050 net-zero target, the EU is reforming this market to raise renewable shares from 37% in 2022 to 69% by 2030

(ACER, 2023). Investment in modernising power grids has surged to support this ambition, with grid-related investments reaching $65 billion in 2023 (IEA, 2023). To optimise electricity distribution, the EU relies on advanced data analytics to distribute electricity efficiently, reduce congestion, and address renewable intermittency. To manage data in the energy sector, the EU has set overarching frameworks, including the Regulation on Wholesale Energy Market Integrity and Transparency (REMIT), the Clean Energy for All Europeans Package, the Third Energy Package, and the Green Deal (European Commission, 2010, 2016, 2019; Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011, 2011). These regulations underpin this effort by requiring data-sharing rules to align with standardised practices and market integrity across member states, while also establishing data transparency and accuracy, mandating real-time information sharing.

Data governance in the EU's electricity market integration is facilitated by coordination efforts from the Agency for the Cooperation of Energy Regulators in collaboration with other agents such as the European Network of Transmission System Operators for Electricity (ENTSO-E) and the National Regulatory Authorities (NRAs; ACER, 2025). Established in 2011, ACER fosters cooperation among NRAs to ensure a well-functioning, integrated EU electricity market. It develops frameworks like network codes to standardise data collection and sharing for cross-border electricity trade and grid management. It supports data interoperability for cross-border grids and balancing markets, critical for renewable integration and regional cooperation. It also collects trading data to support the integrity and transparency of the wholesale energy market—a role that has been strengthened since the 2022 Ukraine crisis to address market volatility (Regulation (EU) 2024/1106 of the European Parliament and of the Council of 11 April 2024, 2024). ACER's 2025-2027 Work Programme highlights reforms to the REMIT framework, strengthening data governance through improved reporting and analysis to navigate uncertainties and reduce reliance on Russian energy (ACER, 2024). Its impact is amplified by collaboration with ENTSO-E, which manages technical data flows to ensure interoperability across EU member states (ENTSO-E, 2017) and NRAs, which implement ACER's guidelines at the local level. These measures embed standardised reporting, real-time data sharing, and interoperable systems into the EU's energy framework, reflecting a sustained commitment to collaboration and resilience.

3.2. The EU's Critical Raw Material Initiative

The EU's pursuit of mineral security is driven by a global resource race and surging demand for CRM essential to the energy transition, heightened by the 2022 Ukraine crisis. With renewable energy and digital technologies projected to increase the EU's CRM demand six-fold by 2030, securing reliable supplies has become a strategic priority to meet the EU's 2050 net-zero target and reduce import vulnerabilities (European Parliament, 2023). This urgency has prompted regional cooperation among member states to address mineral supply risks and market competition since the early 2000s. EU mineral policies, including the Raw Materials Initiative (RMI), the Circular Economy Action Plan, and the Critical Raw Materials Act (CRMA), have evolved to strengthen this cooperation by enabling data sharing on resources, risks, and recycling across the region (European Commission, 2008, 2020a, 2023). These policies advance CRM cooperation of EU member states by encouraging digital tools and platforms for sharing data among member states, boosting transparency and efficiency to identify risks and guide EU-wide supply strategies.

Data governance in the EU's CRM initiative is facilitated by key agencies that enhance regional cooperation through data-sharing frameworks, with the European Commission's Directorate-General for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) as a central agent (European Commission, 2020b). Since launching the Raw Materials Initiative (RMI) in 2008, DG GROW has fostered member state collaboration by establishing early data-sharing platforms on supply and trade. It supported projects like MINATURA 2020 (2015–2018) and MIN-GUIDE (2016–2019), which standardised mineral deposit data and enhanced policy data for sustainable supply (IMA, 2020). DG GROW has also chaired the European Critical Raw Materials Board under the CRMA, overseeing advanced data-sharing frameworks with member state representatives and the European Parliament as an observer (European Commission, 2025c). It coordinates supply chain monitoring and strategic projects through subgroups like monitoring and circularity to unify regional CRM strategies. The Joint Research Centre (JRC) has managed the Raw Materials Information System (RMIS) since 2015, providing a centralised platform that enables member states to share data on supply risks and circularity, strengthening regional resilience (European Commission, 2025e). The European Raw Materials Alliance (ERMA), formed in 2020, connects industry, research, and policymakers across the EU, fostering data exchange to align supply chain efforts (ERMA, 2025).

3.3. The EU's Carbon Market

As part of the EU's climate action since 2005, the EU Emissions Trading System (ETS) employs a cap-and-trade mechanism to reduce greenhouse gas emissions across member states (European Commission, 2025a). Amid rising global climate pressures, the ETS aims at driving a 62% emission reduction by 2030 from 2005 levels, aligning with the EU's 2050 net-zero target under the European Climate Law (European Commission, 2025a). Since 2013, the ETS has generated cumulative revenues of over €200 billion, which are channelled into the Innovation Fund and Modernisation Fund, which finance low-carbon technologies and infrastructure projects (European Commission, 2025b). EU carbon policies, including the ETS Directive (2003/87/EC), the EU Climate Law (2021), and 2023 revisions under the "Fit for 55" package, have evolved to foster regional cooperation by establishing robust data-sharing frameworks (Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003, 2003; European Commission, 2021; European Parliament, 2023). Participants in the ETS, such as power plants, industrial facilities, and airline companies, are required to meticulously monitor and report emissions, which are independently verified to maintain data accuracy and credibility.

Data governance within the EU's carbon market is facilitated by key agencies such as the European Commission's Directorate-General for Climate Action (DG CLIMA), the European Environment Agency (EEA), and the European Securities and Markets Authority (ESMA). Since the ETS's launch in 2005, DG CLIMA has overseen emissions data integrity by enforcing standards under the Monitoring and Reporting Regulation and the Accreditation and Verification Regulation, which standardise monitoring, reporting, and verification (MRV) across member states to ensure consistency and reliability in emissions reporting (European Commission, 2025d). DG CLIMA also manages the Union Registry Public Website, which replaced the EU Transaction Log Public in 2024, providing a centralised market system that enables member states and operators, such as power plants and airlines, to share verified emissions and trading data under the Union Registry (European Commission, 2025f). This platform standardises data reporting across the region, ensuring compliance with ETS and Effort Sharing obligations, while facilitating regional cooperation by recording member state allowance transfers and supporting harmonised climate policy development and market integrity. The EEA supports this governance by aggregating and disseminating ETS data, supporting

policy and solutions of Europe's transition on the ground (EEA, 2025). Since 2011, ESMA has enhanced market stability by enforcing financial data-sharing standards under the Markets in Financial Instruments Directive II (ESMA, 2022), thereby addressing trading risks. These agencies collectively underpin regional decarbonisation with data exchange coordination and equitable standard enforcement, ensuring the EU's competitiveness in global carbon markets and the broader climate agenda.

4. Case Study of Data Governance in ASEAN's Energy Transition

Similar to the EU, the ASEAN pursues its energy transition through regional cooperation, exemplified by initiatives in cross-border power grid integration, carbon pricing, and CRM strategies, aiming to balance economic growth with sustainability. Despite these efforts, ASEAN's diverse energy landscape and rapid demand growth expose gaps in data governance, which is essential for effective coordination and transparency across member states. Rising regional energy needs, projected at 7.3% annually through 2030, underscore the urgency to strengthen data frameworks to enhance ASEAN's energy security and decarbonisation ambitions.

4.1. ASEAN's Power Grid Integration

ASEAN's pursuit of energy security and sustainability is illustrated in the ASEAN Power Grid (APG), a regional initiative first included in the ASEAN Plan of Action for Energy Cooperation (APAEC) in 1999 (Huda et al., 2023). The APG aims to interconnect the power systems of ASEAN's 10 member states to facilitate cross-border electricity trade and integrate renewable energy sources, supporting a regional electricity demand projected to triple by 2040 (Huda et al., 2023). A major progress of this regional cooperation is the Lao PDR–Thailand–Malaysia–Singapore Power Integration Project (LTMS-PIP), which transmits 100 MW of hydropower from Lao PDR to Singapore via Thailand and Malaysia (Rufaidah, 2023). Operational since June 2022, the LTMS-PIP marks ASEAN's first initiative in multilateral electricity trade, serving as a model for further cooperation in cross-border power grids, such as the proposed Brunei–Indonesia–Malaysia–Philippines Power Integration Project (Huda et al., 2023; Rufaidah, 2023). Although APAEC provides an overarching framework to promote harmonised technical standards for grid interconnections through the Heads of ASEAN Power Utilities/Authorities (HAPUA), development in regional data-sharing frameworks remains limited, and member states tend to rely on bilateral data exchange protocols managed by national utilities (Huda et al., 2023; Rufaidah, 2023). As a result, ASEAN has yet to establish a centralised platform or binding authority that mandates data governance for grid operations or cross-border electricity flow.

With no regional institution dedicated to data governance, oversight for the APG is primarily coordinated by the ASEAN Centre for Energy (ACE), established in 1999, alongside the HAPUA, the ASEAN Power Grid Consultative Committee (APGCC), and the ASEAN Energy Regulators Network (AERN). The ACE has supported studies like the ASEAN Interconnection Masterplan Study, which recommends harmonising regulatory frameworks, standards, and data availability through digital platforms to enhance regional grid connectivity (ACE & HAPUA, 2021). The LTMS-PIP Working Group exemplifies effective coordination, uniting utility companies (e.g., EGAT in Thailand, TNB in Malaysia, and SP Group in Singapore), regulators, and ministries through four task forces, which have developed trade and emergency protocols and a web-based platform for real-time data exchange (Huda et al., 2023). However, this group lacks representation from international financial institutions, such as multilateral development banks, limiting

funding for scalable data systems beyond bilateral protocols (Huda et al., 2023). HAPUA, the specialised body tasked with implementing the APG, focuses on harmonising technical standards and operational procedures (HAPUA, 2025), supported by the APGCC and AERN. Although these efforts emphasise digitalisation of bilateral trade, studies indicate that data sharing across borders and long-term commitment to data governance remain limited, impeding trade flexibility (Huda et al., 2023; IEA, 2022).

4.2. ASEAN's Critical Raw Materials Strategy

Abundant in CRM resources, ASEAN nations play an increasingly influential role in the global supply chain for clean energy technologies, such as electric vehicles, batteries, and solar panels. According to Bhaskara (2025), the region accounts for 63% of the world's nickel production and 42% of tin, alongside smaller outputs of manganese (3%), REE (8%), and copper (4%). ASEAN also demonstrates downstream processing capacity, notably through Indonesia's development of an integrated battery industry that leverages its extensive nickel reserves to support EV production. In the renewables market, Vietnam, Malaysia, Cambodia, Indonesia, and Thailand also collectively contribute around 9–10% to global solar PV cell and module production (Bhaskara, 2025). On the regional level, ASEAN formulates the ASEAN Minerals Cooperation Action Plan (AMCAP-III 2016–2025), an overarching policy positioning ASEAN as a competitive minerals investment destination. It aims to advance the mineral sector by fostering investment, sustainability, capacity building, and data management, primarily through the ASEAN Minerals Database and Information System (AMDIS; ASEAN Secretariat, 2021). It employs coordinated mechanisms such as the ASEAN Minerals Exploration Strategy (2023) to improve geological data availability and support exploration (ASEAN Secretariat, 2025). However, these data approaches seek to consolidate resource information, but the scarcity of quality geological data and mineral development data constrains standardised data-sharing efforts (IGF, 2023).

Data governance of CRM in ASEAN involves a network of regional and national actors, yet lacks a centralised authority to enforce consistent data-sharing or policy alignment. The ASEAN Ministerial Meeting on Minerals (AMMin), established in 2005, acts as the primary policy-making body, guiding strategic directions through biennial meetings and declarations (ASEAN Secretariat, 2025). The ASEAN Senior Officials Meeting on Minerals supports AMMin by overseeing implementation, directing four working groups, including the Working Group on Minerals Information and Database, which manages the AMDIS (ASEAN Secretariat, 2025). It aims to centralise data on reserves, production, and trade of minerals in the region. However, poor coordination across member states results in uneven data quality and capacity disparities, hindering data sharing and standardisation in regional mineral cooperation. Although the ASEAN Secretariat facilitates AMCAP-III coordination, it lacks regulatory power, resulting in gaps in data governance (ASEAN Secretariat, 2022).

4.3. ASEAN's Carbon Market Development

ASEAN and its member states have identified carbon markets, projected to reduce 1.1 gigatonnes of CO_2 annually (Pandey, 2024), as a key low-carbon solution to balance economic development and sustainability, but regional frameworks remain in the early stages. Across the region, carbon market development varies, with a mix of carbon taxes, ETS, and voluntary carbon markets. Indonesia launched a compliance-based ETS for its coal-fired power sector in 2023, while Singapore advances its carbon market industry through its carbon tax

and exchange platforms (Rakhiemah et al., 2024). Meanwhile, Malaysia and Thailand are exploring domestic trading mechanisms to attract investors (Rakhiemah et al., 2024). The overarching policy, embedded in the ASEAN Strategy for Carbon Neutrality, seeks to operationalise carbon markets by fostering collaboration, with a focus on alignment with Article 6 of the Paris Agreement, and high-quality carbon credits for global trade (Siew, 2025). Highlighting the importance of reliable emission data, ASEAN aims to develop a regional MRV framework to ensure credit quality and facilitate trade (ASEAN Secretariat, 2023).

Data governance for ASEAN's carbon markets involves a mix of regional and national actors, yet lacks a centralised authority to enforce standardisation. The ASEAN Climate Change Working Group (ACCWG), under the ASEAN Senior Officials on Environment, leads the development of a regional MRV framework, coordinating data protocols to support the ASEAN Strategy for Carbon Neutrality (OECC, 2025). The ASEAN Alliance on Carbon Markets, through its COP29-established ACCF, contributes by setting minimum governance standards for carbon project data, aiming to enhance transparency across member states (Lau, 2024). At the national level, Singapore-based Climate Impact X, a global carbon exchange platform developed by SGX, began spot trading in November 2024. It employs satellite monitoring and blockchain technology to strengthen data integrity, ensuring robust validation and tracking of credits to support market credibility (Fogarty & Tan, 2024). Additionally, regional initiatives, such as TRACTION, launched by Singapore's Monetary Authority (MAS) in December 2023 with nearly 30 partners, including banks and international organisations, aim to standardise transition credit data protocols and enhance market integrity (MAS, 2023). Although a comprehensive ASEAN-wide platform for data integrity or registry standards has yet to be established, these regional initiatives highlight the importance of data governance in fostering trust and scalability in ASEAN's carbon markets despite disparities in national capacities hindering progress.

5. Comparison of Data Governance and Geopolitical Considerations

Through the lens of regional integration theory, this section compares the EU's centralised and formalised data governance, applied across power grids, CRM supply chains, and carbon markets, with ASEAN's more informal and decentralised coordination. While the core focus is on the institutional and policy structures of data governance, these differences also influence how each region navigates the evolving geopolitics of energy transition.

5.1. Comparison of EU–ASEAN Data Governance

5.1.1. Comparison 1: Institutional Capacity

Institutional capacity reflects differences in policy enforcement structures and coordination mechanisms. In the EU, data governance for energy transitions is anchored in centralised institutions with executive authority and binding mandates to oversee data-sharing and standardisation (ACE, 2019; Do & Burke, 2022; Huda, 2025; Sung & Ho, 2024). Agencies like ENTSO-E, ACER, DG CLIMA, and DG GROW play key roles in ensuring effective data cooperation in cross-border electricity trade and supply chain coordination across member states. In contrast, whilst government-to-government collaboration has supported energy trade in Southeast Asia, studies have highlighted the need to strengthen ASEAN's institutional capacity to facilitate multilateral electricity trade (ACE, 2019; Huda, 2025; Sung & Ho, 2024). ASEAN has yet to establish a centralised governance body for energy integration with an enforcement authority comparable to that of

the EU. Instead, it relies on a network of informal cooperation among regional and national agencies, including the ACE, ACCWG, and AMMin (Andrews-Speed, 2016). ASEAN's preference for bilateral negotiations and informal arrangements over binding mechanisms is also reflected in the absence of a regional dispute resolution body or neutral arbitration centre (Aalto, 2014; Do & Burke, 2022). This decentralised institutional approach limits ASEAN's ability to formalise and implement regional data-sharing mechanisms (Do & Burke, 2022; Huda, 2025).

5.1.2. Comparison 2: Policy Alignment

Policy alignment reflects the extent to which countries prioritise coordinated approaches to data governance. In the EU, consistent data policies are enforced through binding regulatory frameworks such as REMIT, ETS, and the CRMA. These frameworks established standardised data-sharing obligations, market integrity measures, and emissions monitoring systems. High levels of policy alignment minimise regulatory inconsistency and facilitate regional cooperation in power grid operation, CRM management, and carbon markets. In contrast, ASEAN's data policy landscape demonstrates varying degrees of alignment, often shaped by national and geopolitical priorities (IRENA, 2018). Regional strategies such as APAEC, AMCAP-III, and the ASEAN Strategy for Carbon Neutrality provide strategic direction but remain non-binding, resulting in informal institutional cooperation (Andrews-Speed, 2016). This contributes to inconsistencies in data availability and coordination across member states (Do & Burke, 2022). Unilateral actions, such as Indonesia's and the Philippines' nickel export restrictions, emphasise the preference for national policy interests (Bhaskara, 2025).

5.1.3. Comparison 3: Interdependence

Interdependence reflects the necessity for robust data governance in the energy transition. In the EU, high interdependence among member states incentivises the development of strong data-sharing mechanisms across power grids, CRM management, and carbon markets. The ENTSO-E Regulation facilitates coordinated cross-border electricity flows, while the EU ETS ensures a standardised framework for emissions trading. This mutual reliance creates a strong impetus for transparent and harmonised data governance. In contrast, due to geopolitical complexities, ASEAN's regional energy cooperation is predominantly bilateral, limiting the collective demand for a fully integrated data-sharing framework (Aalto, 2014; Andrews-Speed, 2016). While initiatives such as the APG and LTMS-PIP demonstrate progress toward cross-border electricity integration, ASEAN has yet to establish a comprehensive governance structure to support coordinated data management (Huda, 2025). Similarly, the governance of CRM and the carbon market continues to be shaped primarily by national strategies (Rakhiemah et al., 2024), which tend to limit progress towards the regional standardisation of data reporting interoperability.

5.1.4. Comparison 4: Political Will

Political will is a critical prerequisite for achieving high levels of market integration, particularly when it involves the exchange of sensitive data. In the EU, robust data governance is supported by strong political commitment among member states to align their data policies and delegate authority to supranational institutions (Ricart, 2023). This institutional trust facilitates the cross-border sharing of sensitive data and contributes to the development of a unified digital market. In contrast, ASEAN faces greater challenges in

this area due to differing levels of political will and institutional coordination (Do & Burke, 2022; Yao et al., 2021). Sensitive surrounding data sovereignty, particularly concerning energy-related information such as production, trade, and reserves, can complicate regional cooperation. In some cases, concerns over economic competitiveness have led governments to prioritise domestic energy development and maintain control over their energy sectors, often favouring bilateral arrangements over broader regional integration (Shi & Kimura, 2013; Wu et al., 2012; Yao et al., 2021). These dynamics can limit cross-border data access and hinder efforts to enhance market integration (Do & Burke, 2022; Long, 2023).

Regional integration theory underscores the EU's comparatively higher effectiveness in data governance integration for energy transition, enabled by stronger institutional capacity, policy alignment, mutual interdependence, and political commitment. These conditions support cross-border electricity trade, CRM coordination, and harmonised carbon market frameworks. By contrast, ASEAN's varied institutional capacities, limited policy coordination, and lower levels of political will result in a more informal, fragmented approach to data governance. Additionally, gaps in data availability further hinder the development of a regional data-sharing framework, reinforcing reliance on national systems and bilateral approaches. This divergence highlights the EU's cohesive and strategically aligned model in contrast to ASEAN's coordination challenges, with important implications for each region's role in global energy and climate governance.

5.2. Geopolitical Implications of EU–ASEAN Energy Data Governance

As discussed in Section 2, the geopolitics of energy transition is increasingly shaped by data-enabled cooperation underpinning decarbonisation efforts. Within this context, the EU and ASEAN have diverging approaches to energy data governance that shape their geopolitical positioning. The EU's centralised data governance enhances its energy security and allows it to project a unified stance in the global climate agenda, reinforcing its geopolitical influences (Kivimaa, 2024; Maltby, 2013; Yu, 2018). In contrast, ASEAN's informal approach limits its geopolitical leverage, making it more vulnerable to external market pressures and regulatory pressures. This section explores how the differences in data governance influence their geopolitical leverage with a focus on energy security and the climate agenda.

Both case studies show that a strong data governance framework is crucial for enhancing energy security, as it enables regional integration to diversify sources and reduce vulnerability to external threats. Robust data systems facilitate coordinated cross-border energy flows and renewable integration, whereas weak governance leaves regions vulnerable to supply disruptions. In the EU, data governance is considered a critical enabler of energy integration (European Commission, 2024a), which is intertwined with its energy security and geopolitical strategy. This became particularly evident following the escalation of tensions with Russia, especially after the outbreak of the war in Ukraine. In response to the resulting energy supply risks, the EU made a concerted effort to reduce its dependency on Russian fossil fuels. In 2023, the EU's natural gas imports from Russia declined to about 15% from 45% in 2021 (European Commission, 2024b). This reduction reflects the EU's strategic shift towards energy diversification and resilience. Central to this approach was the diversification of energy sources, including increased imports of US LNG and Norway's pipeline gas. The EU also accelerated investments in renewable energy infrastructure, aligning with initiatives like the REPowerEU plan, which seeks to phase out dependence on Russian fossil fuels (European Commission, 2024b). Within this context, geopolitical disruptions have heightened pressures on both energy security and energy transition, reinforcing the need for more robust data governance to support the coordination of diversified energy flows and the operation of an integrated energy system.

In ASEAN, however, informal data governance constrains the region's coordinated efforts to enhance energy security. While there are regional initiatives and projects to facilitate energy trade, they mostly rely on bilateral agreements rather than a centralised governance approach (Andrews-Speed, 2016). Moreover, protectionist approaches could undermine regional energy cooperation. The use of market leverage, such as export control over energy resources, which can be intertwined with regional rivalries, results in discontinuities in energy trade policy (Huda et al., 2023). The lack of a centralised institution constrains ASEAN's ability to integrate renewables or manage energy trade effectively, risking supply disputes and geopolitical vulnerabilities.

Data governance also plays a pivotal role in enhancing competitiveness in climate agendas and standard-setting. High data integrity and unified standards enable countries to shape global markets, whereas fragmentation erodes climate leadership and reduces economic advantages. This strategic use of data governance is well demonstrated in the EU's Carbon Border Adjustment Mechanism (CBAM), which is backed by advanced monitoring and verification systems and imposed carbon prices on imports like steel and cement. Benchmarking its price against the EU ETS, CBAM helps level the playing field for EU industries while compelling global trading partners to align with its stringent environmental standards (Benson et al., 2023). By embedding robust data governance into its climate agenda, the EU not only fosters the adoption of transparent and accountable frameworks globally but also strengthens its influence over international carbon markets. Policy alignment and data cohesion reinforce EU industries' competitiveness, pressuring trade partners to adopt stricter carbon reporting norms (Benson et al., 2023). With strong data governance, it is in a better position to set global standards, leveraging detailed emissions registries to enforce compliance and gain economic leverage (Boocker & Wessel, 2024).

In contrast, ASEAN's informal approach to data governance presents challenges to its competitiveness in the global climate agenda, potentially undermining its attractiveness as a trade partner and investment destination (Elder et al., 2025). The absence of a centralised framework of carbon pricing schemes and project registry hinders the development of a unified market. This regulatory gap risks placing the region at an economic disadvantage, with its exports becoming subject to higher carbon-related tariffs under mechanisms such as the EU's CBAM (Elder et al., 2025). Without robust data governance, ASEAN risks becoming a rule-taker in global climate governance and remains vulnerable to evolving international climate regulations and trade measures imposed by more data-driven regulatory blocs such as the EU. Countries with weaker data systems could face higher costs in aligning with these standards and risk losing market influence, deepening economic disparities. These findings reflect the broader risks identified in Section 2, where fragmented data governance in energy transition can exacerbate geopolitical vulnerabilities.

6. Conclusion

Data governance in the energy transition is both shaped by geopolitics and reshapes geopolitical dynamics, with the EU and ASEAN exemplifying divergent paths through regional integration. This article has shown how the EU and ASEAN diverge in their regional integration strategies and institutional capacities, shaping not only their regional energy cooperation but also their ability to influence global climate governance. While the EU leverages centralised frameworks to strengthen energy security, coordinate resource supply chains, and set international carbon market standards, ASEAN's decentralised and informal approach constrains its strategic leverage. The comparative analysis offers three broader implications for regions navigating the energy transition.

First, it underscores the need for regionally tailored data governance frameworks that reflect national capacities. While energy transition is a global consensus, not all governments can advance at the same pace due to differing domestic capabilities and constraints (Finley & Gross, 2025). Developed economies are better positioned to absorb the upfront costs of renewable expansion, whereas many developing economies remain reliant on fossil fuels while pursuing alternative decarbonisation pathways, often constrained by affordability, infrastructure deficits, and fragmented markets (Huda, 2022). Recognising this divergence is essential for crafting inclusive regional strategies that accommodate differentiated capabilities.

Second, it highlights that data governance is not only a technical consideration but also a strategic enabler of energy transition. Robust data frameworks underpin effective cooperation in cross-border power grids, CRM tracking, and carbon market transparency, each of which is essential for managing the new geopolitical risks of decarbonisation. For regions like ASEAN and other developing regions, improved data governance presents a pathway to overcome institutional fragmentation and enhance regional energy resilience. However, it requires targeted reforms in capacity-building to address existing coordination challenges, in particular institutional disparities.

Third, as global decarbonisation accelerates, the capacity to govern energy data has become a key factor in shaping energy resilience and strategic influence. With energy systems becoming increasingly data-intensive, regional blocs—both formal and informal—are under growing pressure to adopt more integrated and transparent data-sharing frameworks while still respecting national sovereignty. The ability to govern energy data collaboratively will influence not only decarbonisation outcomes but also regional positioning in the evolving geopolitics of energy.

Acknowledgments

The authors express gratitude towards the reviewers and editors, especially Dr. Xinchuchu Gao and Dr. Xuechen Chen, for their valuable feedback. The views expressed in this article are solely those of the authors and do not necessarily represent the views of their employers or any affiliated organisations.

Conflict of Interests

The author declares no conflict of interest.

References

Aalto, P. (2014). Energy market integration and regional institutions in East Asia. *Energy Policy*, *74*, 91–100. https://doi.org/10.1016/j.enpol.2014.08.021

ACER. (2023). *Flexibility solutions to support a decarbonised and secure EU electricity system* (EEA/ACER Report 09/2023). European Environment Agency. https://www.acer.europa.eu/sites/default/files/documents/Publications/EEA-ACER_Flexibility_solutions_support_decarbonised_secure_EU_electricity_system.pdf

ACER. (2024). *Single programming document 2025-2027*. European Environment Agency. https://www.acer.europa.eu/sites/default/files/documents/Documents/ACER_Programming_Document_2025-2027.pdf

ACER. (2025). *About ACER*. https://www.acer.europa.eu/the-agency/about-acer

ADBI. (2020). *Role of regional cooperation and integration in improving energy insecurity in South Asia* (No 1120). https://www.adb.org/sites/default/files/publication/602071/adbi-wp1120.pdf

Andrews-Speed, P. (2016). *Energy security and energy connectivity in the context of ASEAN energy market integration* [Paper presentation]. ASEAN Energy Market Integration, Bangkok, Thailand.

Ansari, D., Gehrung, R. M., & Pepe, J. (2025). *The geopolitics of the energy transition in greater Asia*. SWP German Institute for International and Security Affairs. https://www.swp-berlin.org/en/publication/the-geopolitics-of-the-energy-transition-in-greater-asia

ASEAN Centre for Energy. (2019). *Report on ASEAN renewable energy grid integration review*.

ASEAN Centre for Energy & HAPUA. (2021). *ASEAN interconnection masterplan study (AIMS) III report*. https://aseanenergy.org/publications/asean-interconnection-masterplan-study-aims-iii-report

ASEAN Secretariat. (2021). *ASEAN minerals cooperation action plan 2016-2025 (AMCAP-III) Phase 2: 2021–2025*. ASEAN. https://asean.org/book/asean-minerals-cooperation-action-plan-2016-2025-amcap-iii-phase-2-2021-2025

ASEAN Secretariat. (2022). *Strengthening ASEAN cooperation in minerals: Development prospects of ASEAN minerals cooperation (DPAMC)*. ASEAN. https://asean.org/wp-content/uploads/2022/04/Development-Prospects-of-ASEAN-Minerals-Cooperation-DPAMC.pdf

ASEAN Secretariat. (2023). *ASEAN strategy for carbon*. ASEAN. https://asean.org/wp-content/uploads/2023/08/Brochure-ASEAN-Strategy-for-Carbon-Neutrality-Public-Summary-1.pdf

ASEAN Secretariat. (2025). *ASEAN minerals cooperation*. ASEAN. https://asean.org/our-communities/economic-community/asean-minerals-cooperation

Ashford, E. (2024). *The green transition: Implications for energy security and geopolitics*. Stimson. https://www.stimson.org/2024/the-green-transition-implications-for-energy-security-and-geopolitics

Beltramo, A., Leonard, A., Tomei, J., & Usher, W. (2024). Data governance and open science in energy planning: A case study of the Kenyan ecosystem. *Energy Research & Social Science*, *118*, Article 103821. https://doi.org/10.1016/j.erss.2024.103821

Benson, E., Majkut, J., Reinsch, W., & Steinberg, F. (2023). *Analyzing the European Union's carbon border adjustment mechanism*. CSIS. https://www.csis.org/analysis/analyzing-european-unions-carbon-border-adjustment-mechanism

Bhaskara, R. (2025). *Cooperate, not compete: ASEAN's critical mineral strategy for energy transition*. Economic Research Institute for ASEAN and East Asia. https://www.eria.org/news-and-views/cooperate--not-compete--asean-s-critical-mineral-strategy-for-energy-transition

BOAI. (2021). *Budapest open access initiative*. https://www.budapestopenaccessinitiative.org/read

Boocker, S., & Wessel, D. (2024). *What is a carbon border adjustment mechanism?* Brookings. https://www.brookings.edu/articles/what-is-a-carbon-border-adjustment-mechanism

Chestney, N. (2025, May 6). EU power grid needs trillion-dollar upgrade to avert Spain-style blackouts. *Reuters*. https://www.reuters.com/sustainability/climate-energy/eu-power-grid-needs-trillion-dollar-upgrade-avert-spain-style-blackouts-2025-05-05

Chingono, M., & Nakana, S. (2009). The challenges of regional integration in Southern Africa. *African Journal of Political Science and International Relations*, *3*(10), 396–408. https://www.academicjournals.org/app/webroot/article/article1381823504_Chingono%20and%20Nakana%20pdf.pdf

Directive 2003/87/EC of the European Parliament and of the Council of 13 October 2003 establishing a scheme for greenhouse gas emission allowance trading within the Community and amending Council Directive 96/61/EC. (2003). *Official Journal of the European Union*, L 275/32. https://eur-lex.europa.eu/eli/dir/2003/87/oj/eng

Do, T., & Burke, P. (2022). Is ASEAN ready to move to multilateral cross-border electricity trade? *Asia Pacific View Point*, *64*(1), 110–125. https://onlinelibrary.wiley.com/doi/full/10.1111/apv.12343

EEA. (2025). *EU emissions trading system (ETS) data viewer*. https://www.eea.europa.eu/en/analysis/maps-and-charts/emissions-trading-viewer-1-dashboards?activeTab=265e2bee-7de3-46e8-b6ee-76005f3f434f

EITI. (2023). *Out mission*. https://eiti.org/our-mission

Elder, M., Hopkinson, S., Zhou, X., Arino, Y., & Matsushita, K. (2025). *Implications of the EU's carbon border adjustment mechanism (CBAM) for ASEAN: An argument for more ambitious carbon pricing*. Institute for Global Environmental Strategies. https://www.iges.or.jp/en/pub/asean-cbam-implications/en

ENTSO-E. (2017). *Data exchange in electric power system: European state of play and perspectives* (THEMA Report 2017-03). THEMA Consulting Group. https://www.entsoe.eu/Documents/News/THEMA_Report_2017-03_web.pdf

ERMA. (2025). *EU policy*. https://erma.eu/eu-policy

ESMA. (2022). *Report on quality and use of transaction data* (ESMA74-427-719). https://www.esma.europa.eu/sites/default/files/2023-04/ESMA74-427-719_2022_Report_on_Quality_and_Use_of_Transaction_Data.pdf

European Commission. (2008). *Communication from the Commission to the European Parliament and the Council—The raw materials initiative: Meeting our critical needs for growth and jobs in Europe* (COM/2008/0699 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:52008DC0699

European Commission. (2010). *EU strengthens rules on security of gas supply for citizens* (IP/10/1151). https://ec.europa.eu/commission/presscorner/detail/en/ip_10_1151

European Commission. (2016). *Clean energy for all Europeans—Unlocking Europe's growth potential*. https://ec.europa.eu/commission/presscorner/detail/en/ip_16_4009

European Commission. (2019). *Communication from the Commission. The European Green Deal* (COM(2019) 640 final). https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52019DC0640

European Commission. (2020a). *Circular economy action plan*. https://environment.ec.europa.eu/strategy/circular-economy-action-plan_en

European Commission. (2020b). Strategic plan 2020-2024—Internal market, industry, entrepreneurship and SMEs. https://commission.europa.eu/publications/strategic-plan-2020-2024-internal-market-industry-entrepreneurship-and-smes_en

European Commission. (2021). *Forging a climate-resilient Europe—The new EU strategy on adaptation to climate change* (COM(2021) 82 final). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52021DC0082&qid=1742814644561

European Commission. (2023). *Critical raw materials act*. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act_en

European Commission. (2024a). *EU policy supporting the digital and green transformation of the energy system*. https://digital-strategy.ec.europa.eu/en/policies/eu-policy-digitalisation-energy

European Commission. (2024b). In focus: EU energy security and gas supplies. European Commission. https://energy.ec.europa.eu/news/focus-eu-energy-security-and-gas-supplies-2024-02-15_en

European Commission. (2025a). About the EU ETS. https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets/about-eu-ets_en

European Commission. (2025b). Auctioning of allowances. https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets/auctioning-allowances_en#auctioning-revenues-and-their-use

European Commission. (2025c). *European critical raw materials board*. https://single-market-economy.ec.europa.eu/sectors/raw-materials/areas-specific-interest/critical-raw-materials/critical-raw-materials-act/board_en

European Commission. (2025d). Monitoring, reporting and verification. https://climate.ec.europa.eu/eu-action/eu-emissions-trading-system-eu-ets/monitoring-reporting-and-verification

European Commission. (2025e). *Raw materials information system*. https://data.jrc.ec.europa.eu/collection/id-00192

European Commission. (2025f). Union registry public website. https://union-registry-data.ec.europa.eu/report/welcome

European Parliament. (2023). *Revision of the renewable energy directive: Fit for 55 package*. https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/698781/EPRS_BRI(2021)698781_EN.pdf

Feng, Y., Sun, M., Pan, Y., & Zhang, C. (2024). Fostering inclusive green growth in China: Identifying the impact of the regional integration strategy of Yangtze River Economic Belt. *Journal of Environment Management*, *358*, Article 120952. https://www.sciencedirect.com/science/article/abs/pii/S0301479724009381

Finley, M., & Gross, S. (2025). *Navigating market and political uncertainties in the age of energy transition*. Brookings. https://www.brookings.edu/articles/navigating-market-and-political-uncertainties-in-the-age-of-energy-transition

Fogarty, D., & Tan, A. (2024, April 3). Singapore-backed platform CAD Trust boosts transparency, covers 85% of carbon credit market. *Straits Times*. https://www.straitstimes.com/singapore/singapore-backed-platform-boosts-transparency-covers-85-of-carbon-credit-market

Gao, H. (2021). Data sovereignty and trade agreements: Three digital kingdoms. In A. Chander & H. Sun (Eds.), *Data sovereignty: From the digital Silk Road to the return of the state* (pp. 213–239). Oxford University Press. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3940508

Gao, X., & Chen, X. (2024). The regime complex for digital trade in Asia and China's engagement. *Asia Europe Journal*, *22*. https://doi.org/10.1007/s10308-024-00705-0

Garske, B., Holz, W., & Ekardt, F. (2024). Digital twins in sustainable transition: Exploring the role of EU data governance. *Research Policy and Strategic Management*, *9*. https://doi.org/10.3389/frma.2024.1303024

Ginsberg, R. (2007). *Demystifying the European Union: The enduring logic of regional integration*. Rowman and Littlefield.

GoFair. (2016). *FAIR principles*. https://www.go-fair.org/fair-principles

HAPUA. (2025). *About Hapua*. https://hapua.org/main/hapua/about

Huda, M. (2022). *Can the Russia-Ukraine conflict derail Southeast Asia's decarbonisation efforts*. Fulcrum. https://fulcrum.sg/can-the-russia-ukraine-conflict-derail-southeast-asias-decarbonisation-efforts

Huda, M. (2025). *New ASEAN power grid agreement must reflect new needs*. Fulcrum. https://fulcrum.sg/new-asean-power-grid-agreement-must-reflect-new-needs

Huda, M., Seah, S., & Qiu, J. (2023). *Accelerating the ASEAN power grid 2.0*. ISEAS. https://www.iseas.edu.sg/wp-content/uploads/2023/11/2023-LTMS-PIP-Policy-Report-FA-V2-Online.pdf

IEA. (2021). *The role of critical minerals in clean energy transitions*. https://www.iea.org/reports/the-role-of-critical-minerals-in-clean-energy-transitions/executive-summary

IEA. (2022). *Southeast Asia energy outlook 2022*. https://www.iea.org/reports/southeast-asia-energy-outlook-2022

IEA. (2023). *European Union*. https://www.iea.org/reports/world-energy-investment-2024/european-union

IEA. (2025). *Data and statistics*. https://www.iea.org/data-and-statistics/about

IGF. (2023). *ASEAN-IGF minerals cooperation: Scoping study on critical minerals supply chains in ASEAN*. https://asean.org/book/asean-igf-minerals-cooperation-scoping-study-on-critical-minerals-supply-chains-in-asean

IMA. (2020). *Raw material initiatives*. https://ima-europe.eu/eu-policy/industrial-policy-and-circular-economy/raw-material-initiative

IRENA. (2018). *Renewable energy market analysis: Southeast Asia*. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2018/Jan/IRENA_Market_Southeast_Asia_2018.pdf

IRENA. (2023). *Geopolitics of the energy transition*. https://www.irena.org/-/media/Files/IRENA/Agency/Publication/2023/Jul/IRENA_Geopolitics_energy_transition_critical_materials_2023.pdf

IRENA. (2024). *Renewable power generation costs in 2023*. http://large.stanford.edu/courses/2024/ph240/lutz1/docs/irena-2024.pdf

Kirkegaard, J. (2023). *Russia's invasion of Ukraine has cemented the European Union's commitment to carbon pricing*. Peterson Institute for International Economics. https://www.piie.com/publications/policy-briefs/2023/russias-invasion-ukraine-has-cemented-european-unions-commitment

Kivimaa, P. (2024). Evaluating policy coherence and integration for adaptation: The case of EU policies and Arctic cross-border climate change impacts. *Climate Policy*, *25*(1), 59-75. https://doi.org/10.1080/14693062.2024.2337168

KPMG. (2023). *Navigating evolving cyber risks in the energy sector*. https://kpmg.com/sg/en/home/insights/2023/10/navigating-evolving-cyber-risks.html

Krol-Sinclair, M. (2023). *Bring commodities market regulators into the critical minerals discussion*. CSIS. https://www.csis.org/analysis/bring-commodities-market-regulators-critical-minerals-discussion

Lau, A. (2024). *Five ASEAN carbon market associations unite at COP29 to support the ASEAN common carbon framework*. Singapore Sustainable Finance Association. https://www.ssfa.org.sg/five-asean-carbon-market-associations-unite-at-cop29-to-support-the-asean-common-carbon-framework

Li, H., & Kim, J. (2024). *The growth of voluntary carbon markets and challenges for further development* (Policy brief 72). Energy Studies Institute. https://esi.nus.edu.sg/docs/default-source/esi-policy-briefs/esi-pb-72_the-growth-of-vcms-and-challenges-for-further-development.pdf?sfvrsn=1e128848_1

Lo, J., & Yu, K. (2024). *Voluntary carbon markets: Opportunities and challenges* (SID Director Bulletin (QTR3)). https://www.sid.org.sg/Web/Resources/SID_DIRECTORS_BULLETIN/Flipbooks/2024_Q3_Flipbook.aspx

Long, K. (2023). *Data residency laws frustrate Asian banks' cross-border activity*. The Banker. https://www.thebanker.com/content/dca2cf48-3983-583f-a59c-bff2a764107c

Maltby, T. (2013). European Union energy policy integration: A case of European Commission policy entrepreneurship and increasing supranationalism. *Energy Policy*, *55*, 435-444. https://doi.org/10.1016/j.enpol.2012.12.031

MAS. (2023). *MAS launches coalition and announces pilots to develop transition credits for the early retirement of Asia's coal plants*. https://www.mas.gov.sg/news/media-releases/2023/mas-launches-traction-and-announces-pilots-to-develop-transition-credits

Naeher, D., & Narayanan, R. (2020). Untapped regional integration potential: A global frontier analysis. *The Journal of International Trade & Economic Development*, *29*(6), 722-747. https://www.tandfonline.com/doi/full/10.1080/09638199.2020.1722204

Nakano, J. (2020). The geopolitics of critical minerals supply chains. CSIS. https://www.csis.org/analysis/geopolitics-critical-minerals-supply-chains

O'Sullivan, M. (2017). *Windfall: How the new energy abundance upends global politics and strengthens America's power*. Simon & Schuster.

O'Sullivan, M. (2023). The new geopolitics of energy with Meghan O'Sullivan [Speech transcript]. Harvard Kennedy School. https://www.hks.harvard.edu/wiener-conference-calls/meghan-osullivan#transcript-1146210

Overseas Environmental Cooperation Center. (2025). *MRV information platform for ASEAN region*. Overseas Environmental Cooperation Center. https://mrv-info.com

Pandey, N. (2024, December 5). *ASEAN can unlock $3 trillion revenue from carbon markets*. Carbon Pulse. https://carbon-pulse.com/349101

Patrahau, I. (2023). Emerging from the war in Ukraine into a secure energy transition. *Journal of International Affairs*, *75*(2). https://jia.sipa.columbia.edu/content/emerging-war-ukraine-secure-energy-transition

Rakhiemah, A., Pradnyaswari, I., & Rizaldi, M. (2024). *Toward ASEAN's carbon neutral future: How interoperable carbon markets will make a difference*. ASEAN Center for Energy. https://aseanenergy.org/post/toward-aseans-carbon-neutral-future-how-interoperable-carbon-markets-will-make-a-difference

Regulation (EU) 2024/1106 of the European Parliament and of the Council of 11 April 2024 amending Regulations (EU) No 1227/2011 and (EU) 2019/942 as regards improving the Union's protection against market manipulation on the wholesale energy market. (2024). *Official Journal of the European Union*, L 2024/1106. https://www.acer.europa.eu/sites/default/files/REMIT/REMIT%20Legislation/Regulation%20amending%20REMIT.pdf

Regulation (EU) No 1227/2011 of the European Parliament and of the Council of 25 October 2011 on wholesale energy market integrity and transparency Text with EEA relevance. (2011). *Official Journal of the European Union*, L 326/1. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32011R1227

Ricart, R. J. (2023). *Geopolitical aspects of the EU's data strategy*. Elcano Royal Institute. https://www.realinstitutoelcano.org/en/work-document/geopolitical-aspects-of-the-eus-data-strategy

Rufaidah, R. (2023). *Growing momentum of LTMS-PIP and Its impact on regional integration*. ASEAN Centre for Energy. https://aseanenergy.org/post/growing-momentum-of-ltms-pip-and-its-impact-on-regional-integration

Sapir, A. (2011). European integration at the crossroads: A review essay on the 50th anniversary of Bela Balassa's theory of economic integration. *Journal of Economic Literature*, *49*(4), 1200–1229. https://www.jstor.org/stable/23071666

Schimmelfennig, F. (2018). Regional integration theory. In W. Thompson (Eds.), *Oxford research encyclopedia of politics*. Oxford University Press. https://doi.org/10.1093/acrefore/9780190228637.013.599

Scholten, D. (2024). *The power of energy: The geopolitics of the energy transition*. E-International Relations. https://www.e-ir.info/2024/06/17/the-power-of-energy-the-geopolitics-of-the-energy-transition

Shi, X., & Kimura, F. (2013). The status and prospects of energy market integration in East Asia. In Y. Wu & F. Kimura (Eds.), *Energy market integration in East Asia: Deepen understanding and move forward* (pp. 9–24). Routledge.

Siew, R. (2025). *COP29 affirms cooperation is key to ASEAN's carbon markets*. East Asia Forum. https://eastasiaforum.org/2025/01/10/cop29-affirms-cooperation-is-key-to-aseans-carbon-markets

Stuermer, M., & Wittenstein, M. (2023). *Why we need international data sharing on critical minerals*. World Economic Forum. https://www.weforum.org/stories/2023/12/why-we-need-international-data-sharing-on-critical-minerals

Sung, J., & Ho, K. (2024). *Development of ASEAN power grid and factors affecting regional power market integration* (Policy brief 71). Energy Studies Institute. https://esi.nus.edu.sg/docs/default-source/bulletin/esi-pb-71_development-of-asean-power-grid-and-factors-affecting-regional-power-market-integration.pdf?sfvrsn=f4c6687b_1

UN Conference on Trade and Development. (2021). *Digital economy report 2021*. https://www.un-ilibrary.org/content/books/9789210058254

UNDP. (2011). *Regional integration and human development: A pathway for Africa*. https://www.undp.org/sites/g/files/zskgke326/files/publications/RIR%20English-web.pdf

UNESCO. (2021). *UNESCO recommendation on open science* (SC-PCB-SPP/2021/OS/UROS). https://unesdoc.unesco.org/ark:/48223/pf0000379949?posInSet=3&queryId=cdb6384d-230d-4b28-8ccc-ccf9a3c5fb3d

van Boven, D. (2023, March 2). *The EU's Green Deal is an opportunity to improve data governance*. The Banker. https://www.thebanker.com/content/17db7034-3c6a-5931-baf5-dd0e5efb5da5

Wang, J., Gao, F., Gou, Q., & Tan, C., Song, J., & Wang, Y. (2023). Data sharing in energy systems. *Advances in Applied Energy*, *10*, Article 100132. https://doi.org/10.1016/j.adapen.2023.100132

World Bank. (2025). *World Bank open data*. https://data.worldbank.org

Wu, Y. (2023). *How will the EU carbon border adjustment mechanism impact China businesses?* China Briefing. https://www.china-briefing.com/news/how-will-the-eu-carbon-border-adjustment-mechanism-impact-china-businesses

Wu, Y., Shi, X., & Kimura, F. (2012). *Energy market integration in East Asia: Theories, electricity sector and subsidies*. ERIA. https://econpapers.repec.org/scripts/redir.pf?u=http%3A%2F%2Fwww.eria.org%2FChapter%25201-The%2520Electricity%2520Sector%2520Leads%2520Energy%2520Market%2520Integration%2520in%2520East%2520Asia-Introduction.pdf;h=repec:era:eriabk:2011-rpr-17

Yao, L., Andrews-Speed, P., & Shi, X. (2021). ASEAN electricity market integration: How can Belt and Road Initiative bring new life to it? *Singapore Economic Review*, *66*(1), 85–103. https://doi.org/10.1142/S0217590819500413

Ye, R., Yang, X., Zhou, Y., Lin, C., Chen, Y., Chen, J., & Bian, M. (2025). Energy demand security in OPEC+ countries: A revised 4As framework beyond supply security. *Energy*, *320*, Article 135261. https://doi.org/10.1016/j.energy.2025.135261

Yu, K. (2018). Energy cooperation in the Belt and Road Initiative: EU experience of the Trans-European Networks for Energy. *Asia Europe Journal*, *16*, 251–265. https://doi.org/10.1007/s10308-018-0512-y

Yu, K. (2019). Energy cooperation under the Belt and Road Initiative: Implications for global energy governance. *The Journal of World Investment & Trade*, *20*(2/3), 243–258. https://doi.org/10.1163/22119000-12340130

Yu, K. (2023a). *China's energy security in the twenty-first century*. Hong Kong University Press. https://doi.org/10.1515/9789888805174

Yu, K. (2023b). Critical minerals strategy of Asia-Pacific countries: Diversification, circular economy and multilateral initiatives. In C. Hübner (Eds.), *Geoeconomics of decarbonization in Asia-Pacific*. Konrad Adenauer Stiftung. https://www.kas.de/en/web/recap/single-title/-/content/geoeconomics-of-decarbonization-in-asia-pacific

About the Authors

Kaho Yu is the chief research officer at the Asia Carbon Institute. His research focuses on energy transition, carbon markets, and global energy governance. He previously held academic positions at Harvard Kennedy School, King's College London, and the Chinese University of Hong Kong.

Jinseok Sung is a research fellow at the Energy Studies Institute, National University of Singapore. His research focuses on global natural gas markets and energy markets in Asia and Eurasian countries. Prior to his current position, he held research and academic roles in South Korea, Russia, and Finland.

Yunheng Zhou is an associate professor at the School of Public Affairs, Zhejiang University, China. He also serves as the secretary-general of the Environmental & Energy Policy Centre at Zhejiang University. His research interests encompass energy security, energy transition, and global energy governance.

Politics and Governance
2025 • Volume 13 • Article 10508
https://doi.org/10.17645/pag.10508

ARTICLE

Open Access Journal

Fragmented Governance, Shared Norms: Navigating Regime Complexity in Aid Data Governance

Kyung Ryul Park

Graduate School of Science and Technology Policy, Korea Advanced Institute of Science and Technology, Republic of Korea

Correspondence: Kyung Ryul Park (park.kr@kaist.ac.kr)

Submitted: 10 April 2025 **Accepted:** 26 June 2025 **Published:** 23 October 2025

Issue: This article is part of the issue "The Geopolitics of Transnational Data Governance" edited by Xinchuchu Gao (University of Lincoln) and Xuechen Chen (Northeastern University London), fully open access at https://doi.org/10.17645/pag.i437

Abstract

This study examines the evolution of transnational aid data governance through an in-depth analysis of the OECD Creditor Reporting System and the International Aid Transparency Initiative. Conceptualizing data governance as a socio-technical and politically contested process, it explores how the norms of aid transparency and aid effectiveness have diffused globally, and how reporting standards have emerged and become institutionalized within the fragmented architecture of international development cooperation. The study highlights how regime complexity, characterized by overlapping mandates, institutional tensions, and competing mechanisms, has shaped the trajectory of aid data governance. The findings demonstrate that aid data governance is driven not only by technical rationales and functional imperatives but also by political interests and institutional dynamics. Drawing on qualitative case analysis, the study identifies persistent challenges in aligning transparency norms with reporting practices. It calls for a multidisciplinary approach to future research and for adaptive, interoperable frameworks tailored to post-2030 development agendas.

Keywords

aid effectiveness; aid transparency; Creditor Reporting Systems; data governance; International Aid Transparency Initiative; international development cooperation; regime complexity; transnational governance

1. Introduction

No longer confined to technical or functional domains, data now shapes everyday life, organizational cultures, national data sovereignty, and global power dynamics. More importantly, this phenomenon of datafication—the process of converting aspects of society into quantifiable data—has both produced and legitimized outcomes with profound socio-political and global impacts. Uncertainty and rapid change have

led to a growing demand for more agile and effective data governance that supports policymaking and ensures compliance with emerging international norms. Data governance has become a critical issue in contemporary global technology governance and international development. As digital transformation accelerates, data is no longer a passive byproduct of individual, corporate, and governmental activity. It actively shapes how state actors allocate resources, how agencies monitor progress, and how transparency and accountability are framed and enforced. In particular, international development cooperation has witnessed a proliferation of data-driven mechanisms aimed at improving aid effectiveness, enhancing transparency, and enabling evidence-based aid targeting and decision-making.

However, the rise of data-driven mechanisms raises fundamental questions about who sets the standards, who governs data flows, and whose interests these systems ultimately advance. Aid data governance is often portrayed as a neutral and technocratic process, rather than as a deeply political and institutionally embedded practice. This study argues that data governance in development cooperation should be understood as a socio-technical system in which actors, norms, institutions, and technologies co-evolve to shape transnational governance outcomes within the global development field.

To investigate aid data governance, this study focuses on two prominent aid data standards, the OECD's Creditor Reporting System (CRS) and the International Aid Transparency Initiative (IATI), to offer a historically grounded and analytically in-depth understanding of how transnational data governance has emerged, diffused, and become standardized, and how it operates in the practice of international development.

This research contributes to broader debates on transnational data governance by showing how global standards for aid transparency are not merely technical instruments but contested arenas of norm diffusion, power negotiation, and technological innovation. It demonstrates how data governance in development is shaped by geopolitical asymmetries between donor and recipient countries, by the strategic interests of international organizations, and by normative pressures embedded in global development regimes such as the Paris Declaration on Aid Effectiveness in 2005, the Accra Action Agenda in 2008, the Addis Ababa Action Agenda in 2016, and the United Nations Sustainable Development Goals (SDGs), particularly in light of SDG 17. The development agenda has placed significant emphasis on the need for more open, granular (sub-national level), and continuously shareable development cooperation data. The growing importance of transnational data governance underscores the role of global partnerships and monitoring in enhancing development effectiveness. Despite its relevance, academic research has paid relatively little attention to how transnational aid data standards have emerged and evolved.

The article addresses the following research questions. First, how have international standards for aid data governance, particularly IATI and CRS, emerged and evolved within the global field of development cooperation? Second, what institutional, normative, and technical forces have shaped their diffusion, adoption, and institutionalization? Third, what does this evolution reveal about the broader characteristics and challenges of transnational data governance in international development?

This article is structured as follows. The next section reviews existing work on data governance across various academic disciplines, as well as development norms that anchor data governance within the aid sector. Section 3 provides background on the emergence of aid data governance. Section 4 outlines the research design and methodology, examining the appropriateness of a case study approach for this analysis.

Section 5 presents the findings and the empirical analysis of IATI and CRS, and Section 6 discusses implications for both aid governance and global data politics. Section 7 concludes with reflections on future research directions, advocating for a multidisciplinary approach to the study of transnational data governance.

2. Aid Data Governance as an Evolving Institutional Field

This section offers a focused literature review and underscores the critical intersection between data governance and international development cooperation. It also revisits key debates surrounding widely recognized norms in the aid sector, such as aid transparency and aid effectiveness, and incorporates insights from International Relations theory, particularly the concept of regime complexity, to better understand the tensions between global norms and the practical realities of transnational aid data governance. Throughout this review, this study emphasizes the multidisciplinary nature of data governance and the importance of socio-technical perspectives for understanding transnational aid data governance.

2.1. Data Governance as a Multidisciplinary Concept

In recent years, there has been a proliferation of scholarly work on the topic of data governance across disciplines. Data governance commonly refers to how planning, oversight, and control of the management and use of data are exercised and by whom (Data Management Association, 2009). It involves working with stakeholders to consolidate diverse goals and set common standards for data production, sharing, and anonymization, and to ensure that data flows are effectively and ethically transformed into public goods. Researchers have further sought to define data governance from the perspective of information systems (Alhassan et al., 2019; Basukie et al., 2020), public administration (Janssen et al., 2020), communication (Winter & Davidson, 2019), philosophy (Hummel et al., 2021), and political science (Dammann & Glasze, 2023; Liu, 2021). Systematic literature reviews reflect the importance of multidisciplinarity, highlighting the diverse conceptualizations, domains, cross-functionality, and applications of data governance across academic fields (Abraham et al., 2019; Alhassan et al., 2016; Al-Ruithe et al., 2019). Whereas "governance" is widely acknowledged as a basic concept in political science and international relations, early studies of data governance were conducted predominantly within Information Systems and Technology Management (Zuboff, 2023; Zuiderwijk et al., 2012). To date, however, too little attention has been paid to creating deeply contextualized understandings of data governance and investigating its political dynamics.

Scholars recognize that data governance provides a structured framework for data-driven decision-making in organizations (Janssen et al., 2012; Weller, 2008). It identifies responsible actors and codifies procedures that guide their actions and ensure compliance with shared norms, thereby setting the operating rules for data management. In transnational contexts, common data standards and reporting schemes are crucial for coordinating practice across heterogeneous institutional, legal, and political environments in states. However, existing scholarship has paid insufficient attention to the historical and cross-border dynamics by which data governance evolves, focusing instead on stakeholders within national boundaries and sectoral silos. For example, studies examine data governance in relation to private-sector innovation (George et al., 2014), open government initiatives (Janssen et al., 2020; Luna-Reyes et al., 2014), interorganizational coordination (Markus & Bui, 2012), citizen participation, and public-sector data use (Meijer & Potjer, 2018; Sahay, 2016). These approaches often remain bounded by national systems or technical institutions,

overlooking the transnational complexities that increasingly shape global data practices. International development, therefore, settings require frameworks that account for transnational complexity.

2.2. Rethinking Data Governance Through a Transnational Lens

The limited attention to international dynamics in data governance underscores the need for a conceptual lens from international relations, one that elucidates how governance arrangements evolve across borders and why national perspectives often collide with global norms and legal jurisdictions. Data sovereignty has emerged as one of the central concepts for analyzing these tensions. Data sovereignty serves as a normative reference point for determining who governs data, who can access them, and which legal frameworks apply when diverse conflicts arise (Hummel et al., 2021). While it is frequently asserted at the national level, data sovereignty cannot be discussed in isolation. Its inherently transnational nature is evident in ongoing tensions between the EU's General Data Protection Regulation (GDPR), the US's platform liability regimes, and emerging approaches to AI governance. These frictions are not merely legal disagreements. They also reflect strategic assertions of data sovereignty, with states seeking to impose their normative and regulatory preferences within a fragmented and contested global data governance landscape. In this context, conflicting standards represent more than technical incompatibilities. They are expressions of competing visions of control, accountability, and public interest in the digital era.

While data sovereignty centers on who governs and controls data across borders, the concept of regime complexity shifts attention to how multiple international governances coexist and interact without a clear hierarchy or coordination mechanism (Alter, 2022; Alter & Meunier, 2009; Drezner, 2009). As defined by Raustiala and Victor (2004, pp. 278–279), regime complexity is "an array of partially overlapping and nonhierarchical institutions governing a particular issue-area." Early contributions by Alter and Meunier (2009) emphasize that such complexity arises when state and non-state actors pursue their interests across multiple institutional venues, leading to forum shopping, norm collision, and strategic layering of institutions. Drezner (2009) further highlights the power asymmetries and governance challenges that emerge from a fragmented institutional environment.

This view is especially relevant for understanding transnational data governance in international development, where initiatives often operate across competing normative frameworks and overlapping institutional arrangements. Alter and Raustiala (2018) argue that regime complexity is no longer exceptional but a systemic feature of global governance, particularly in domains where power is diffuse and authority is contested. More recently, Alter (2022) underscores how geopolitical and technological transformations continue to shape these dynamics, with direct implications for digital governance, global health, and climate policy.

These governance tensions are closely linked to the diffusion of international norms, which do not always progress linearly. As Finnemore and Sikkink (1998) suggest, norms may emerge, cascade, and become institutionalized, though often unevenly and contentiously in transnational contexts. Norm entrepreneurs promote new institutional visions, such as aid transparency and data governance that gain traction through persuasion, systematization of practices, and their formal embedding within international frameworks. Beyond norm diffusion, coercive, and mimetic isomorphic mechanisms also shape institutionalization (DiMaggio & Powell, 1983). Across these accounts, a core insight is that regime complexity reflects not only

institutional proliferation but also the strategic behavior of actors navigating uncertainty and contested authority. The result is a landscape in which norms and standards coexist, overlap, and compete, shaping how data governance unfolds in practice.

Viewed through this lens, the case of CRS and IATI illustrates regime complexity in practice. IATI emerged in response to limitations within the OECD's CRS but did not replace it. Rather, it coexists alongside it, contributing to overlapping mandates, reporting requirements, and institutional tensions. These overlaps reflect deeper normative and structural divergences, including tensions between transparency and state-centric claims to data sovereignty, access, localization, and control. Understanding IATI's evolution thus requires analytical frameworks that go beyond socio-technical and institutional perspectives, engaging directly with the strategic politics of regime complexity in transnational governance.

2.3. A Socio-Technical View on Data Governance

While the concept of regime complexity highlights the fragmented and overlapping nature of transnational governance arrangements, it does not fully explain how data governance emerges, is negotiated, and becomes institutionalized across countries. To illuminate these dynamics in the aid sector, this study adopts a socio-technical perspective that foregrounds the mutual shaping of technical systems and socio-institutional structures. Originating as a critique of technological determinism, the socio-technical tradition provides a foundation for examining the political, social, and institutional dimensions of diffusion, standardization, and governance (Avgerou, 2000; Bostrom & Heinen, 1977). Prior works trace the socio-economic and organizational consequences of technological change and data standards in globally embedded contexts (Avgerou, 2002; Walsham, 2017). From this point, data governance is co-constructed under organizational and infrastructural constraints. Likewise, the design, adoption, and diffusion of aid information systems reflect power relations, norms, and global dynamics, rendering purely technical explanations insufficient (K. R. Park, 2017a).

A socio-technical lens is therefore well suited to account for the emergence and institutionalization of data governance. Data platforms and information systems must be analyzed in situ (Kling & Lamb, 2000; Lyytinen et al., 2009; Orlikowski & Iacono, 2002). Systems such as ERP, e-government, and contemporary AI function not only as technological artifacts but as socio-institutional arrangements (Orlikowski & Iacono, 2002). This insight is particularly salient in international development, where heterogeneous institutional configurations prevail and authority over data management is anchored in pre-existing hierarchies (Avgerou, 2002; Walsham & Sahay, 2006). Rejecting apolitical or teleological accounts of technology, socio-technical studies emphasize the contingent, embedded, and evolving character of technological governance (Williams & Edge, 1996). Data governance and its related technical standards typically prevail not because of intrinsic technical superiority but because they align with the interests, capacities, and power structures of influential actors.

In sum, transnational data governance is shaped by intersecting technical, political, and institutional forces across national and transnational arenas. Concepts such as norm diffusion, regime complexity, and socio-technical systems together indicate that data governance emerges through negotiation among heterogeneous stakeholders, rather than through technical optimality alone. These insights motivate an integrated analytical framework for explaining how aid data governance has evolved and how it is exercised in practice.

3. Contextualizing Data Governance in International Development

This study traces the historical emergence and institutionalization of transnational aid data governance, and in doing so offers theoretical and policy insights into the evolving relationship among standard-setting, digital transformation, and international development cooperation. While perspectives of regime complexity and socio-technical systems illuminate how data governance emerges through institutional negotiation and technological constraint, these dynamics must be situated within the longer-standing debates, norms, and practices of development cooperation.

In particular, challenges in aid data governance—fragmented implementation, uneven technical and statistical capacity, and competing standards—now intersect with core normative agendas. Among the many norms that have evolved over the past three decades, aid transparency and aid effectiveness have been especially prominent. Understanding how data governance operates therefore requires tracing the historical institutionalization of aid reporting systems, the diffusion of transparency norms, and the changing interplay among international actors, data platforms, and accountability mechanisms.

Foreign aid has been the most direct policy instruments and a major source of external finance for pursuing global development agendas, including the Millennium Development Goals endorsed in 2000 and the Sustainable Development Goals established in 2015 (Fukuda-Parr & McNeill, 2019; Fukuda-Parr & Muchhala, 2020). Debates on aid data governance are closely intertwined with long running discussions of transparency (Ghosh & Kharas, 2011). Amid mixed evidence of economic progress in recipient countries, debates over transparency and effectiveness intensified. Scholars and practitioners sought to determine whether, and under what conditions, aid is transparent and effective (Collier & Dollar, 2004). Efforts to enhance transparency and standardize aid data have been advanced by international norm entrepreneurs such as the OECD Development Assistance Committee (OECD-DAC), and the World Bank. The OECD-DAC's CRS, established in the late 1970s, was the very first effort for data reporting, and has served as the most comprehensive aid database among OECD DAC countries (Findley et al., 2011; Kilama, 2016; Powell & Findley, 2011; Tierney et al., 2011). CRS data function as metadata that clarifies who provides aid, where and how it is delivered, and to what extent cooperation occurs.

The Paris Declaration on Aid Effectiveness (2005) signaled a pivotal moment by emphasizing aid data sharing and the effectiveness of its delivery and use. Its five core principles, including ownership, alignment, harmonization, managing for results, and mutual accountability (OECD, 2005) presuppose robust data sharing. In this architecture, the CRS has operated as a foundational transnational data governance instrument, providing the database and reporting framework that underpin the Paris commitments. The Accra Agenda for Action in 2008 further elevated the role of aid data sharing and drove the use of information systems for sharing aid data. This shift reflected a broader process of coalition building and negotiation among state and non-state actors. In this context, sharing aid data increasingly constituted a norm—understood as "collective understandings that make behavioral claims on actors" (Checkel, 1998).

Meanwhile, attention to emerging information and communication technologies (ICTs) has grown, given their potential to catalyze and support international development cooperation (Gomez & Pather, 2012). Expected benefits of ICTs and aid-data sharing include increased transparency, greater cost-effectiveness in delivery, and enhanced decision-making quality and government capacity (Basu, 2004; Ndou, 2004). By collecting and

managing aid data through a centralized, country-level aid information management system, stakeholders aim to improve aid targeting and overall aid effectiveness (K.R. Park, 2017b). With broadband connectivity and advanced ICT tools expanding in many low- and middle-income countries, such systems became technically feasible, reshaping expectations for aid data governance.

With this backdrop, the IATI was launched in 2008 as a global response to growing demands for more timely, detailed, and accessible aid data. While building upon the foundations of the CRS, the IATI sought to address some of CRS' key limitations, most notably its focus on quantitative and aggregated data set, retrospective and OECD DAC-centered reporting. IATI introduced a complementary standard aimed at enabling real-time, project-level, and forward-looking information sharing across a broader spectrum of development actors, including non-OECD DAC donors, international organizations, recipient governments, and civil society organizations (CSOs; Netherlands Ministry of Foreign Affairs, 2015).

IATI's technical standard was designed to improve interoperability and promote transparency through open data principles. This technical architecture cohered with IATI's institutional aim to constitute an inclusive, multi-stakeholder publishing and access platform, beyond OECD-DAC donors, for machine-readable, comparable aid information (Powell et al., 2015), thereby underpinning the initiative's legitimacy and facilitating endorsement by major bilateral and multilateral donors.

This section examined how aid data governance has evolved as a normative and institutional response to long-standing challenges in international development cooperation. Tracing the emergence of IATI alongside the pre-existing CRS illuminates how global actors have pursued the standardization of aid data in the name of transparency, accountability, and effectiveness. With this context in place, the next section outlines the methodological approach used to analyze the institutionalization of aid data governance in greater empirical depth.

4. Methodology

This study adopts an interpretive case study design. The purpose is to investigate how aid data governance and information-disclosure standards are institutionalized and implemented through interactions among various actors. A case study is appropriate when the main research questions are the "how" and "why" of a social phenomenon in its natural setting (Yin, 2009). Data collection primarily involved semi-structured interviews, the most commonly used method in qualitative case studies, and was supplemented by a literature review and participant observation for triangulation. A total of 12 interviews were conducted with participants, including representatives from IATI and the World Bank, statisticians and aid-reporting specialists from donor agencies; government officials from partner countries; one academic; and two high-level development policymakers deeply engaged with the IATI. Most interviews were conducted between 2016 and 2019, with two follow-up interviews in 2022 and one in 2025 with previously interviewed participants. Each interview lasted 45 minutes to one hour. While a prepared questionnaire guided the interviews, the interaction was adapted to the interviewee's responses, encouraging open and natural dialogue (Kvale, 2009).

Data was also collected from various sources, including project documents, technical reports, policy reports, and other information on the OECD-DAC and the IATI websites. Data was also collected from various

sources, including project documents, technical reports, policy reports, and other information on the OECD-DAC and IATI websites. Because IATI and the OECD-DAC CRS are based on open data, most meetings, minutes, resolutions, and related documents are publicly available on their websites, where researchers have relatively high access to data. The English versions of the full standards and official publications released with each version update were included as subjects of analysis. Official annual reports from the CRS and IATI provided foundational material for detailed analysis of their objectives, direction, and scope of aid data disclosure. Early data collection comprised archival research mainly from 2016 to 2018, with additional data gathered in 2024. Data collected in the first stage, particularly from development agencies, were continuously cross-checked and revisited during analysis to iteratively refine interpretations.

Data analysis followed the general steps of thematic analysis, which involves identifying differences in interpretation and themes across contexts (Fereday & Muir-Cochrane, 2006). While thematic analysis is typically inductive, this study also employed a deductive approach. Certain themes derived from existing research, along with pre-existing categories such as indicators and the data structures of the CRS and IATI, were used to design the interview questions and guide data collection. These predefined themes and categories were subsequently reinterpreted based on the interviews and documentary evidence.

5. Evolution of Aid Data Governance in International Development

5.1. Norm Diffusion and the Emergence of IATI

This study examines the CRS and IATI as a case study of an emerging aid data governance standard and traces the emergence and institutionalization of IATI as an alternative to the OECD CRS. While CRS had served as the dominant aid reporting standard since the 1970s, by the 2000s, it faced increasing criticism due to its limited scope, donor-centric design, reliance on aggregated and retrospective data, and inability to adequately capture data from emerging donors and multilateral initiatives. These limitations, alongside growing normative pressure for openness and accountability, created a policy window for IATI.

As briefly discussed in Section 3, IATI was launched in 2008 through the Accra Agenda for Action. IATI introduced a more flexible, open-data-based, and participatory approach to aid data governance. Though it draws on CRS classifications, IATI distinguishes itself through greater granularity and interoperability. Designed to provide an open data standard for publishing aid data, IATI accommodates a broader array of actors, including non-OECD DAC donors, CSOs, and recipient countries. Unlike CRS, which is centrally governed and standardized, IATI operates as a voluntary initiative with a more open data structure, signaling a shift in governance toward interoperability and openness.

Beyond functional concerns, IATI's emergence also reflected mechanisms of norm diffusion and the political needs of powerful donor countries and international organizations (DiMaggio & Powell, 1983; Finnemore & Sikkink, 1998). Its founding members, mostly affiliated with the OECD-DAC, sought to respond to the changing aid landscape and strategically diffuse a new model for aid data governance. Following the 2008 financial crisis, leading donors pushed for broader burden-sharing and inclusion of new actors in development finance, positioning IATI as a normative and technical tool to achieve these goals. While IATI framed itself as a departure from the CRS regime, its diffusion was also shaped by existing power hierarchies and institutional interests. This can be illustrated as an example of standardization through strategic norm promotion.

IATI's diffusion can be analyzed through the lens of institutional isomorphism to explain its spread and institutional legitimacy. IATI's diffusion is best explained by primarily normative, complementary mimetic, and limited coercive pressures. Normatively, major donors and the World Bank, together with advocacy organizations such as Publish What You Fund, Transparency International, constructed IATI as the appropriate standard for transparency and inclusiveness through knowledge brokering, policy advocacy, and evaluative infrastructures. The Aid Transparency Index, for example, assigned explicit weight to IATI membership and use, thereby codifying expectations and conferring social legitimacy (Publish What You Fund, 2016; Weaver, 2016). In this way, IATI became more than a reporting protocol; it functioned as a platform for institutionalizing transparency norms and reconfiguring authority among standard-setting actors.

Mimetic isomorphism operated under uncertainty surrounding annual CRS reporting among OECD-DAC members and SDG reporting among other actors. Agencies in Sweden, Denmark, and the Netherlands adopted IATI to align with peers and open data practices, producing convergence in functionalities and interfaces. Evidence from versions 2.01 and 2.02 indicates that such emulation fed back into the standard's design, privileging open data formats (Netherlands Ministry of Foreign Affairs, 2015). Also, technical harmonization, interface similarities, and the drive toward machine-readable data formats also reflect mimetic processes, suggesting standardization across agencies.

Coercive isomorphism was comparatively modest, emerging indirectly via incorporation of IATI benchmarks into Global Partnership monitoring and conditionalities, notably following U.S. endorsement after the 2011 Busan Forum. Taken together, these mechanisms account for IATI's institutional recognition despite its voluntary character. At the same time, coexistence with the OECD and CRS overlapping mandates but distinct technical and normative bases sustains regime complexity and organizational tensions. Overall, normative and mimetic pressures appear to be the principal engines of institutionalization, with coercion playing a secondary, enabling role. Together, these dynamics underscore the multifaceted nature of IATI's diffusion and its evolving role in the governance of international development.

5.2. Regime Complexity and Overlapping Memberships: Navigating Aid Data Governance

As of 2025, according to the IATI registry, 105 organizations have formally joined it and adopted the IATI standard for aid reporting and data disclosure, and 20 out of the 35 OECD-DAC members (Australia, Belgium, Canada, Denmark, Estonia, the EU, Finland, France, Germany, Ireland, Italy, Japan, Korea, Luxembourg, the Netherlands, New Zealand, Sweden, Switzerland, the UK, and the US) have formally joined IATI. This reflects a participation rate of approximately 57% of OECD-DAC countries, with a concentration among high-capacity donors and norm entrepreneurs. Their engagement has played a pivotal role in shaping the global aid data governance architecture. In addition to donor countries, the IATI membership includes 23 CSOs, 35 partner countries (aid recipients), major United Nations agencies, international development banks, and five private sector entities. The participation of CSOs reflects the initiative's emphasis on inclusiveness and public accountability in particular. This reflects the significant diffusion of the IATI standard since its launch in 2008. This broad base confirms that IATI is not merely an intergovernmental initiative, but rather a multi-stakeholder governance mechanism that integrates diverse voices into the standard-setting and data-sharing process.

As shown in Figure 1, the growth of IATI membership was most notable between 2008 and 2012, with a marked spike in 2011–2012. A significant turning point occurred in 2011 at the Fourth High-Level Forum in Busan, where the then US Secretary of State Hillary Clinton formally announced the US' accession to IATI. This endorsement by a major donor accelerated momentum and led to a surge in new memberships, peaking in 2012, the year with the highest recorded number of new members joining the initiative. However, in more recent years, membership expansion has slowed considerably.

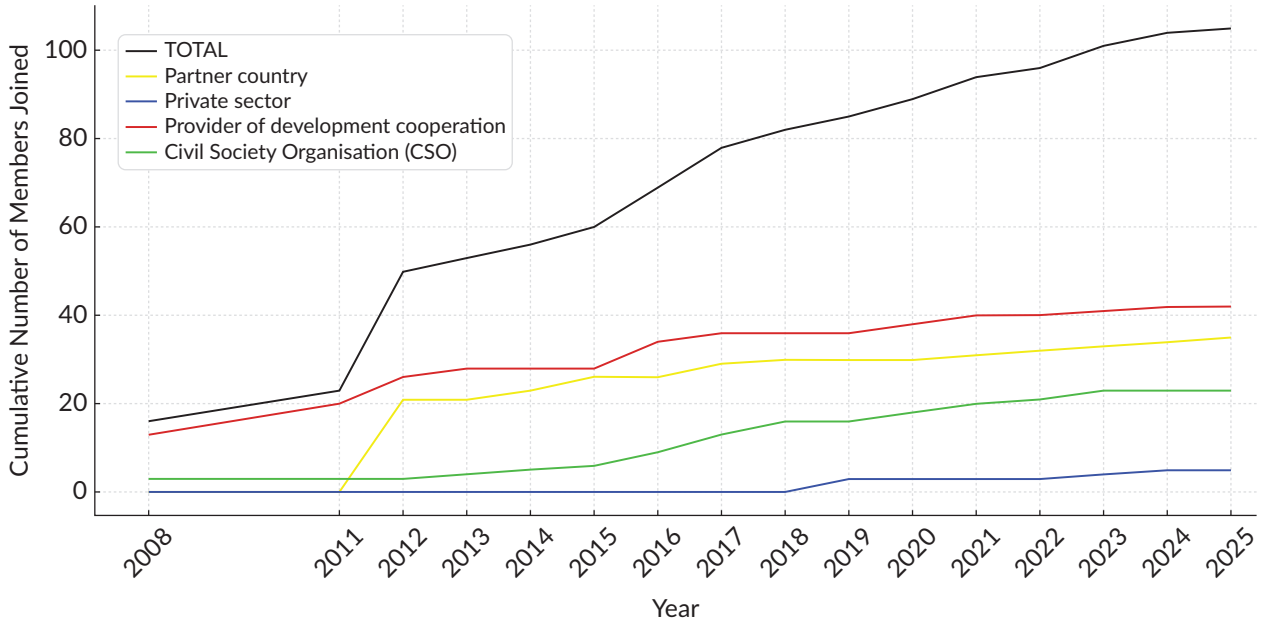


Figure 1. Cumulative IATI membership.

Building upon Raustiala and Victor (2004, p. 279), two prominent features of regime complexity are: (a) the overlaps in scope, membership, and subject matter; and (b) the absence of a clear hierarchy among regimes. From this perspective, in the domain of aid data governance, regime complexity emerged when IATI was introduced alongside the OECD-DAC's CRS. While the CRS had long served as the dominant reporting mechanism for traditional donors, emerging donors such as China and India did not participate in the OECD-led framework, nor did they align with the normative commitments, including transparency and harmonization, as emphasized in the Paris Principles. Moreover, many non-state actors, such as CSOs and philanthropic foundations, had limited or no entry points into the OECD-DAC system, which remained largely donor-centric. The establishment of IATI, with its broader membership and alternative aid data reporting scheme, further contributed to the fragmentation of governance in international development cooperation, exemplifying the dynamics of regime complexity.

Although both IATI and CRS were designed to promote better aid data governance and endorse the Paris Principles, including aid transparency and harmonization, their co-existence clearly shows how overlapping mandates and rule settings within the same policy domain can generate institutional tension and complexity. This reflects a core feature of regime complexity: the absence of a clear hierarchy among multiple governance institutions, which often leads to strategic competition over authority and legitimacy among actors. The early confusion and friction between CRS and IATI also highlighted how different normative foundations, openness versus peer-reviewed intergovernmental accountability, can result in competing standard-setting logics. Such

divergence is not unusual, as actors may choose among overlapping institutions to advance their interests, a dynamic known as "forum shopping" (Drezner, 2009).

The landscape became increasingly marked by overlapping mandates, competing reporting norms, and strategic positioning among actors navigating multiple venues of legitimacy and standard-setting. While the CRS functioned as a central repository tied to OECD-DAC norms, it lacked flexibility and adaptability in response to the shifting configurations of aid delivery and accountability. The emergence of these parallel challenges reflects the growing fragmentation of institutional authority in global aid governance.

Although there are significant similarities between the CRS and the IATI, the very similarities created unexpected organizational and technical challenges in aid reporting practices (Pamment, 2019). One of the main sources of confusion was the duplication of aid reporting practices. While many donor agencies supported the overall vision of IATI, they perceived its additional data reporting requirements as duplicative of their existing CRS reporting systems, resulting in increased labor and time with limited added value. For non-state actors, including CSOs, and partner countries with limited statistical, technical, and financial capacity, IATI implementation was delayed and faced structural obstacles to compliance.

In response to these challenges, IATI released a formal report in 2013 reaffirming its mandate and outlining its commitment to resolving implementation difficulties (IATI, 2013). Also, the IATI secretariat organized technical workshops and capacity-building sessions aimed at helping member organizations align their systems with IATI standards. Despite these efforts, however, structural and political challenges persisted. Technical incompatibilities, inconsistent data ownership, and concerns about overlapping standards continued to hinder broader adoption. Moreover, the underlying tension between IATI's ambition for "real-time, forward-looking transparency" (IATI, 2013) and the more conservative, retrospective orientation of CRS data reporting remained unresolved. These dynamics underscored the enduring complexity of embedding a new transnational standard within an already fragmented aid data governance regime.

More importantly, for potential or future members, uncertainty about the long-term future of IATI has become a key consideration in deciding whether to adopt the standard. As one donor country official noted:

> Honestly, the difference between IATI and CRS is not really significant enough to justify the extra efforts for us. IATI asks for more granular and qualitative data, but we simply do not have the capacity to do both. Maybe 10 years ago, joining IATI helped with visibility and international recognition, but that moment was gone. Now, we are approaching the post-2030, a new post-SDG framework. Who can say if IATI will even survive? From our view, continuing with CRS alone is the most pragmatic option. (Interview, senior aid reporting official)

Interviews reflect a tension within the shared norms but fragmented aid data governance. Donor governments, international organizations, and CSOs often share normative commitments to transparency and accountability. However, these shared values do not always translate into sustained institutional engagement. As the regime complexity literature suggests, the coexistence of overlapping and non-hierarchical standards, such as CRS and IATI, can create coordination problems, institutional fatigue, and strategic disengagement. Even when actors agree with the underlying norms, they may opt out of certain regimes due to resource constraints, perceived redundancy, or uncertainty about institutional longevity.

Therefore, the diffusion of a data governance framework is not necessarily followed by coherent or continuous participation, especially when regime complexity allows actors to selectively align with institutions that better suit their own strategic or operational priorities. Such dynamics help account for why IATI membership has continued to grow incrementally, but at the same time without any significant or sustained surge in recent years. While the normative appeal of aid transparency and the need for transnational aid data governance remain broadly supported, the practical challenges and institutional ambiguities within the regime complex have tempered momentum for large-scale expansion.

5.3. Adopting Data Governance Under the New Norm: From the SDGs to the Post-2030 Landscape

At the United Nations General Assembly in September 2015, attended by heads of state from around the world, the SDGs were adopted as the international community's shared development objectives, replacing the Millennium Development Goals (Fukuda-Parr & McNeill, 2019). In terms of aid data governance, this adds another layer of complexity to aid management practices for development agencies, as organizations are required to report their aid activities annually. Discussions on the use of the IATI standard for implementing the SDGs officially began earlier that year, during the third International Conference on Financing for Development held in July. In Chapter 127 of the Addis Ababa Action Agenda, adopted at this conference, the IATI standard was once again highlighted as a global public data standard for managing aid and for monitoring and evaluation of the SDGs, reaffirming its importance for the international community (United Nations, 2015).

Building on this foundation, the development of a concrete standard reflecting the monitoring mechanisms and implementation plans for the 17 SDGs and their 169 targets began. Notably, the IATI standard underwent its most significant revision in late 2015, transitioning from version 1.05 to 2.01, and later evolving into version 2.03 by 2024. This overhaul aimed to align the standard with the SDGs and their 17 goals and 169 targets. In version 2.02, three new codes—Code 7 (goals), Code 8 (targets), and Code 9 (indicators)—were introduced to reflect SDG goals, targets, and indicators, respectively, integrating them into the IATI framework. The technical and administrative discussions during this process were primarily led by the Inter-Agency and Expert Group on Sustainable Development Goal Indicators, which played a central role in shaping the integration of SDG indicators into the IATI standard.

However, detailed discussions on how the IATI standard can be practically utilized and applied to SDG implementation monitoring remain insufficient. While the IATI standard's vision strongly advocates for participatory and open approaches, the standardization and development processes for linking the IATI to the SDG indicators have been largely top-down. As previously discussed, IATI was developed and refined as a more inclusive, public data-based standard that incorporates qualitative information to address the limitations of CRS. However, IATI continues to map development cooperation projects using the existing CRS codes. This reliance on CRS means that each project can only be assigned a single CRS code, creating structural limitations.

To address this issue, the OECD-DAC discussed the reconfiguration of aid data governance and adoption of "multiple purpose" codes that allow individual development activities to be classified under more than one sector or policy objective, moving beyond a restrictive single code. This direction was also a dedicated topic at the IATI Technical Committee meeting held in Ottawa in 2015. While new discussions and standardization efforts on multiple CRS codes were planned for 2018, another pressing need emerged: the development of a

new SDG mapping code to identify which specific SDG targets individual projects contribute to. Despite its importance, this mapping code has yet to be sufficiently incorporated into the IATI standard since discussions began in 2015.

This reflects the broader challenge of modifying legacy standards like CRS, which, due to their institutional longevity and the OECD-DAC governance structure, exhibit path dependency. At the policy level, CRS purpose codes are rhetorically aligned with SDG targets, but operationally, major gaps remain. This clearly illustrates a case of organizational decoupling, where official alignment with norms exists, but actual practices fail to meet those commitments (Crilly et al., 2012). In this process of decoupling, organizations may symbolically adopt the language of alignment while continuing to operate under legacy systems and simplified coding schemes that limit meaningful integration with SDG monitoring frameworks (Crilly et al., 2012). The IATI, while more flexible and inclusive in design, has been constrained by its dependency on CRS, limiting its responsiveness to SDG-specific data demands. Further challenges include the limited use of optional fields within the IATI standard. While 13 fields are mandatory, most SDG-relevant information resides in optional fields that are often underutilized, particularly by donor agencies with constrained capacity. The absence of user-friendly data platforms to analyze IATI data and a lack of local embeddedness also hinder its effective application for aid management and SDG tracking. As a result, the full potential of IATI as a dynamic, SDG-aligned data infrastructure remains under-realized.

Looking ahead to the post-2030 era, the future of aid data governance is likely to be shaped by three converging trends: the exponential growth of development data (Independent Expert Advisory Group on a Data Revolution for Sustainable Development, 2014), the integration of machine learning and AI for decision-making (Lee et al., 2023; S. W. Park et al., 2025; Vinuesa et al., 2020), and the increasing ICT capacity in many developing countries (Walsham, 2017). These trends are altering how aid is conceptualized, reported, and governed. The SDGs introduced a complex monitoring system without a unified standard, and this complexity is only deepening—posing significant institutional challenges even for advanced economies (K. R. Park & Y. S. Park, 2024). In this context, the future of IATI, and aid data governance more broadly, will depend to the extent to which the standards remain interoperable, inclusive, and responsive to rapidly changing development priorities. As the influence of AI and science, technology, and innovation (STI) continues to expand, aid data governance must increasingly align with both national and global STI strategies for sustainable development (K. R. Park, 2022). This shift calls for a more integrated, adaptive, and forward-looking aid data governance framework suited to the post-SDG era.

6. Discussion

This study traces the historical emergence and institutionalization of transnational aid data governance, offering theoretical insights and policy implications for the evolving relationship between standard-setting, digital transformation, and international development cooperation.

First, this research addresses a clear gap at the intersection of data governance and development cooperation. Despite growing policy attention to aid transparency, especially under the SDG framework, scholarly analysis of international aid data governance remains limited. By focusing on the CRS and the IATI, the study provides an institutional and comparative account of how data governance has emerged, diffused, and taken root across organizations, clarifying the mechanisms through which these structures operate in practice.

Second, shared international norms, such as aid transparency, openness and effectiveness, do not automatically yield coherent practices. Regime complexity and overlapping mandates often generate tensions that impede durable commitment and inter-organizational coordination. Drawing on socio-technical perspectives, the analysis situates aid data governance as historically contingent and politically embedded. The core challenge is less about technical compliance than about the navigation of competing institutional logics, uneven capacities, and asymmetric power relations across actors and regimes.

Third, this research foregrounds the heterogeneity of actors who are not only norm entrepreneurs and data providers, but also negotiators of what counts as legitimate knowledge, standard practices, and accountable behavior in the aid sector. The institutionalization of aid data governance within organizations and across countries is accordingly a socio-political construction. The IATI standard emerged from negotiations among major donor countries, international organizations, and norm entrepreneurs seeking to embed their interests and ideas in the aid regime. The durability of legacy systems, such as the CRS, signals inertia and path dependence. Although a broad coalition participates (including donor agencies, CSOs, data professionals, and partner-country ministries), marked power asymmetries persist, with major donors and multilateral institutions continuing to dominate agenda-setting, thereby constraining inclusive ambitions. Unlike the trade (WTO) or climate (Paris Agreement) regimes, aid regime lacks binding enforcement, resulting in fragmented standards and uneven implementation.

Fourth, despite the growing attention to digital technologies and AI, the practical utility of disclosed aid data is constrained. Many IATI fields are optional and underused. SDG integration faces technical barriers, and accessible analytical platforms remain scarce. These gaps exemplify organizational decoupling, formal alignment with global norms amid weak implementation capacity. Recent advances in machine learning, particularly natural language processing and satellite image processing, can improve the usability of aid data. Automated aid classification and SDG reporting, semantic tagging, and text mining can address data gaps, enable more granular, real-time analysis of aid flows and finally support evidence-based policymaking (Lee et al., 2023). Realizing this potential, however, requires institutional commitment, capacity building, and inclusive governance so that data- and AI-driven transformation genuinely enhances transparency and accountability in the aid sector.

Finally, the study calls for interdisciplinary, methodologically plural approaches that link international relations, policy studies, information systems, and development studies. Priorities include actor-centered and institutional analyses of how data governance affects organizations' behavior and development outcomes, and co-production with diverse stakeholders to strengthen capacity and local uptake. This direction also aligns with SDG 17's emphasis on data-enabled global partnerships to "increase significantly the availability of high-quality, timely and reliable data" (SDG, 17). This study also underscores the need for more integrated, policy-relevant scholarship in addressing the fragmentation of global aid data governance.

7. Conclusion

This research examines the evolution of transnational aid data governance through an in-depth analysis of CRS and IATI. Conceptualizing data governance as a socio-technical and politically contested process, it investigates how the norm of aid transparency has diffused and how global reporting standards have emerged and institutionalized within the field of international development cooperation. This study demonstrates that

aid data governance is not just a technical and functional exercise, but a deep political and institutional process shaped by competing norms, power asymmetries, and regime complexity. The coexistence of overlapping systems like IATI and CRS illustrates persistent fragmentation in global development governance. As the post-2030 agenda approaches, future aid data governance must prioritize interoperability, usability, and responsiveness to diverse stakeholder needs within post-global aid governance.

Acknowledgments

This work was supported by the Global Center for Development and Strategy at Korea Advanced Institute of Science and Technology (KAIST) (Grant Number: A0601006006).

Conflict of Interests

The author declares no conflict of interests.

LLMs Disclosure

During the preparation of this manuscript, an AI-based tool (DeepL) was used for grammar checking and proofreading. All analytical and theoretical work was carried out by the author.

References

Abraham, R., Schneider, J., & Vom Brocke, J. (2019). Data governance: A conceptual framework, structured review, and research agenda. *International Journal of Information Management*, *49*, 424–438.

Alhassan, I., Sammon, D., & Daly, M. (2016). Data governance activities: An analysis of the literature. *Journal of Decision Systems*, *25*(Suppl. 1), 64–75. https://doi.org/10.1080/12460125.2016.1187397

Alhassan, I., Sammon, D., & Daly, M. (2019). Critical success factors for data governance: A theory building approach. *Information Systems Management*, *36*(2), 98–110. https://doi.org/10.1080/10580530.2019.1589670

Al-Ruithe, M., Benkhelifa, E., & Hameed, K. (2019). A systematic literature review of data governance and cloud data governance. *Personal and Ubiquitous Computing*, *23*(5), 839–859 https://doi.org/10.1007/s00779-017-1104-3

Alter, K. J. (2022). The promise and perils of theorizing international regime complexity in an evolving world. *The Review of International Organizations*, *17*(2), 375–396. https://doi.org/10.1007/s11558-021-09448-8

Alter, K. J., & Meunier, S. (2009). The politics of international regime complexity. *Perspectives on Politics*, *7*(1), 13–24. https://doi.org/10.1017/S1537592709090033

Alter, K. J., & Raustiala, K. (2018). The rise of international regime complexity. *Annual Review of Law and Social Science*, *14*(1), 329–349.

Avgerou, C. (2000). IT and organizational change: An institutionalist perspective. *Information Technology & People*, *13*(4), 234–262.

Avgerou, C. (2002). *Information systems and global diversity*. Oxford University Press. https://doi.org/10.1093/acprof:oso/9780199263424.001.0001

Basu, S. (2004). E-government and developing countries: An overview. *International Review of Law, Computers & Technology*, *18*(1), 109–132. https://doi.org/10.1080/13600860410001674779

Basukie, J., Wang, Y., & Li, S. (2020). Big data governance and algorithmic management in sharing economy platforms: A case of ridesharing in emerging markets. *Technological Forecasting and Social Change*, *161*, Article 120310. https://doi.org/10.1016/j.techfore.2020.120310

Bostrom, R. P., & Heinen, J. S. (1977). MIS problems and failures: A socio-technical perspective. Part I: The causes. *MIS Quarterly*, *1*(3), 17–32.

Checkel, J. T. (1998). The constructive turn in international relations theory. *World Politics*, *50*(2), 324–348.

Collier, P., & Dollar, D. (2004). Development effectiveness: What have we learnt? *The Economic Journal*, *114*(496), F244–F271.

Crilly, D., Zollo, M., & Hansen, M. T. (2012). Faking it or muddling through? Understanding decoupling in response to stakeholder pressures. *Academy of Management Journal*, *55*(6), 1429–1448. https://doi.org/10.5465/amj.2010.0697

Dammann, F., & Glasze, G. (2023). Governing digital circulation: The quest for data control and sovereignty in Germany. *Territory, Politics, Governance*, *11*(6), 1100–1120. https://doi.org/10.1080/21622671.2022.2141850

Data Management Association. (2009). *The DAMA guide to the data management body of knowledge (DAMA-DMBOK Guide)*. Technics Publications.

DiMaggio, P., & Powell, W. W. (1983). The iron cage revisited: Institutional isomorphism and collective rationality in organizational fields. *American Sociological Review*, *48*(2), 147–160.

Drezner, D. W. (2009). The power and peril of international regime complexity. *Perspectives on Politics*, *7*(1), 65–70. https://doi.org/10.1017/S1537592709090100

Fereday, J., & Muir-Cochrane, E. (2006). Demonstrating rigor using thematic analysis: A hybrid approach of inductive and deductive coding and theme development. *International Journal of Qualitative Methods*, *5*(1), 80–92.

Findley, M. G., Powell, J., Strandow, D., & Tanner, J. (2011). The localized geography of foreign aid: A new dataset and application to violent armed conflict. *World Development*, *39*(11), 1995–2009. https://doi.org/10.1016/j.worlddev.2011.07.022

Finnemore, M., & Sikkink, K. (1998). International norm dynamics and political change. *International Organization*, *52*(4), 887–917. https://doi.org/10.1162/002081898550789

Fukuda-Parr, S., & McNeill, D. (2019). Knowledge and politics in setting and measuring the SDGs: Introduction to special issue. *Global Policy*, *10*(S1), 5–15. https://doi.org/10.1111/1758-5899.12604

Fukuda-Parr, S., & Muchhala, B. (2020). The Southern origins of sustainable development goals: Ideas, actors, aspirations. *World Development*, *126*, Article 104706. https://doi.org/10.1016/j.worlddev.2019.104706

George, G., Haas, M. R., & Pentland, A. (2014). Big data and management. *Academy of Management Journal*, *57*(2), 321–326.

Ghosh, A., & Kharas, H. (2011). The money trail: Ranking donor transparency in foreign aid. *World Development*, *39*(11), 1918–1929.

Gomez, R., & Pather, S. (2012). ICT evaluation: Are we asking the right questions? *The Electronic Journal of Information Systems in Developing Countries*, *50*(5), 1–14.

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

Independent Expert Advisory Group on a Data Revolution for Sustainable Development. (2014). *A world that counts: Mobilising the data revolution for sustainable development*. United Nations. https://www.undatarevolution.org/report

International Aid Transparency Initiative. (2013). *Complementary roles for the OECD-DAC Creditor Reporting System and the International Aid Transparency Initiative*.

Janssen, M., Brous, P., Estevez, E., Barbosa, L. S., & Janowski, T. (2020). Data governance: Organizing data for trustworthy artificial intelligence. *Government Information Quarterly*, *37*(3), Article 101493. https://doi.org/10.1016/j.giq.2020.101493

Janssen, M., Charalabidis, Y., & Zuiderwijk, A. (2012). Benefits, adoption barriers and myths of open data and

open government. *Information Systems Management*, *29*(4), 258–268. https://doi.org/10.1080/10580530.2012.716740

Kilama, E. G. (2016). Evidences on donors competition in Africa: Traditional donors versus China. *Journal of International Development*, *28*(4), 528–551. https://doi.org/10.1002/jid.3198

Kling, R., & Lamb, R. (2000). IT and organizational change in digital economies: A socio-technical approach. In B. Kahin & E. Brynjolfsson (Eds.), *Understanding the digital economy—Data, tools and research* (pp. 295–324). MIT Press.

Kvale, S. (2009). *Interviews: Learning the craft of qualitative research interviewing*. Sage.

Lee, J., Song, H., Lee, D., Kim, S., Sim, J., Cha, M., & Park, K. R. (2023). Machine learning driven aid classification for sustainable development. In *Proceedings of the thirty-second international joint conference on artificial intelligence* (pp. 6040–6048). IJCAI.

Liu, L. (2021). The rise of data politics: Digital China and the world. *Studies in Comparative International Development*, *56*(1), 45–67. https://doi.org/10.1007/s12116-021-09319-8

Luna-Reyes, L. F., Mellouli, S., & Bertot, J. C. (2014). Open government, open data, and digital government. *Government Information Quarterly*, *31*(1), 4–5.

Lyytinen, K., Newman, M., & Al-Muharfi, A. R. A. (2009). Institutionalizing enterprise resource planning in the Saudi steel industry: A punctuated socio-technical analysis. *Journal of Information Technology*, *24*(4), 286–304. https://doi.org/10.1057/jit.2009.14

Markus, M. L., & Bui, Q. N. (2012). Going concerns: The governance of interorganizational coordination hubs. *Journal of Management Information Systems*, *28*(4), 163–198. https://doi.org/10.2753/MIS0742-1222280407

Meijer, A., & Potjer, S. (2018). Citizen-generated open data: An explorative analysis of 25 cases. *Government Information Quarterly*, *35*(4), 613–621. https://doi.org/10.1016/j.giq.2018.10.004

Ndou, V. D. (2004). E-government for developing countries: Opportunities and challenges. *The Electronic Journal of Information Systems in Developing Countries*, *18*(1), 1–24.

Netherlands Ministry of Foreign Affairs. (2015). *How to use the IATI standard: Publication guidelines for partners, contractors and suppliers.* Helpdesk Open Data. https://helpdesk-opendata-minbuza.nl/wp-content/uploads/2019/05/how-to-use-the-iati-standard-1.pdf

OECD. (2005). *The Paris Declaration on Aid Effectiveness*.

Orlikowski, W. J., & Iacono, C. S. (2002). Desperately seeking the "IT" in IT research—A call to theorizing the IT artifact. *Information Systems Research*, *12*(2), 121–134.

Pamment, J. (2019). Accountability as strategic transparency: Making sense of organizational responses to the International Aid Transparency Initiative. *Development Policy Review*, *37*(5), 657–671. https://doi.org/10.1111/dpr.12375

Park, K. R. (2017a). An analysis of aid information management systems (AIMS) in developing countries: Explaining the last two decades. In T. X. Bui & R. H. Sprague Jr. (Eds.), *Proceedings of the 50th Annual Hawaii International Conference on System Sciences* (pp. 2580–2589). IEEE Computer Society. https://doi.org/10.24251/HICSS.2017.312

Park, K. R. (2017b). *Why do aid information management systems fail? Understanding global diffusion of data-driven development initiatives and sustainability failure in the case of Indonesia* [Unpublished doctoral dissertation]. London School of Economics and Political Science.

Park, K. R. (2022). Science, technology, and innovation in sustainable development cooperation: Theories and practices in South Korea. In H. Kwon, T. Yamagata, E. Kim, & H. Kondoh (Eds.), *International development cooperation of Japan and South Korea: New strategies for an uncertain world* (pp. 179–208). Springer Nature.

Park, K. R., & Park, Y. S. (2024). Addressing institutional challenges in sustainable development goals implementation: Lessons from the Republic of Korea. *Sustainable Development*, *32*(1), 1354–1369. https://doi.org/10.1002/sd.2725

Park, S. W., Lee, D. J., Ahn, K., Choi, Y., Lee, J., Cha, M., & Park, K. R. (2025). Classifying and tracking international aid contribution towards SDGs. In *Proceedings of the thirty-fourth international joint conference on artificial intelligence* (pp. 9845–9852). IJCAI. https://doi.org/10.48550/arXiv.2505.15223

Powell, J., Arancibia, B., Cisse, H., & Ferreyra, F. (2015). *Use of IATI in country systems*. International Aid Transparency Initiative (IATI) & Development Gateway.

Powell, J., & Findley, M. (2011). *The swarm principle? A sub-national spatial analysis of donor coordination in Sub-Saharan Africa*. Brigham Young University.

Publish What You Fund. (2016). *Aid Transparency Index 2016 report*. Publish What You Fund. https://www.publishwhatyoufund.org/the-index/2016

Raustiala, K., & Victor, D. G. (2004). The regime complex for plant genetic resources. *International Organization*, *58*(2), 277–309.

Sahay, S. (2016). Big data and public health: Challenges and opportunities for low and middle income countries. *Communications of the Association for Information Systems*, *39*(1), 419–438. https://doi.org/10.17705/1CAIS.03920

Tierney, M. J., Nielson, D. L., Hawkins, D. G., Roberts, J. T., Findley, M. G., Powers, R. M., Parks, B., Wilson, S. E., & Hicks, R. L. (2011). More dollars than sense: Refining our knowledge of development finance using AidData. *World Development*, *39*(11), 1891–1906. https://doi.org/10.1016/j.worlddev.2011.07.029

United Nations. (2015). *Transforming our world: The 2030 agenda for sustainable development*.

Vinuesa, R., Azizpour, H., Leite, I., Balaam, M., Dignum, V., Domisch, S., Felländer, A., Langhans, S. D., Tegmark, M., & Fuso Nerini, F. (2020). The role of artificial intelligence in achieving the Sustainable Development Goals. *Nature Communications*, *11*(1), Article 233. https://doi.org/10.1038/s41467-019-14108-y

Walsham, G. (2017). ICT4D research: Reflections on history and future agenda. *Information Technology for Development*, *23*(1), 18–41. https://doi.org/10.1080/02681102.2016.1246406

Walsham, G., & Sahay, S. (2006). Research on information systems in developing countries: Current landscape and future prospects. *Information Technology for Development*, *12*(1), 7–24. https://doi.org/10.1002/itdj.20020

Weaver, C. E. (2016, September 1–4). *The donor scramble: The aid transparency index and the power of global performance assessments* [Paper presentation]. Annual Meeting of the American Political Science Association (APSA), Philadelphia, United States.

Weller, A. (2008). Data governance: Supporting datacentric risk management. *Journal of Securities Operations & Custody*, *1*(3), 250–262.

Williams, R., & Edge, D. (1996). The social shaping of technology. *Research Policy*, *25*(6), 865–899.

Winter, J. S., & Davidson, E. (2019). Big data governance of personal health information and challenges to contextual integrity. *The Information Society*, *35*(1), 36–51. https://doi.org/10.1080/01972243.2018.1542648

Yin, R. K. (2009). *Case study research: Design and methods* (Vol. 5). Sage.

Zuboff, S. (2023). *The age of surveillance capitalism: The fight for a human future at the new frontier of power*. PublicAffairs.

Zuiderwijk, A., Janssen, M., Choenni, S., Meijer, R., & Alibaks, R. S. (2012). Socio-technical impediments of open data. *Electronic Journal of e-Government*, *10*(2), 156–172.

About the Author

Kyung Ryul Park is an associate professor in the Graduate School of Science and Technology Policy, Korea Advanced Institute of Science and Technology (KAIST), and an adjunct professor at New York University. He is the Founding Director of KAIST Global Center for Development and Strategy (G-CODEs).

POLITICS AND GOVERNANCE
ISSN: 2183-2463

Politics and Governance is an international, peer-reviewed open access journal that publishes significant and cutting-edge research drawn from all areas of political science.

Its central aim is thereby to enhance the broad scholarly understanding of the range of contemporary political and governing processes, and impact upon of states, political entities, international organisations, communities, societies and individuals, at international, regional, national and local levels.

cogitatio

www.cogitatiopress.com/politicsandgovernance