Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33841

Analysis of China's Legal Regulation of Cross-Border Data Flow in Comparison with General Data Protection Regulation

Yuqing Tang

Law College, Nankai University, Tianjin, China
2310264@mail.nankai.edu.cn

Abstract. In the era of digital economy, data has become the core carrier of global digital trade and industrial development, and its cross-border flow has become a key regulatory target. Using the General Data Protection Regulation (GDPR) as a frame of reference, this paper employs comparative research and normative analysis to systematically compare the paths, logics, and practical differences in cross-border data flow regulations between China and Europe. The study reveals five core issues in China's cross-border data flow regulations: a singular regulatory path, separate compliance and certification systems, imperfect extraterritorial application rules, inadequate international compliance capabilities of enterprises, and a lack of mutual recognition of international rules. Based on the development of China's digital economy and data security needs, this article draws on the reasonable core of GDPR, proposes an optimization path to improve the legislative system, integrate compliance mechanisms, strengthen enterprise adaptation, and promote international cooperation. The aim is to balance cross-border data security and circulation efficiency, enhance China's data governance capabilities, and provide theoretical support for the safe expansion of China's digital economy overseas.

Keywords: Cross-border data flow, regulatory comparison, data compliance, Brussels effect

1. Introduction

In today's world, economic globalization serves as the grand backdrop, and data, as the new production factor of the present era, has emerged as one of the core driving forces behind global economic development. This inevitably brings about the issue of large-scale cross-border data flows, and different countries have formulated different laws to regulate cross-border data flows. As a pioneer in the field of data security, the European Union has established a relatively comprehensive regulatory framework based on the GDPR. Under the influence of the Brussels Effect, it is now exporting EU data rules globally [1].As a major digital economy country, China has successively introduced the Data Security Law of the People's Republic of China, the Personal Information Protection Law of the People's Republic of China, and the Provisions on Promoting and Regulating Cross-border Data Flow. However, compared with the GDPR, China's relevant laws have certain gaps in terms of the level of regulatory path, the relationship between data compliance and data

DOI: 10.54254/2753-7048/2026.33841

certification, and international rule cooperation [2].This article uses the GDPR as a reference to analyze the deficiencies of China's current legal system for cross-border data flows, and proposes an optimized path based on the experience of the European Union.

2. Literature review

Globally, major economies have introduced laws regulating cross-border data flows. Currently, the most influential ones are the GDPR introduced by the European Union and the Clarifying Lawful Overseas Use of Data Act in the United States (CLOUD Act). Although China boasts a huge digital economy market, it lacks a relatively comprehensive data legal system. In terms of its position in the global digital economy, China currently does not hold such a dominant position as the United States. Therefore, referring to the EU's system is more feasible for China. As of today, the GDPR is approaching its 10th anniversary. Despite ongoing calls for improvements to certain provisions, it has become a consensus in academia that any such improvements must not compromise the fundamental rights protected by the GDPR [3]. It can be seen that the comprehensive legal regulation system for cross-border data flow established by GDPR is unanimously recognized by the theoretical community, and its application in the EU over the past 10 years is sufficient proof that it has also gained unanimous recognition in practice. This article combines the views of many scholars and presents my own opinions, thereby conducting research from the perspective of improving China's legal system regulation for cross-border data flow based on the premise of comparing with GDPR.

3. Core issues of regulation on cross-border data flow in China

Compared to the mature regulatory system of GDPR, China's regulation of cross-border data flow faces three core issues, which have become constraints for the digital economy to expand overseas.

Firstly, the regulatory approach is singular, lacking a diverse and flexible adaptation mechanism.

The GDPR has established a three-tiered path for cross-border data regulation. The first tier, the adequacy decision, is the priority path. The EU has included countries on a whitelist that meet its data protection standards, allowing for free data transfer. Currently, only 12 countries/regions have achieved this status [4]. China has not yet obtained adequacy recognition from the EU, and Chinese enterprises are unable to achieve free data transmission to Europe through the preferred path. Those who have not obtained adequacy recognition can adopt appropriate safeguards at the second level [5]. Including Standard Contractual Clauses (SCC) and Binding Corporate Rules (BCR). The former requires the signing of an EU template contract, with limited binding force, while the latter is only applicable to multinational enterprises with EU institutions. In addition, occasional transfers can be an exception to the first two levels, provided that they meet statutory conditions.

In comparison, China has only clarified three compliance paths, namely data cross-border security assessment, personal information protection certification, and standard contracts, and has not established a system similar to the EU's adequacy determination and appropriate safeguards measures. The overall regulatory approach lacks some room for flexible adjustments. In terms of data flow within multinational enterprises, China lacks a streamlined process like the EU's BCR), forcing companies to repeatedly sign standard contracts, resulting in high compliance costs. For micro, small, and medium-sized enterprises (MSMEs), the existing security assessment process is overly cumbersome, making it fundamentally unsuitable for their small-scale, occasional cross-border data needs. This falls short when compared to the GDPR's tiered regulatory model for different entities [2].

DOI: 10.54254/2753-7048/2026.33841

Secondly, the separation of data compliance and data certification systems leads to a lack of an incentive compatibility mechanism.

The GDPR adopts a certification-compliance integration model, forming a "quasi-governmental dual regulatory framework" [6]. The government does not directly supervise enterprises, but rather supervises intermediary institutions such as certification bodies and industry associations, which in turn supervise enterprises. Intermediary institutions can formulate data compliance rules on their own and issue compliance certifications to qualified enterprises, subject to approval by regulatory authorities. Certification certificates carry high credibility. In judicial practice, even if data risks arise (such as being hacked), enterprises can avoid or reduce penalties as long as they present the certification to prove that their measures are in place. In this way, enterprises do not need to eliminate all data risks, but instead proactively improve their data governance system to gain the business reputation and compliance credibility brought by certification, objectively fulfilling the regulatory requirements for data security and personal information protection, forming a positive cycle of spontaneous compliance, and creating an incentive-compatible mechanism.

In China, data compliance and certification belong to two separate systems, and there is no mutual recognition rule stating that "certification is deemed to be compliance". Enterprises need to complete both compliance construction and certification application simultaneously, and the dual costs lead to insufficient enthusiasm for compliance. At the same time, compliance rules are overly principled, lacking industry specificity, and the supervision of certification institutions is imperfect. The credibility and validity of certification results are difficult to guarantee, and the incentive effect of compliance cannot be fully realized.

Thirdly, there is insufficient cooperation on international rules and a lack of a mutual recognition mechanism for data.

The EU has established an adequacy decision system based on Article 45 of the GDPR, which conducts systematic assessments of the data protection level of third countries or regions, focusing on factors such as their legal safeguards, human rights protection, operation of independent regulatory bodies, and fulfillment of international obligations [3]. Countries or regions that are deemed to have achieved the same level of protection as the EU will be included in the adequacy whitelist, allowing free cross-border flow of personal data between them and the EU without the need for additional safeguards.

China has not yet reached an adequacy decision on data protection with the European Union, and the mutual recognition of rules and collaborative regulatory mechanisms with major digital economies are still imperfect. Cross-border data transfers require compliance procedures to be fulfilled on a case-by-case basis, resulting in extremely high transaction costs.

4. Analysis of the causes behind the regulatory differences in cross-border data flow between China and Europe

Some scholars argue that China and the EU are already de facto "digital empires", representing two distinct regulatory models: the state-driven model and the rights-driven model, respectively. However, there is no global consensus on which model is best suited to building a vibrant and resilient digital economy and society [7]. The disparity between China and the EU in regulating cross-border data flows stems from differences in legislative philosophy and practical foundations, which directly determines that the two regulatory systems are evolving in different directions.

Firstly, from the perspective of legislative philosophy, the EU has always adhered to the concept of the supremacy of personal data rights. Although there is still controversy over whether the right to data protection is an independent fundamental right, it has a strong preventive effect on potential

DOI: 10.54254/2753-7048/2026.33841

data abuse, thereby protecting the underlying fundamental rights such as speech, privacy, and equality. This concept has been deeply rooted in the hearts of people in EU countries [8].

The core of EU legislation lies in safeguarding the rights of data subjects, and it imposes strict control over arbitrary cross-border data transfers. All regulatory designs in GDPR are essentially centered around individual rights, whether it is the adequacy decision or the SCC system, all are premised on "achieving an equivalent level of protection in the EU". In contrast, China adheres to the principle of equal emphasis on data security and development. Legislation prioritizes the protection of national security and public interests, while also considering personal information protection and the development of the digital economy. The entire regulatory system leans more towards data control rather than rights protection, resulting in a slightly conservative institutional design with less flexibility.

From a practical perspective, the EU's data governance system started early and has achieved a high level of maturity. After years of institutional accumulation and practical refinement, it has formed a stable and efficient operating mechanism. The data protection provisions in the GDPR prevent EU enterprises from avoiding risks solely by adjusting relevant contracts. Instead, they must fundamentally re-examine the collection, storage, and processing modes of personal information across the entire enterprise scope [9]. Moreover, EU enterprises generally have a strong compliance awareness, integrating compliance into every aspect of their business. They are also willing to invest in data security technology research and development and system construction, demonstrating solid technical support capabilities. In addition, the EU has a mature and comprehensive system of third-party certification, compliance auditing, and professional regulatory agencies, which can provide standardized services and strong supervision for data governance. The entire governance chain forms a complete closed loop.

Compared with the EU, China's digital economy expands faster in scale and has more rich application scenarios, but the data governance system started late and is still in the stage of continuous improvement as a whole. For example, each member state of the European Union has an independent "regulatory body" as the regulatory body, and the European Commission provides institutional support to form a complete set of GDPR regulatory systems. However, Personal Information Protection Law of the People's Republic of China has only made a principled definition of the authority of China's cyberspace department. Because this law has not been legislated for a long time, and China's cyberspace department has not yet issued sufficient judgment cases and policy guidelines, it is more difficult for relevant subjects to ensure that their data processing and other activities fully meet the legal requirements [10].

At present, the awareness of data compliance of domestic enterprises is generally weak, most of them have not yet established a systematic compliance mechanism, the reserve of data security technology and professionals is obviously insufficient, and the compliance framework suitable for international prevailing rules has not yet been formed. In addition, China's supporting service systems such as data certification, compliance audit and risk assessment have lagged behind, and the service capabilities and standards are not sound enough. This leads to the fact that when enterprises meet the strict regulatory requirements of the EU GDPR, they will always encounter such practical problems as unclear compliance paths, high costs and difficulties in landing, and the capacity for cross-border data compliance is insufficient.

5. Optimization path for regulation of cross-border data flow in China

Based on the previous analysis, the author summarizes the following four optimization paths to improve China's legal system for cross-border data flow, drawing from the three core issues of

DOI: 10.54254/2753-7048/2026.33841

China's regulations on cross-border data flow and the two major causes of differences in regulations between China and the European Union.

5.1. Improving the diversified and hierarchical legislative system

First, an accreditation system for peer-to-peer data protection should be added. Similar assessment criteria can be established in China with reference to the three-level cross-border data regulation path of the European Union, such as giving a white list to countries and regions with relatively sound rule of law, data protection level equivalent to China and independent regulatory agencies, instead of the current one size fits all examination and approval mode, which can improve the efficiency of data cross-border while protecting data security.

The second is the formal introduction of BCR. China should allow multinational enterprises with branches at home and abroad to use unified internal data charters to transfer data within the group after approval by regulatory authorities, so that they do not have to sign standard contracts repeatedly, which can solve the problem of high compliance costs for large enterprises.

Third, refine the applicable boundaries of the existing three types of routes, and clarify the applicable scenarios and processes of exit security assessment, personal information protection certification and standard contracts. The data classification and hierarchical protection system is China's "Regulations on the Administration of Network Data Security (Draft for Comments)" One of the core contents of. According to the impact and importance of data on national security, public interests or the legitimate rights and interests of individuals and organizations, the system divides data into three levels: general data, important data and core data. China should make specific legislation to clarify how to implement differentiated control over the above three-level data, appropriately improve the flexibility of the current rules under the concept of data security priority, and narrow the institutional gap with the hierarchical governance of the EU.

5.2. Integrating data compliance and certification mechanisms to establish an incentive-compatible governance model

Relevant department should draw inspiration from the integrated "certification-compliance" framework and the dual quasi-governmental regulatory structure of the GDPR, aiming to break down the current fragmented situation where compliance and certification are separate entities in China.

Firstly, by legislating clear rules for the connection between certification and compliance, enterprises can be directly presumed to meet the corresponding data export compliance requirements after obtaining officially recognized compliance certification. Regulatory authorities will no longer conduct repeated reviews, reducing institutional costs for enterprises.

Secondly, establish a hierarchical and categorized data authentication system. General data should undergo voluntary authentication, important data should undergo mandatory authentication, and core data should be directly supervised by state authorities, consistent with China's current data security management logic.

Furthermore, relevant departments should strengthen the whole-process supervision of certification bodies and industry organizations, set strict access thresholds, standardize certification procedures, clarify responsibilities for violations, enhance the credibility of third-party institutions, and gradually form a collaborative governance pattern where "the government supervises intermediary institutions, and intermediary institutions oversee enterprises". This will address the

DOI: 10.54254/2753-7048/2026.33841

shortcomings of China's weak practical foundation and insufficient motivation for corporate compliance and promote enterprises to shift from passive compliance to active governance.

5.3. Deepening the alignment and cooperation of international rules, and promoting mutual recognition in bilateral and multilateral contexts

In view of the fact that China has not been included in the EU white list and the mutual recognition of regional rules is insufficient, after revising China's current data regulations with reference to the EU GDPR, China should continue to promote the EU China data protection mutual recognition negotiation, systematically link up with the adequacy determination standards of the GDPR, strengthen communication and cooperation in key areas such as the independence of regulatory agencies and specific law enforcement mechanisms, strive for EU recognition, and fundamentally reduce the cost of cross-border compliance of Chinese enterprises with European data.

5.4. Strengthening the construction of corporate compliance capabilities and consolidating the foundation of governance practices

For the challenges of weak enterprise compliance awareness and insufficient talent and technology reserves caused by the late start of China's digital economy, the author has the following two corresponding suggestions. First of all, China should guide enterprises to establish a compliance system covering data collection, storage, transmission and use in accordance with the requirements of the full life cycle protection of the GDPR, and require enterprises to set up persons in charge of data protection, while using the media to publicize the importance of data compliance. At the same time, people will increase technical investment in encryption, desensitization and access control in major universities and scientific research institutions.

6. Conclusion

This paper, taking GDPR as a reference, systematically compares the institutional design, operational logic, and practical effects of China-EU cross-border data flow regulations. The research indicates that China has initially established a framework for cross-border data regulation, but there are still significant shortcomings in terms of regulatory tools, compliance mechanisms, international mutual recognition, and practical foundations. These shortcomings are mainly reflected in three core issues: a single regulatory path, the separation of compliance and certification systems, and the lack of international rule mutual recognition.

The root cause of regulatory differences between China and the EU lies in the dual differences in legislative philosophy and practical foundation: the EU takes the supremacy of individual data rights as its core, forming a mature market-oriented and collaborative governance system; China adheres to the principle of equal emphasis on security and development, with a prominent government-led characteristic, and the compliance capabilities of enterprises and the supporting service system are not yet perfect. Based on this, this paper proposes four optimization paths: improving the diversified and hierarchical legislative system, introducing quasi-adequacy recognition and binding corporate rules, and filling the shortcomings of regulatory tools; integrating data compliance and certification mechanisms, establishing mutually recognized rules and a hierarchical certification system, and forming an incentive-compatible governance pattern; deepening international cooperation, promoting mutual recognition between China and the EU and the alignment of regional rules,

DOI: 10.54254/2753-7048/2026.33841

breaking down cross-border barriers; strengthening the construction of enterprise compliance capabilities, and filling the shortcomings in technology, talent, and governance practices.

In the future, the improvement of China's regulations on cross-border data flow cannot be a simple imitation of the GDPR, but should, in light of China's own actual situation, find out the part of the institutional model system designed by the European Union that is still valid in the context of China's digital economy, and incorporate this part of the system into China's data legal system by means of legislation. For China, this can ensure the convenience of Chinese enterprises going to sea. For the whole world, a country absorbing the reasonable contents of the legal systems of other countries is also conducive to reducing the economic costs caused by the legal differences between countries in the context of economic globalization, contributing to the further deepening of economic globalization, and thus forming a more perfect international data governance order.

References

[1] Yang, S. (2026) The International Law Implications of the "Brussels Effect" and China's Response. German Studies, 41(1), 94-116+151-152.
[2] Qiao, J. and Wang, C. (2025) Regulatory Pathways for Cross-Border Flow of Personal Data in the EU: Challenges and Responses. Journal of Southwest University of Science and Technology (Philosophy and Social Sciences Edition), 42(5), 37-43.
[3] Kloza, D., Drechsler, L., Fernandes, E., Birth, A., Rossi, J., Dewitte, P., Greser, J., Mustert, L., Malgieri, G. and Bentzen, H.B. (2026) If it ain't broke, don't fix it? Ten improvements for the upcoming tenth anniversary of the General Data Protection Regulation. Computer Law & Security Review: The International Journal of Technology Law and Practice, 60, 106251.
[4] European Commission (2021) Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries. EUR-Lex.
[5] European Parliament & Council of the European Union (2021) Commission Implementing Decision (EU) 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries. EUR-Lex.
[6] Loconto, A. and Busch, L. (2010) Standards, techno-economic networks, and playing fields: performing the global market economy. Review of International Political Economy, 17(3), 507-536.
[7] Bradford, A. (2023) Digital empires: The global battle to regulate technology. Oxford University Press.
[8] Poscher, R. (2017) The right to data protection: A no-right thesis. In R.A. Miller (Ed.), Privacy and power: A transatlantic dialogue in the shadow of the NSA-affair (pp. 129-142). Cambridge University Press.
[9] Labadie, C. and Legner, C. (2023) Building data management capabilities to address data protection regulations: Learnings from EU GDPR. Journal of Information Technology, 38(1), 16-44.
[10] Kam, O.M.T. (2025) A comparative analysis of customer data privacy protection under the European Union's General Data Protection Regulation and the People's Republic of China's Personal Information Protection Law. Beijing Law Review, 16(3), 1721-1741.