Legal Compliance Risks and Strategic Responses in Cross-Border Data Flows of Chinese Enterprises

Xu Hao*

Faculty of Laws, University College London, London, United Kingdom

*xu.hao.23@alumni.ucl.ac.uk

Abstract. In today's global landscape, economic globalisation is gathering pace, deepening the interdependence of trade relations between nations and regions. Data, as a fundamental economic resource and a crucial element of international trade cooperation, has become a key driver of new growth models and a central influence on productivity. As a result, three issues have become central in national and regional regulations: the management of cross-border data flows, the protection of personal information, and the safeguarding of data security at a macro level. This paper explores the legal risks and response strategies linked to cross-border data flows, highlighting the protection of Chinese enterprises' rights and interests. Based on a review of China's current regulatory framework, it identifies several ongoing challenges. The legal definition of data-related objects still requires clarification, and the implementation of data localisation rules shows certain limitations. In addition, the allocation of responsibilities among regulatory authorities needs better coordination, while rising de-globalisation trends pose potential risks of imbalance in global data governance. Through an analysis of China's existing regulatory mechanisms for cross-border flows of personal data, this study argues that China should continue strengthening relevant laws and regulations while improving the allocation of institutional responsibilities. At the same time, it should closely track developments in international legislation, engage in cross-border data cooperation and dialogue, and coordinate with the international community in managing these flows.

Keywords: Cross-border data flows; Data compliance; Corporate data governance; Personal data protection; China

1 Introduction

The rapid growth of the digital economy has accelerated the datafication of corporate and personal information, highlighting data's dual role as both an economic resource and a driver of productivity. In an interconnected world, data underpins global trade by supporting the flow of goods, services, and people, and has emerged as a strategic factor in international competitiveness. Consequently, the governance of cross-border data flows has become a key policy concern for governments and international organisations alike. Driven by the dual imperatives of data sovereignty and privacy protection, many

T. Chamaratana et al. (eds.), *Proceedings of the 2026 12th International Conference on Digital Humanities and Frontiers in Social Sciences (DHFSS 2026)*, Advances in Social Science, Education and Humanities Research 1031,
https://doi.org/10.2991/978-2-38476-611-6_47

jurisdictions have established comprehensive regulatory frameworks to govern data use and cross-border transfers. And these regimes aim to protect national security, safeguard individual privacy, and provide legal certainty, yet their enforcement can limit the flow of data, thus affecting operational efficiency, market integration, and digital innovation [1]. Existing studies on data compliance look at several aspects, including the classification, collection, and cross-border transfer of both personal and non-personal data, as well as the responsibilities of different actors, like government agencies, businesses, and individuals [2]. In this complex regulatory environment, enterprises encounter growing compliance challenges that demand careful legal understanding and flexible governance approaches. In this context, the paper examines the legal and operational issues faced by Chinese enterprises in cross-border data transfers, analyses the structural risks present in China's current regulatory framework, and considers potential legal reforms to support secure, efficient, and internationally interoperable data governance.

2 Evaluation of Risks in China's Cross-Border Data Flows

2.1 Difficulties in Identifying the Relevant Legal Objects

The classification of legal objects determines how cross-border data compliance is implemented in China. However, the definitional ambiguities surrounding personal information and important data create significant uncertainty for enterprises, thereby increasing compliance risks and administrative burdens. For example, China's Data Security Law (DSL) broadly defines "data" as any recorded information but provides little guidance on distinguishing categories subject to different compliance obligations [3,4]. Consequently, enterprises often struggle in practice to determine which data types fall under cross-border transfer controls [5].

The main challenge lies in defining personal information. The Personal Information Protection Law (PIPL) adopts a "relational" model, covering all information linked to an identifiable natural person. While this ensures comprehensive legal coverage, it also broadens the regulatory scope, potentially encompassing routine operational data such as IP addresses, communication logs, or payment records. This maximalist approach risks turning the PIPL into a "law of everything," under which nearly all cross-border data activities may require complex compliance reviews, leaving enterprises uncertain about which transfers implicate protected rights [6,7]. Under the PIPL, enterprises bear specific legal obligations when processing or exporting personal information. These include conducting personal information protection impact assessments (PIPIAs) before export, signing standard contractual clauses (SCCs) with overseas recipients, and ensuring third-party supervision in cases involving sensitive data. Non-compliance may trigger administrative penalties, suspension of operations, or inclusion on the national credit blacklist. The national standard Personal Information Security Specification seeks to reduce this uncertainty by dividing personal information into thirteen categories and specifying "sensitive information." In practice, however, inconsistencies remain [5]. Yet, this standard has played a positive harmonising role by providing structured classification templates and compliance checklists that facilitate automated audits

within enterprises (CNIS, GB/T 35273–2020). Many technology firms have already implemented these guidelines through data-tagging systems and machine-learning tools that automatically flag high-risk personal information, enhancing internal compliance efficiency. The identification of important data poses another challenge. The concept appears in the Cybersecurity Law and sectoral regulations but remains ill-defined. The 2017 Draft Measures for Security Assessment of Cross-Border Data Transfers described important data as information affecting national security, economic development, or public interests. This definition is abstract and hard to operationalise. Later instruments, such as the Provisions on Automotive Data Security and the 2022 Draft Guide to the Identification of Important Data, added industry-specific examples but did not resolve the underlying ambiguity.

Nevertheless, these efforts reflect gradual progress toward operational clarity. Some pilot sectors, such as the automotive and energy industries, have begun developing industry-level data maps to distinguish "important" from "core" datasets, which has improved predictability for enterprises. Over-classification can lead to unnecessary localisation costs, while under-identification risks regulatory penalties. Therefore, rather than viewing the system as purely restrictive, China's emerging multi-tiered framework is progressively refining its taxonomy of data obligations, supporting both national security and cross-border business certainty. The blurred boundary between personal information and important data continues to pose interpretive challenges, but coordinated legislative refinement and technological standardisation have begun to enhance regulatory predictability.

2.2 Limitations and Applicability of Data Localisation

By strengthening national security, data localisation policies simultaneously create key compliance challenges and operational uncertainty for businesses. China's data localisation policy centres on Article 37 of the Cybersecurity Law, which requires operators of critical information infrastructure (CII) to store the personal information and important data they collect within the country, thereby safeguarding national security [8,9]. Under this provision, cross-border transfers are permitted only following an official security assessment [10]. While this policy inevitably increases compliance demands, it also enhances national capacity for cybersecurity oversight and incident response. According to the Cyberspace Administration of China (CAC), localisation measures have facilitated the establishment of unified national monitoring platforms for data export security and improved the traceability of cross-border transfers.

Localisation imposes practical constraints on business operations. Multinational corporations and digital platforms must build separate domestic data centres, duplicate storage systems, and conduct pre-transfer reviews, elevating transaction costs and prolonging project schedules. In industries such as finance, transportation, and cloud computing, these requirements disrupt the integration of global workflows and limit the efficiency of data-driven services. For small and medium-sized enterprises (SMEs), excessive compliance obligations may hinder participation in cross-border activities, thus leading to fragmented digital markets. Nonetheless, localisation has produced measurable gains in risk control. A 2022 report by the China Academy of Information and

Communications Technology (CAICT) found that centralised domestic storage reduced average incident response times for major cybersecurity breaches by nearly 35% compared to pre-localisation levels. Similarly, the Banking and Insurance Data Governance Pilot Program has shown that localised storage improves the ability of regulators to trace financial data breaches and prevent cross-border fraud. At the same time, the security gains from localisation remain limited beyond critical infrastructure sectors. Data security depends more on effective technical and organisational safeguards, such as encryption, anonymisation, and access controls, than on the geographic location of data storage. Even when data is stored domestically, leaks and cyberattacks continue to occur. Given the ongoing and decentralised nature of global data flows, simply restricting data within national borders cannot fully prevent leakage or misuse. The European Union (EU) has similarly acknowledged that localisation does not, by itself, guarantee data protection or cybersecurity resilience. Finally, the long-term economic and systemic costs of localisation cannot be ignored. Overly strict restrictions on outbound data flows may impede China's integration into global value chains and digital trade networks. In the absence of interoperable mechanisms, such as mutual recognition of adequacy decisions or trusted transfer channels, enterprises face dual compliance obligations and heightened administrative risks. According to an OECD simulation study, full localisation could reduce cross-border digital service trade by 5 - 7% annually. In the long term, research and development and high-value-added processing may shift overseas, weakening domestic innovation capacity and reducing the competitiveness of cross-border digital commerce.

2.3 Fragmented Governance and Regulatory Uncertainty

Fragmented responsibilities and unclear regulatory standards characterize China's cross-border data governance system. These conditions increase compliance uncertainty for enterprises and affect the country's ability to coordinate international cooperation. Although data laws have become more comprehensive, the absence of a unified regulatory framework leads to overlapping departmental responsibilities, repeated procedures, and inconsistent interpretations across agencies, complicating enterprises' cross-border data management.

The dispersion of regulatory authority increases compliance complexity. Under Article 8(2) of the Cybersecurity Law, the Cyberspace Administration of China (CAC) coordinates cybersecurity governance, while the Ministry of Industry and Information Technology (MIIT), the People's Bank of China, and other sectoral regulators oversee activities within their respective domains [8]. While aimed at ensuring broad coverage, this multi-agency model results in fragmented enforcement. For example, the transmission of financial data is overseen by multiple regulatory authorities, resulting in inconsistent review practices and extended approval processes. This dispersion not only weakens accountability but also raises the risk of regulatory conflicts. Multiple reports from the Organisation for Economic Co-operation and Development (OECD) and the United Nations Conference on Trade and Development (UNCTAD) have highlighted the issue of fragmented data governance [11,12]. At the same time, China has taken steps to improve coordination and reduce administrative overlap. Since 2022, the CAC

has launched the National Data Security Coordination Working Mechanism, which integrates 20 ministries and provincial departments to standardise enforcement procedures and share risk information across agencies. Pilot cooperation frameworks between the MIIT and the People's Bank of China in the financial technology sector have also demonstrated improved efficiency in cross-departmental supervision, reducing average data review times by 25%. Unclear and frequently changing regulatory standards add to uncertainty [13]. The Data Security Law sets out a national coordination mechanism under the Central National Security Commission, yet operational rules lack clarity and show variation across provinces and industries. The guidance documents, such as the Measures for Security Assessment of Cross-Border Data Transfers (2022), provide only general principles, leaving enterprises to determine the boundaries of "important data" or "sensitive information" on a case-by-case basis. Even so, the rollout of provincial data compliance guidelines, notably in Shanghai and Guangdong, has provided more concrete procedural standards for enterprises, including pre-assessment templates and model compliance checklists. The lack of detailed and stable standards reduces predictability and, to some extent, limits foreign investment, thus reflecting a broader issue of legal uncertainty in China's digital regulatory environment. In addition, China's fragmented regulatory structure influences its ability to coordinate internationally, with overlapping agency responsibilities complicating the establishment of interoperable mechanisms with other jurisdictions. However, emerging cooperative mechanisms illustrate gradual improvement. The CAC has initiated formal dialogue with the ASEAN Digital Ministers' Meeting (ADGMIN) on cross-border data governance and mutual recognition of security assessment standards, signalling China's intent to participate in regional rule-making. In contrast to the EU and Japan, China lacks a central agency for cross-border data agreements [14]. This adds complexity to participation in global governance initiatives, such as the OECD's Data Free Flow with Trust (DFFT) or the Asia-Pacific Economic Cooperation (APEC) Cross-Border Privacy Rules [15]. Nevertheless, the establishment of inter-ministerial and regional coordination pilots indicates a progressive institutional evolution toward a more integrated governance model, balancing central oversight with sectoral autonomy. Consequently, Chinese enterprises must comply with domestic data localisation rules while also meeting external data transfer requirements, which increases transaction costs and compliance obligations for cross-border trade.

3 Legal Responses to Risks in Cross-Border Data Flows

Based on the preceding risk analysis, this chapter examines the legal and institutional measures addressing compliance challenges for Chinese enterprises in cross-border data transfers. The focus of reform is on establishing a governance framework that accounts for security, economic openness, and international interoperability.

3.1 Clarifying Legal Objects and Adjusting Data Localisation Policy

Ambiguous definitions of personal information and important data, combined with rigid domestic storage requirements, create widespread compliance uncertainty. Under the PIPL, nearly all forms of digital data may fall within the legal perimeter, generating operational and regulatory pressures for enterprises across sectors. However, narrowing statutory definitions would address only part of the problem [16]. By adopting a risk-based approach that adjusts compliance duties based on data sensitivity and potential impact, organisations can better align obligations with actual risk [6,17]. This approach, supported by OECD and APEC privacy frameworks, allows regulatory intensity to correspond to the nature of the data, ensuring proportionality between compliance requirements and potential harm.

Mandatory domestic storage has demonstrated limited effectiveness in strengthening security. It increases operational costs and slows the efficiency of digital trade. At the same time, reciprocal restrictions in other jurisdictions constrain lawful cross-border data flows, and enterprises operating across multiple regions often face overlapping compliance requirements, which may restrict their role in global digital markets [18]. The growing extraterritorial reach of data regimes in the U.S. and EU further amplifies these challenges. The establishment of a dedicated Cross-Border Data Transfer Law could address these issues by specifying the jurisdictional reach of domestic regulations, defining conditions for outbound transfers, and implementing transparent, standardised risk-assessment protocols. Such a framework would reduce ambiguity in compliance obligations, improve operational predictability, and facilitate lawful, efficient exchanges of information across borders. By linking regulatory intensity to data sensitivity and providing clear procedural guidance, China could balance security, economic openness, and international interoperability, while reducing unnecessary burdens on enterprises.

3.2 Streamlining Institutional Design and Clarifying Responsibilities

Fragmented authority continues to challenge coherent data governance in China. Multiple agencies, including the Cyberspace Administration of China (CAC), the Ministry of Industry and Information Technology (MIIT), and sectoral regulators, share overlapping mandates. This overlap can result in inconsistent enforcement, repeated approvals, and higher compliance costs for enterprises.

In practice, enterprises operating across multiple sectors often face conflicting guidance on data classification, reporting, and cross-border transfer rules, thus highlighting the operational impact of fragmented authority. This underscores the importance of both independence and coordination in international experience. For instance, the EU GDPR associates the effectiveness of cross-border adequacy decisions with the presence of independent supervisory authorities (Article 45), thereby ensuring consistent and impartial enforcement [19]. Similarly, the APEC Cross-Border Privacy Rules (CBPR) framework relies on recognised enforcement authorities to maintain interoperability among participating economies [20,21]. These models reveal that centralised coordination, coupled with institutional independence, enhances predictability and trust

in cross-border data governance. Building on these examples, China could consider the establishment of a national data governance authority to consolidate rulemaking, supervision, and international coordination functions. Such an authority could operate under the Central National Security Commission (CNSC) while maintaining professional independence. Responsibilities would include coordinating between central and local regulators, harmonising sectoral rules, and representing China in international data governance initiatives. By consolidating authority, clarifying responsibilities, and providing consistent guidance, this model could reduce administrative overlap, improve domestic coordination, and increase the credibility and efficiency of cross-border data flows.

3.3 Enhancing International Cooperation and Avoiding Data Fragmentation

The fragmentation of global data governance, combined with isolationist policies, can impede both innovation and trade efficiency. While concerns over data sovereignty are legitimate, excessive restrictions tend to limit mutual trust between jurisdictions. Incompatible rules have arisen due to divergent regulatory regimes, like the EU's General Data Protection Regulation (GDPR) adequacy framework, the United States' Clarifying Lawful Overseas Use of Data (CLOUD) Act, and India's data localisation mandates. This patchwork increases transaction costs, complicates compliance, and restricts lawful cross-border data flows [22]. Therefore, China could prioritise interoperability and international cooperation to address these challenges.

Participation in multilateral initiatives, including the OECD's Data Free Flow with Trust (DFFT) and the APEC Cross-Border Privacy Rules (CBPR) system, would enable China to influence global norms while maintaining sovereignty. At the domestic level, boosting certification and assessment systems to accept foreign safeguards could cut duplicate compliance rules for firms. Bilateral or regional agreements on data transfer and privacy protection would further strengthen trust and facilitate digital trade. Effective cooperative regulation depends on risk-based assessment, clear institutional roles, and mechanisms to ensure global interoperability. This approach would allow China to safeguard data sovereignty, support lawful cross-border flows, and cut the operational and compliance burdens caused by fragmented international rules. Eventually, it could also enhance China's role in shaping global digital governance standards while maintaining participation in the global digital economy.

4 Conclusion

This study analysed the main legal and institutional risks in China's cross-border data governance and proposed corresponding reform pathways. It found that ambiguous definitions of legal objects, excessive data localisation, and fragmented regulatory authority together impose major compliance burdens and hinder international cooperation. Accordingly, the paper suggests adopting risk-based, proportionate compliance duties, establishing a unified and independent regulatory coordination mechanism, and deepening China's participation in international governance frameworks such as the

OECD's Data Free Flow with Trust and APEC's CBPR system. Nevertheless, this study has several limitations. Its findings rely mainly on normative and qualitative analysis of legislative and policy materials, rather than on empirical data. Future studies could include quantitative assessment of compliance costs, case-based comparative research, and empirical evaluation of cross-border data practices among firms. Furthermore, as global data regulation evolves, longitudinal research will be needed to examine how China's domestic reforms interact with international developments. Despite these limitations, the analysis offers a conceptual foundation for understanding structural tensions in China's data governance and points to future reforms aimed at ensuring both national security and global interoperability.

References

1. Greenleaf., G ., & Reid., A. (2022). Geopolitical fragmentation, the AI race, and global data flows: the new reality. https://fpf.org/blog/geopolitical-fragmentation-the-ai-race-and-global-data-flows-the-new-reality/
2. Haelterman, H. (2022). Breaking silos of legal and regulatory risks to outperform traditional compliance approaches. European Journal on Criminal Policy and Research, 28(1), 19-36. https://doi.org/10.1007/s10610-020-09468-x
3. The National People's Congress of People.s Republic of China. (2021). Data Security Law of the People's Republic of China. http://www.npc.gov.cn/english-npc/c2759/c23934/202112/t20211209_385109.html.
4. Xu, C. (2021). From Personal Data to National Data: The Escalation of Data Security Issues on Internet Platforms. News Tribune, 35(05), 10-12. https://doi.org/10.19425/j.cnki.cn15-1019/g2.2021.05.004.
5. Li, L. (2022). Compliance Research on Cross-Border Data Flow of Chinese Enterprises [M]. Hebei University. https://doi.org/10.27103/d.cnki.ghebu.2022.002357.
6. 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. https://doi.org/10.1080/17579961.2018.1452176
7. Lynskey, O. (2023). Complete and effective data protection. Current Legal Problems, 76(1), 297-344. https://doi.org/10.1093/clp/cuad009
8. DigiChina. (2017). Cybersecurity Law of the People's Republic of China (Effective June 1, 2017). https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/
9. Sohu.com. (2016). Cybersecurity Law Passed with High Votes: Websites Violating Privacy May Be Shut Down. https://www.sohu.com/a/118380052_115401
10. Chen, B., & Yang, L. (2022). Research on International Cooperation Mechanisms for Data Security Governance in the Overseas Expansion of Digital Enterprises. Journal of Liaoning Normal University (Social Sciences Edition), 45(05), 50-58. https://doi.org/10.16216/j.cnki.lsxbwk.202205050.
11. Organisation for Economic Co-operation and Development. (2019). Enhancing Access to and Sharing of Data: Reconciling Risks and Benefits for Data Re-use Across Societies. https://www.oecd.org/en/publications/enhancing-access-to-and-sharing-of-data_276aaca8-en.html
12. UNCTAD (2024). Digital Economy Report 2024: Shaping an environmentally sustainable and inclusive digital future. https://unctad.org/publication/digital-economy-report-2024

13. Khasanova, L., & Tai, K. (2024). Shades of authoritarian digital sovereignty: divergences in Russian and Chinese data localisation regimes. Journal of Cyber Policy, 9(1), 70-94. https://doi.org/10.1080/23738871.2024.2413938
14. Xu, W., Wang, S., & Zuo, X. (2025). Whose victory? A perspective on shifts in US-China cross-border data flow rules in the AI era. The Pacific Review, 1-27. https://doi.org/10.1080/09512748.2025.2462239
15. OECD. (2025). Recommendation of the Council on Enhancing Access to and Sharing of Data. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0463
16. Koops, B. J. (2014). The trouble with European data protection law. International data privacy law, 4(4), 250-261. https://doi.org/10.1093/idpl/ipu023
17. OECD. (2023). Data Governance in the Digital Age: Towards Risk-Proportionate Regulation. https://www.unesco.org/en/data-governance-digital-age
18. Wang, Z. (2024). Fundamental Challenges, Divergent Paths and Prospects in Constructing Global Digital Economy Rules. Contemporary World, 2024(04), 23-29. https://jsdd.chinajournal.net.cn/WKH3/WebPublication/paperDigest.aspx?paperID=b75cca9c-b96c-41d4-b44f-71d905bada39#
19. Xu, D. (2020). Legal Safeguards for Enterprises' Two-Way Compliance in Cross-Border Data Flow Regulation. Eastern Law Journal, 185. https://doi.org/10.19404/j.cnki.dffx.20200220.006.
20. Global CBPR Forum. (2023). Cross-Border Privacy Rules (CBPR)Framework (2023). https://www.globalcbpr.org/documents/#elementor-toc__heading-anchor-2.
21. Li, W., & He, W. (2021). Research on the Promotion of Cross-Border Personal Information System Opening in the Pilot Free Trade Zone. International Trade 32. https://doi.org/10.14114/j.cnki.itrade.2021.08.004.
22. Mao, W., & Liu, Y. (2020). Data Nationalism: Rationales and Policy Implications. Global Review, 12(03), 20-42+15. https://doi.org/10.13851/j.cnki.gjzw.202003002.