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.

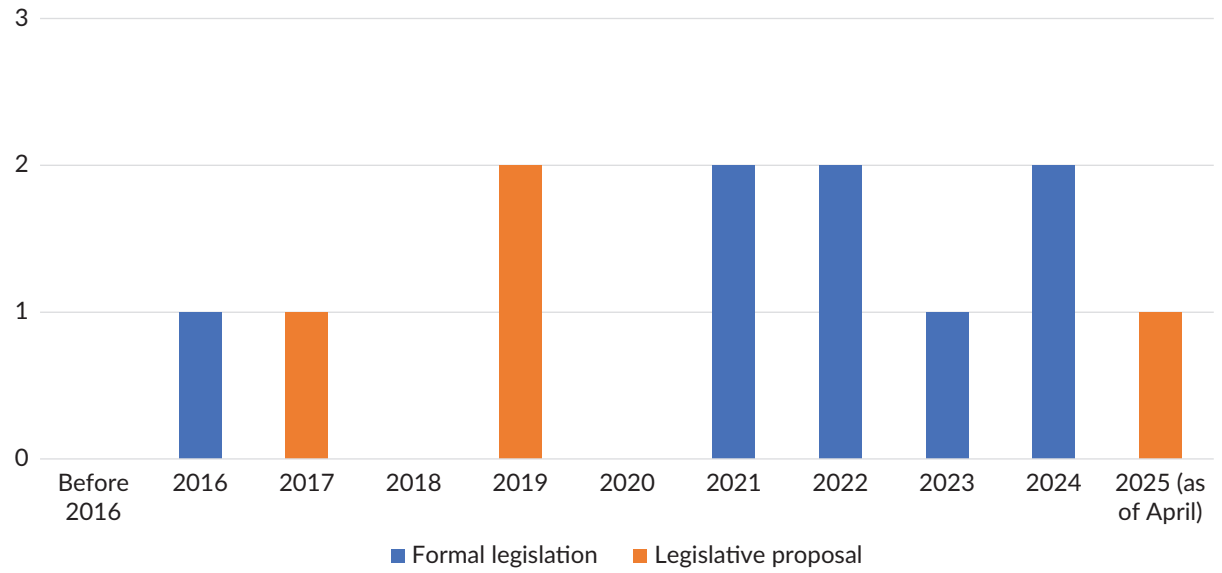


Figure 1. China's legislative activities for transnational data governance.

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

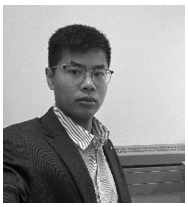
Zhang, Y. (2024). *Personal data protection and data transfer regulation in China*. Vrije Universtiteit Brussel. https://brusselsprivacyhub.com/wp-content/uploads/2024/04/Personal-Data-Protection-in-China.pdf

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.