Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33424

A Comparative Study on Rules for Protecting Personal Privacy in Cross-Border Data Flow-Taking China, the United States, and Europe as Examples

Yuxiu Liu

School of Political Science and Law, Hubei University of Arts and Science, Xiangyang, China
e89962570@gmail.com

Abstract. In the digital economy era, cross-border data flow emerged as a core driver of global economic development, while also posing profound governance challenges including threats to personal privacy rights and national data sovereignty security. No unified, universally accepted global governance system for cross-border data flows has yet been established. This study systematically clarifies the core differences in the governance models of the European Union (EU), the United States (US), and China: the EU has built a human rights-based, rule-export-oriented system featuring "strictness externally and looseness internally"; the US promotes a market-driven hegemonic framework of "lenient entry and strict exit"; and China coordinates security and development, forming a classified balanced mechanism for "secure flow". This paper analyzes the underlying logic behind these differences, providing a reference for China to improve relevant systems and enhance its voice in global digital governance, while noting that further research expansion is needed in the dimensions of corporate compliance and emerging scenarios.

Keywords: Digital trade, cross-border data flow, data security, privacy protection, multinational comparison.

1. Introduction

With the global spread of the digital economy, data has become a core production factor driving economic growth and social progress. Cross-border personal data flows not only underpin the efficient operation of international trade and investment but also shape technological innovation and business model iteration worldwide. However, this cross-border mobility has also given rise to a series of complex legal and governance dilemmas: personal privacy rights face risks of inadequate protection in transnational digital transmission, and inherent tensions exist between national data sovereignty security and the demand for free global data flow. Around these issues, major global economies have launched fierce rule competition and institutional games, failing to form a unified and universally recognized governance system [1].

The EU, with the General Data Protection Regulation (GDPR) at its core, has established a "strict outside and loose inside" governance model with high-standard rules, embodying a "rule export" orientation that regards personal data rights as fundamental human rights [2]. The US adopts an

© 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: 10.54254/2753-7048/2026.33424

asymmetric "lenient entry and strict exit" strategy: it opposes data localization restrictions on one hand, while strictly controlling the outflow of sensitive data through domestic legislation and expanding its global data access capabilities via "long-arm jurisdiction" on the other [3]. The two sides have evolved from the "Safe Harbor", "Privacy Shield Agreement" to the "Transatlantic Data Privacy Framework (TDPF)", reflecting the fundamental differences in their data protection and national security concepts. China, under the framework of overall development and security planning, has formed a "secure flow" mechanism with security assessment, standard contracts, and protection certification as core paths, exploring a balanced approach to promoting the orderly and lawful cross-border flow of data while upholding the bottom line of national security and individual rights.

There are significant differences in the value basis, regulatory paths, and international strategies among the rules of China, the US, and the EU, which constitute the basic landscape of multi-polar competition and complex games in global cross-border data flow governance. Against this backdrop, this study conducts an in-depth and systematic comparative analysis of personal privacy protection rules in cross-border data flows among the three economies. It aims to reveal the underlying logic and interest considerations behind these differences, examine the advantages and limitations of different models, and provide theoretical and practical references for improving China's cross-border data flow systems, enhancing its voice in international rule-making, and promoting the construction of a more just and reasonable global data governance order.

2. Literature review

This literature review sorts out and compares the conceptual models of personal privacy protection rules in cross-border data flows among China, the US, and the EU, exploring the similarities, differences, and development trends of different regulatory paths, as well as their impacts on the global data governance pattern.

Existing scholars have summarized the global mainstream regulatory concepts of cross-border data flow into three typical paradigms through the "three-point method" from the perspective of regulatory concepts and models. For the EU paradigm, scholars widely agree that it emphasizes personal data rights as a fundamental human right and constructs a "strict external and loose internal" regulatory system with the GDPR as the core. Its cornerstone is the "adequacy decision" system, which ensures that data recipients provide a "substantially equivalent" level of protection to that of the EU. This system embodies the "Brussels Effect", meaning the globalization of its high-standard rules through market power.

Regarding the US paradigm, existing research points out that the US has traditionally advocated free data flow and opposed localization requirements to maintain the global competitiveness of its digital industry. Its regulation is characterized by industrialization and decentralization, with a lack of unified federal-level privacy legislation. In recent years, its strategic focus has shifted to "precise containment" and "limited free flow": it imposes strict restrictions in key areas related to national security, while expanding "long-arm jurisdiction" through the Cloud Act to access overseas data and maintain its "digital hegemony".

For the China paradigm, early studies noted that its rules emphasized national security and data sovereignty with strict scrutiny of data outbound transfers. However, the latest research indicates that China's regulatory concept is evolving towards "data development", that is, promoting the orderly and free flow of data in accordance with the law on the premise of safeguarding national security and personal information security. The promulgation of the Regulations on Promoting and

DOI: 10.54254/2753-7048/2026.33424

Regulating Cross-Border Flow of Data in 2024 is widely regarded as a milestone in deregulation and balancing security and development.

In summary, existing literature has clearly depicted the "tripod" pattern of cross-border data flow regulation in China, the US, and the EU. On this basis, this study conducts a systematic comparative analysis of personal privacy protection rules under cross-border data flow scenarios among the three economies, adopting multi-level and multi-dimensional research methods including comparative analysis, literature research, and case analysis to ensure comprehensiveness, profundity, and practicality of the research.

3. Comparative analysis of major global governance models for cross-border data flows

3.1. American model

The core logic of US cross-border data flow governance has always been centered on maintaining the competitive advantages of its domestic digital industry and global digital hegemony, with its core position shifting from early absolute "free data flow" to an asymmetric governance framework of "lenient entry and strict exit" [4].

In the early stage, relying on the first-mover advantage of its digital industry, the US took barrier-free free data flow as its core proposition, opposed data localization requirements, and removed institutional obstacles for domestic tech giants to expand into the global market [5]. With the intensification of global digital competition and geopolitical changes, its position has undergone a fundamental shift: "lenient entry" refers to building an exclusive flow mechanism with its core allies to absorb global high-quality data elements; "strict exit" means strictly controlling the flow of sensitive data to non-allied countries through administrative orders and legislation, with national security and geopolitical competition as the core yardstick.

At the domestic institutional level, the US has not issued unified federal privacy legislation, forming a fragmented governance pattern of industry-specific and state-level legislation. This model not only reserves flexible operating space for domestic enterprises but also provides leverage for its international rule-making games. At the extraterritorial control level, the US delineates control lists through presidential executive orders, sets high penalties to strictly restrict the outbound transfer of sensitive data, and breaks through traditional territorial jurisdiction restrictions via the Cloud Act to build a global data retrieval and long-arm jurisdiction system, forming an asymmetric data access advantage. Meanwhile, it has built an alliance data cooperation mechanism through the TDPF with the EU, though the long-term stability of the framework remains in doubt due to the underlying differences in governance concepts between the two sides. On the whole, the core of the US model lies in the asymmetric rule design with double standards, making global data flow rules always serve its domestic industrial interests and geostrategic goals through loosening internal constraints, setting external restrictions, and expanding global jurisdiction.

3.2. EU model

The EU's cross-border data flow governance, with the GDPR as its core, elevates personal data protection to the level of fundamental human rights, builds a "strict outside and loose inside" governance system, and forms a human rights-oriented global governance paradigm prioritizing rules, which is essentially different from the US hegemonic model [6].

Internally, the EU has established unified high-standard rules through the GDPR, which greatly eliminates barriers to data flow in the internal market, realizes free and barrier-free data circulation

DOI: 10.54254/2753-7048/2026.33424

in the single market, and balances privacy protection and the scale effect of the digital market through unified rules. Externally, the EU takes the "substantially equivalent" protection level as the core criterion, sets strict access thresholds for data transmission to third countries, builds a multi-level compliance transmission mechanism with adequacy identification as the core, supplemented by standard contract clauses (SCCs) and binding corporate rules (BCRs), and expands the compliance alliance covered by its rules through continuous country adequacy assessments [7].

Relying on the huge volume of its single market, the EU has achieved global spillover of its rules through the "Brussels Effect", forcing multinational enterprises to adapt to GDPR standards in their global operations, with personal information legislation in many countries modeled on it. Meanwhile, the EU continues to refine regulatory guidelines, clarify enterprises' compliance obligations in response to overseas data retrieval, hedge against the impact of extraterritorial long-arm jurisdiction, and consolidate regulatory resilience. At present, the "simplification" reform agenda of the GDPR within the EU may weaken the rigidity of the rules and the global influence of the "Brussels Effect", bringing uncertainty to the authority of its regulatory system. On the whole, the EU model takes human rights protection as the bottom line and market access as the core leverage and firmly grasps the discourse power in global cross-border data governance through rule export.

3.3. China's governance model: evolution, current situation, and characteristics

China's cross-border data flow governance is based on data sovereignty, with the core logic of "two-wheel drive of security and development". Its governance concept has evolved from early "control-based governance with security priority" to "balanced governance with equal emphasis on security and development", establishing a characteristic "secure flow" governance system that is different from the US and the EU and adapts to China's national conditions, providing a third paradigm for global digital governance that balances sovereign security and open development.

China has built a top-level legal framework for cross-border data flow, established the core governance principles of hierarchical classification and risk control, and constructed three legal outbound transfer paths that accurately match risk levels, with the Cybersecurity Law, Data Security Law, and Personal Information Protection Law as the three core pillars. For high-risk outbound scenarios, it implements strict control through security assessment; for conventional business scenarios, it lowers the compliance threshold through standard contracts and protection certification. In recent years, supporting regulations and industry guidelines have been successively implemented, and the negative list pilot programs in free trade zones (FTZs) have been continuously promoted, achieving a dynamic balance between the security bottom line and flow convenience.

China has not adopted a "one-size-fits-all" model of comprehensive data localization requirements and only implements precise control over high-risk subjects through hierarchical classification, minimizing interference in normal business activities. Adhering to the concept of openness and inclusiveness, China takes multilateral and regional cooperation as the core in foreign cooperation, actively participates in the formulation of RCEP rules, promotes regional institutional innovation, and actively aligns with high-standard digital economic and trade agreements such as DEPA and CPTPP, showing a positive attitude of in-depth participation in global digital governance [8].

The core differences among the three models are rooted in multiple dimensions: at the conceptual level, the EU adheres to a rights-based standard, the US pursues a market-based standard, and China upholds the overall consideration of security and development; at the economic level, the US has the world's leading tech enterprises, the EU lacks local industry giants and makes up for industrial

DOI: 10.54254/2753-7048/2026.33424

shortcomings through rule-making, while China has the world's second-largest digital economy and needs to achieve a dynamic balance between security and development; historically, the EU has a profound tradition of fundamental rights protection, the US is highly dependent on market mechanisms, and China, as a catch-up economy, has always attached great importance to national security [9]. The core contradiction of global data governance lies in the inherent conflict between the globalization of data flow and the regionalization of regulatory sovereignty, with cross-border data flow rules becoming a core strategic tool for countries to safeguard digital sovereignty and participate in international competition.

4. Developing a future-oriented data cross-border flow framework with Chinese characteristics

4.1. Direction of domestic system improvement

China should further sublimate the core idea of cross-border data flow governance into "data security sovereignty" on the basis of "overall planning of security and development". This conceptual framework contains two core connotations: internally, the state enjoys sovereign jurisdiction and regulatory power over domestic data activities; externally, the state participates in the formulation of global data governance rules as an equal subject and safeguards its own data interests [10].

The concept of "data security sovereignty" helps China respond to the EU's concerns about "digital sovereignty" in international dialogues, while carrying out constructive exchanges with the US on the free flow of data. Although there are significant value differences among China, the US, and the EU, there is overlapping consensus on bottom-line issues such as "ensuring that cross-border data flows do not harm national security", "basic protection of personal information", and "data flows based on legitimate purposes". Based on the concept of "data security sovereignty", China should actively explore and promote the institutionalization of these overlapping consensuses and participate in building a more balanced and inclusive global data governance order on the premise of safeguarding its own data sovereignty.

4.2. International rule alignment and discourse power enhancement

First, China should actively align with mainstream international rules and enhance the interoperability of its system. At the regional level, relying on multilateral frameworks such as its formal applications to join DEPA and CPTPP, China should put forward a Chinese version of cross-border data flow rules, advocate the principle of "hierarchical classification", set differentiated flow conditions according to data sensitivity, processing purposes, and the security capacity of recipients, and participate in the design of international common legal tools such as standard contract terms to enhance the international compatibility of Chinese rules. At the bilateral level, China should explore the establishment of a dialogue mechanism for adequacy or equivalence identification with the EU, and gradually build a mutually recognized data protection level determination mechanism through system improvement and peer-to-peer dialogue, while learning from the experience of the US-EU DPF framework to explore a Chinese-style "safe harbor" cooperation mechanism on the basis of mutually recognized data protection standards.

Second, China should actively participate in the formulation of global data governance rules to enhance its discourse power. It should shift from a rule-taker to a rule-participant and co-builder, using multilateral platforms such as the UN, WTO, G20, and BRICS, to put forward China's

DOI: 10.54254/2753-7048/2026.33424

proposals on cross-border data flow and personal privacy protection, and promote the construction of a fair, inclusive, and efficient global data governance order based on the principles of hierarchical classification, equivalent mutual recognition, and security and controllability. Meanwhile, it should strengthen cooperation with developing countries and emerging economies, promote the formation of a common position of "Southern countries" on data governance issues, and safeguard the data sovereignty and development interests of developing countries while balancing the rule dominance of developed countries [11].

Third, China should respond to international concerns with an open attitude and enhance the transparency of its rules. The external transparency of China's data governance system is a key prerequisite for international recognition. It should actively introduce the institutional framework, law enforcement practices, and development trends of its cross-border data flow governance to the international community and respond to concerns about data localization and security review. The 2024 Regulations on Promoting and Regulating Cross-Border Flow of Data and the 2025 Measures for the Certification of Personal Information Leaving the Country have released positive signals to the international community. In the future, China should further strengthen dialogue and exchanges with international organizations, foreign governments, multinational enterprises, and academic circles to enhance the international community's understanding and trust in China's data governance policies.

5. Conclusion

This study focuses on personal privacy protection rules in cross-border data flows and conducts a systematic comparative study of China, the US, and the EU. It finds that the three economies have formed differentiated governance models: the EU, based on individual rights, builds a "strict outside and loose inside" system through the GDPR and exports high-standard rules via adequacy identification; the US adheres to a market standard, implements "lenient entry and strict exit" through decentralized legislation and long-arm jurisdiction to maintain digital hegemony; China coordinates security and development, establishes a secure flow mechanism based on the three core upper-level laws, and is evolving towards a "data development" orientation. The differences in value orientation, regulatory tools, and international strategies among the three have created a fragmented and multi-polar game pattern of global data governance.

This study constructs a three-dimensional comparative framework, providing theoretical reference for the improvement of China's cross-border data system and privacy protection, and helping to enhance its voice in international rulemaking. The research is limited to the comparison of macro rules, and does not involve issues such as corporate compliance, technical paths, and emerging scenarios, which can be further expanded in future research to promote the construction of a new global data governance order that takes into account sovereign security, personal rights, and digital development.

References

[1] Wu, J. (2025) Research on the legal regulation of cross-border data flows in the context of the digital economy: start with the "Trilemma Theory". Advances in Social Behavior Research, 16(5), 97-103.

[2] Voss, W.G. (2022) Cross-Border Data Flows, the GDPR, and Data Governance. International Organisations Research Journal, 17(1).

[3] Xu, W., Wang, S. and Zuo, X. (2025) Whose victory? A perspective on shifts in US-China cross-border data flow rules in the AI era. The Pacific Review, 38(6), 963-989.

DOI: 10.54254/2753-7048/2026.33424

[4] Zhang, S. and Sun, J. (2025) Changes in U.S. Policies on Cross-Border Data Flows and China's Responses. Macroeconomic Research, (12), 103-118.
[5] Shen, M., Yu, L. and Zhao, Y. (2026) Institutional Innovation Paths for Governing Cross-Border Data Flows: Theoretical Logic and Regional Practices. Southern Economic Journal, 44(03), 28-42.
[6] Chen, Y. (2026) A Comparative Analysis of Rules and Governance Approaches for Cross-Border Flow of Personal Data between China and Europe. Journal of Shandong Judges Training Institute, 42(01), 169-185.
[7] Guamán, D.S., Rodriguez, D., del Alamo, J.M. and Such, J. (2023) Automated GDPR compliance assessment for cross-border personal data transfers in android applications. Computers & Security, 130.
[8] Du, X. and Liu, A. (2023) Security and Openness: China's Cross-Border Data Flow Scheme. Pacific International Journal, 6(1).
[9] Jin, H. (2025) Exploring Legal Differences and International Harmonization Paths of Cross-Border Data Flows. Journal of Statistics and Economics, 2(4).
[10] Ma, G. and Wu, H. (2025) Cross-border data flow supervision in China's free trade zones: security and compliance rules. Asia Pacific Law Review, 33(2), 231-262.
[11] Zhang, S. and Gao, H. (2025) Bridging the Great Wall: China's Evolving Cross-Border Data Flow Policies and Implications for Global Data Governance. Computer Law & Security Review: The International Journal of Technology Law and Practice, 59, 106208.