Proceedings of ICILLP 2025 Symposium: Property Law and Blockchain Applications in International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.LD30084

The Current State of Global Data Sovereignty Legislation and Chinese Enterprises' Responses

Zihan Guo

College of Foreign Studies, Guilin University of Technology, Guilin, China
guozhlyggut@glut.edu.cn

Abstract. In the digital age, data constitutes an integral component of national sovereignty. Divergent global legislative priorities regarding data ownership and security—specifically those centered on EU protection, US market freedom, and China's state control—create significant and systemic compliance predicaments for enterprises engaged in cross-border data practices. This paper utilizes literature review and case analysis, focusing on the compliance challenges faced by Chinese technology enterprises like TikTok, to systematically compare the current data sovereignty legislation models across the European Union, the United States, and China. The analysis reveals that these predicaments transcend mere legal and technical differences, fundamentally manifesting as an institutional byproduct of great-power competition and digital geopolitics. In response, Chinese enterprises should establish systemic, verifiable compliance management frameworks, utilize technological means to enhance data security and probative force, proactively engage in international standard-setting, and promote regional mutual recognition mechanisms. This comprehensive strategy is essential for continuously elevating China's voice and initiative in the field of cross-border data flows, thereby contributing to the refinement of the global data governance system.

Keywords: Data Sovereignty, Cross-Border Data Flow, Compliance, Geopolitics, Digital Governance

1. Introduction

With the continuous advancement of the digital economy, data has been firmly established as an essential production factor, often ranked alongside traditional factors like land, capital, and labor. Simultaneously, data is recognized globally as a critical factor influencing national security, placing the concept of data sovereignty—which emphasizes that data handling must adhere to the laws of the country where it resides —at the core of legislative processes worldwide [1].

However, a fundamental conflict arises from the varying emphasis nations place on data legislation. The European Union's approach, primarily guided by the General Data Protection Regulation (GDPR), prioritizes personal data protection [2]. In contrast, the United States traditionally favors a decentralized, market-driven approach advocating for data freedom, though this is increasingly tempered by strategic national security interventions [3, 4]. China's model, encapsulated by the Data Security Law , mandates the coordinated development of data resources

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.LD30084

alongside security requirements. These divergent legislative priorities inevitably create systemic friction and impose substantial compliance costs on enterprises undertaking cross-border data activities.

Hence, in response to this key issue, this paper employs two approaches, namely literature review and case study, to analyse these conflicting interests. Through a comparison of data sovereignty legislation models of the EU, the US and China, and an analysis of the recent data sovereignty cases of TikTok, this study attempts to identify the concrete institutional and geopolitical challenges that Chinese enterprises are facing. The research findings are expected to provide practical assistance to improve the compliance capacity and international competitiveness of Chinese enterprises in the global digital economy.

2. Literature review: data sovereignty legislative models

Extensive global literature addresses the fragmentation of data sovereignty laws. Existing research typically categorizes global data sovereignty legislation into three primary models : the EU model focused on data "protection," the US model emphasizing "free trade," and the emerging economies model, exemplified by China, centered on "sovereignty-based" principles.

2.1. The protection-centric EU model

The EU model's evolution consistently emphasizes individual data rights and privacy. Its central regulatory feature is the "adequacy determination" requirement, which places strict protective restrictions on data transfers to third-party countries that do not meet EU standards [5]. While this framework assures data security and safeguards citizens' privacy rights within its borders, its institutional rigidity results in high compliance costs and significant friction for non-EU enterprises engaged in cross-border data flows . The legislative history leading to the current framework includes the 1995 Data Protection Directive, the 2016 GDPR, and the subsequent 2022 Data Governance Act and Data Act.

2.2. The market centric/strategic US model

The US adheres to a market-oriented approach generally advocating for unrestricted data flow. However, this framework is fundamentally rooted in safeguarding US commercial interests and advancing its data sovereignty strategy. This strategic characteristic became increasingly pronounced following the enactment of the CLOUD Act and the Protecting Americans' Data from Foreign Adversaries Act of 2024 (PADFA). These laws effectively redefine the principle of "free flow of data" as "free flow within the circle of allies," meaning that the US model, while promoting domestic digital economic development, ultimately employs its technological hegemony to erect barriers against competitors, complicating international data governance [4, 6, 7].

2.3. The sovereignty-based emerging economies model

Emerging economies, represented by China, center their approach on comprehensive national security. Key legislation, including the Data Security Law, the Personal Information Protection Law, and the Cybersecurity Law, establishes systems for data classification and tiered management, alongside mandated security assessments for cross-border transfers. This model prioritizes strengthening state strategic control over data resources to safeguard national security and public

DOI: 10.54254/2753-7048/2025.LD30084

interests. However, the resulting procedural complexity increases the regulatory burden for enterprises seeking to facilitate cross-border data transfers [5].

2.4. Research context and transition

Existing academic research suggests that effective counterstrategies for Chinese enterprises must be multidimensional, focusing on two main angles: internal corporate compliance (developing transnational data policies aligned with host country laws) and external collaborative cooperation (engaging with regulators to promote risk assessment mechanisms and refine self-regulatory standards) [5]. These foundational strategic angles inform the analysis of specific operational challenges faced by Chinese firms abroad.

3. Challenges facing Chinese enterprises under EU and US data sovereignty models

The challenges experienced by Chinese enterprises, as exemplified by TikTok's regulatory scrutiny, demonstrate that data compliance issues are often inseparable from institutional distrust and geopolitical tensions.

3.1. The EU model: conflicts in logic and transparency predicaments

Use title case for the paper title. Function words like "at", "or", "with", etc. should not be capitalized unless they are the first word of the title.

3.1.1. Data sovereignty logic conflict

The core conflict lies in the fundamental philosophical divergence: the EU prioritizes individual privacy rights through the GDPR, while the Chinese model prioritizes security and state interests. This ensures that China has yet to secure an adequacy determination from the EU [8]. This structural misalignment renders operational compliance measures, such as TikTok's "Clover Plan" to localize data storage in Finland, ultimately insufficient to mitigate systemic regulatory risk.

The continuation of an investigation by the Irish Data Protection Commission (DPC) against TikTok, despite its localization efforts, illustrates that the legal origin and institutional alignment of the parent country (China) are weighted heavier than the local operational compliance efforts of the subsidiary. The problem is thus structural—China's security-focused legal framework is inherently deemed lacking in "adequacy" by the EU, leading Chinese enterprises to face inherent institutional prejudice regardless of their operational setup.

3.1.2. Technological transparency deficit

The EU and Chinese data sovereignty models define technological transparency differently. In China, transparency primarily serves to provide regulators with information necessary to prove compliance with national security and public interest laws [9]. The EU model, in contrast, mandates transparency toward the user, requiring clear disclosure of data processing methods, purpose, legal basis, and the functioning of algorithmic decision-making, as enforced by the GDPR and the Digital Services Act (DSA) [10] .

TikTok's personal preference recommendation mechanism, which relies heavily on complex machine learning and vast behavioral data, is inherently difficult to explain simply to users. Furthermore, TikTok, in protecting its commercial interests, does not disclose its algorithm source

DOI: 10.54254/2753-7048/2025.LD30084

code. This difficulty in furnishing sufficient, simple proof of compliance contributes directly to regulatory suspicion, fueling the DPC's investigation concerning the potential transfer of user data.

3.2. The American model: legal-technological hegemony and geopolitical entanglement

3.2.1. Legal and technological hegemony beneath the facade of "free flow"

While the US advocates for free-market-oriented data flow, its actions often amount to stringent control over foreign cross-border data flows under the pretense of safeguarding national security. The passage of the Protecting Americans from Foreign Adversary Controlled Applications Act (PAFACA) in 2024, which mandated the divestiture or prohibition of TikTok based on prior assertions of national security risks, extended US legal jurisdiction over cross-border data and restricted data freedom [11].

This instrumentalization of legislation for geopolitical objectives validates the perception that US "free flow" is effectively a "one-way flow" that serves US strategic control over foreign entities. By establishing control over cross-border data flows and localization, this approach reinforces America's dual hegemony in law and technology within global digital governance, legitimizing the suppression of foreign competitors.

3.2.2. Compliance subsumed by geopolitical rivalry

The US legal framework explicitly incorporates the enterprise's home country laws and national will into its risk assessments. In the case of TikTok, Inc. v. Garland , the court cited Article 7 of China's National Intelligence Law as a crucial evidentiary basis for Congress to determine if TikTok constituted a "foreign adversary-controlled application". This approach confirms that the regulatory process disregards a company's operational compliance practices within the US market [12].

Instead, the existence of the parent country's law is used as institutional pretext for exercising technological protectionism. The variable driving regulatory action is state-level geopolitical rivalry, rendering corporate compliance efforts moot in high-stakes sectors. The "free flow" data legislation model is thus passively subsumed within a framework of legal and political hegemony, drawing compliant enterprises into geopolitical rivalry.

4. Counterstrategies for Chinese enterprises amidst global data sovereignty

The complex compliance environment necessitates a strategic, dual-pronged response focused on internal system resilience and external governance influence.

4.1. Internal strategies: building integrated compliance systems and technological empowerment

4.1.1. Establishing systemic, adaptive compliance frameworks

Chinese enterprises must move beyond localized fixes to construct a unified, systemic compliance architecture that can dynamically adapt to conflicting national data sovereignty logics (China's security, EU's privacy, US's hegemony).

This internal system requires the implementation of dynamic data classification, moving beyond fixed standards to conduct comprehensive asset reviews and apply flexible, tiered management across diverse legal jurisdictions. Secondly, enterprises must establish cross-jurisdictional vetting,

DOI: 10.54254/2753-7048/2025.LD30084

enforcing mandatory multi-level approval and control mechanisms during data collection, storage, and cross-border transmission to create a verifiable compliance chain. Finally, to formally demonstrate reasonable diligence, the system must continuously generate probative documentation, such as audit reports and compliance assessment materials, which can serve as critical evidence for global regulatory authorities or as leverage in negotiations.

4.1.2. Technological compliance enablement and enhancing probative force

Given the institutional distrust expressed by European and American regulators regarding the transparency of Chinese data processing, enterprises must strategically utilize advanced technology not just for security, but to enhance their probative force—the ability to furnish incontrovertible proof of compliance [13].

This involves two key technical measures: First, leveraging big data and cloud platforms to refine data classification and traceability systems, allowing full oversight of data approval and real-time tracking of data flows. Second, the development of data-sharing platforms must employ privacy-enhancing technologies (PETs). The strategic use of PETs fundamentally addresses the systemic distrust by offering cryptographically verifiable assurance of compliance, allowing data utility to be shared (e.g., auditing, aggregated analysis) without compromising the underlying original information. This technical assurance provides an objective counter-measure against politically charged accusations of "backdoors" or "uncontrollable" risks.

4.2. External strategies: engaging in global governance and fostering mutual recognition

4.2.1. Proactive engagement in international standards and norm setting

To counteract the institutional exclusion inherent in the US's legal and technological hegemony, Chinese enterprises must shift their focus from passive adaptation to active standard formulation.

Enterprise leaders should proactively contribute their technical solutions and governance perspectives during the formation phase of technical standards and data governance norms within major international bodies (such as ISO, ITU, and IEEE) . This participation enhances the voice and initiative of Chinese enterprises and builds global trust [14]. Concurrently, enterprises should advocate for and promote bilateral and multilateral mechanisms to navigate the fragmented digital trade regime complex, exemplified by international agreements like the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP), thereby reducing cross-border compliance friction [15].

5. Conclusion and future outlook

Analysis of foreign data sovereignty legislation shows that the conflicts between different priorities (namely, the privacy-oriented focus of EU, the strategic market control of US and the security focus of China) have formed politically charged compliance situations for Chinese enterprises and proven that cross-border data regulation is an inherently political arena where cross-border data regulation requirements are more and more instrumentalized as strategic barriers to entrench current global power configurations. The four types of predicaments mentioned above are presented in form of four structural patterns: logic conflict of data sovereignty, technical transparency gap, threat of legal and technological hegemony, and involuntary entanglement in great power rivalry. The successful navigation should be constructed upon four pillars: internal systemization and strict verification,

DOI: 10.54254/2753-7048/2025.LD30084

technological empowerment (especially PETs) to alleviate institutional distrust, active participation in global standards formulation, and institutionalization of regional mutual recognition.

This study only involved legislative models of European Union and the United States. It is necessary for future research to broaden its perspective to the data governance models of other emerging markets/regions apart from EU and the United States, so as to formulate more comprehensive and detailed development strategies, this gradual engagement would help enhance China's agency in cross-border data flows and provide inputs for improving the global data governance system.

References

[1] Couture, S., & Toupin, S. (2019). What does the notion of "sovereignty" mean when referring to the digital? New Media & Society, 21(10), 2305–2322.
[2] Zheng, M. (2022). Qianxi Oumeng "Tongyong Shuju Baohu Tiaoli" ji qi Hegui Yaoqiu (A brief analysis of the EU's General Data Protection Regulation and its compliance requirements). Zhongguo Yuanyang Haiyun, (04), 48–52.
[3] Cate, F. H., Cullen, P., & Mayer-Schonberger, V. (2013). Data protection principles for the 21st century.
[4] Li, X. J., & Wang, Z. X. (2023). Meiguo Shuzi Maoyi Zhanlue: Qu Shi, Ying Xiang yu Yingdui (The United States' digital trade strategy: Trends, impacts, and responses). Renmin Luntan, 14, 89–93. https://doi.org/10.3969/j.issn.1004-3381.2023.14.020
[5] Zhou, X. (2025). Qiye Shuju Kuajing Liudong de Hegui Tiaozhan yu Celue Fenxi (Compliance challenges and strategy analysis for cross-border data flows in enterprises). Jingji Shi, (07), 275–276, 281.
[6] Huang, H. Y., & He, M. T. (2019). Jiyu CLOUD Faan de Meiguo Shuju Zhuanquan Zhanlue Jiedu (An interpretation of the US data sovereignty strategy based on the CLOUD Act). Journal of Information Resource Management, 9(2), 34–45.
[7] Tang, Z. (2025). Shuju Kuajing Liudong Guoji Guize Suipianhua yu Xietiao Lujing (Fragmentation and coordination pathways in international rules governing cross-border data flows). Jiangxi Shehui Kexue, 45(06), 112–124, 207, 209.
[8] Voss, W. G. (2024). China data flows and power in the era of Chinese Big Tech. Northwestern Journal of International Law & Business.
[9] Roberts, H. (2023). Governing artificial intelligence in China and the European Union: Policy approaches and regulatory divergence. Journal of Contemporary Asian Studies, 52(4), 421–440.
[10] OECD. (2024). Algorithmic transparency in the public sector: A state-of-the-art report of algorithmic transparency instruments (OECD Working Paper). Organisation for Economic Co-operation and Development.
[11] Protecting Americans from Foreign Adversary Controlled Applications Act, H.R. 7521, 118th Congress (2023). U.S. House of Representatives.
[12] TikTok, Inc. v. Garland, No. 24-1234 (D.C. Cir. filed May 7, 2024).
[13] Czarnocki, J., Giglio, F., Kun, E., Petik, M., & Royer, S. (2021, November). Government access to data in third countries: Final report. Milieu Consulting, for the European Data Protection Board.
[14] Gong, J. J., & Zhang, V. Y. (2025). China's evolution in international standardization: From follower to global leader (Background paper for the World Development Report 2025). World Bank.
[15] Gao, X., & Chen, X. (2024). The regime complex for digital trade in Asia and China's engagement. Asia Europe Journal. Advance online publication.