Governance Core and Localization Strategies for Cross-Border Data Security: European and American Experience and Chinese Solutions

Tianyi Zheng
Foreign Language Institute Zhejiang Wanli College, Ningbo, Zhejiang, China

Keywords: Cross-Border Data Security, Privacy, Governance.

Abstract: In an era of deepening globalized trade and rapid development of digital technology, the digital economy has become an important part of international trade. Therefore, the purpose of this paper is to select typical countries, such as the United States and Europe, and explore how China can optimize its localized governance strategies for cross-border data security in the new era by studying their governance strategies for cross-border data security. This paper adopts case analysis, comparative research and literature review to explore cross-border data security governance experience. By introducing mechanisms such as "Safe Harbor" and "Privacy Shield", this paper summarizes its experience in data protection and flow. This paper introduces the European Union's Power-Driven and American Market-Driven models and analyzes the differences from the dimensions of data sovereignty, governance logic and legal system, so as to provide reference for improving cross-border data governance in China. KEYWORDS cross-border data security, privacy, governance.

1 INTRODUCTION

During recent years, with the deepening of globalized trade and the vigorous development of digital technology, the digital economy has become an essential aspect of international trade. Technological changes have made the storage and cross-border sharing of data more efficient, significantly improving productivity and economic efficiency, and promoting a new type of trade centered on cross-border data - digital trade. The massive cross-border transmission of data has also caused countries to pay attention to information security. Under the influence of the "Brussels effect", global data governance has gradually evolved into a tripartite pattern dominated by China, the United States and the European Union (EU), with China, the EU and the United States as the three major economies (Xu et.al, 2024). How can China, the United States, and the European Union coordinate their information Safeguarding Rules for various cross-border data, resulting in improved international cooperation while safeguarding their own data security. Today’s scholars generally believe that the core contradiction between European and American cross-border data policies stems from the differences in values and interests, and that in the future, a dynamic balance should be sought between national security, privacy protection and economic interests, and at the same time, the conflict of rules should be reduced through technological innovation and international cooperation. As a latecomer, China must select a governance path that aligns with its own growth requirements, building on the experiences of Europe and the United States. This paper employs a case study approach to examine the implementation of several foreign cross-border data security agreements in Europe and the United States, as well as the compliance risks encountered by Chinese enterprises listed abroad, in order to more comprehensively summarize European and American experiences and clarify China's cross-border data security challenges.

To clarify the core concepts of the multiple cross-border data security governance in Europe and the United States, the Variations between Europe and the United States. between Europe and the United States in terms of data sovereignty, governance logic and legal system are analyzed through the comparative research method; the European and American experience is compared with the Chinese solution, highlighting the strengths and weaknesses of China's localized strategy, drawing on the experience, and optimizing the cross-border data governance solution. Plus, today's scholars' views on the fundamental paradoxes of cross-border data governance in Europe and the United States as well as governance policies

Zheng, T.
Governance Core and Localization Strategies for Cross-Border Data Security-European and American Experience and Chinese Solutions.
DOI: 10.5220/0014382900004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 436-441
ISBN: 978-989-758-785-6

are also different, and the literature review method helps this paper to clarify the different initiatives faced by Europe and the United States at home and abroad, so as to more comprehensively draw on European and American governance experience. Through the above research methods, this paper aims to explore the experience of the European Union and the US in cross-border data protection policies in recent years, and to explore how China can better explore new governance paths suitable for itself in international countermeasures and domestic governance in the new era and better participate in international digital trade.

2 LITERATURE REVIEW

In recent years, there has been tension and coordination between the EU and the US about cross-border data protection policies, some scholars have proposed that the differences between Europe and the US on cross-border data protection policies reveal the differences between the two laws in the rule system and the pursuit of values, the EU focuses on data protection, human rights oriented, and emphasizes the protection of citizens' individual privacy through high-intensity legislative protection; however, the US pushes the freedom of data, is market-driven, and greatly pursuit of commercial interests (Wang & Wang, 2022).Furthermore, other scholars have suggested that one of the primary contradictions bringing to the failure of cross-border data protection policy cooperation within Europe as well as the United States is the disparity in cross-border data protection legal enforcement and remedies across the two countries. The European Union has set up DPAs in each member state to safeguard citizens' information privacy and security, while the U.S. has not yet enacted an information protection department that can be universally applied across the country, and the U.S. Federal Trade Commission (FTC) is in charge of the relevant legal affairs, so that European Union citizens who suffer from infringement of rights in the U.S. are unable to obtain effective remedies (He, 2023).

On the question of how China can better explore its cross-border data protection policy in the new era, some scholars suggest that cyberspace should be transformed from "competing sovereignty" to "interdependent sovereignty" (Lessig, 2009). This means that data sovereignty is something that no country should arbitrarily take or leave for its own selfish desires, so China should vigorously promote the inclusiveness and cooperation of data sovereignty and emphasize the international cooperation of data sovereignty for mutual benefit and win-win situation. Other scholars have pointed out that in light of the actual situation of cross-border data governance in China nowadays, as well as the large amount of demand for cross-border data, it is recommended to promote the inflow of data while strictly guarding against the outflow of important data, and to strike a balance between security and development. While constructing a good cross-border data flow environment and establishing a worldwide trans-data flow hub, it further builds a favorable barrier to prevent the illegal outflow of data to achieve a long-term cross-border data governance program (Jiang, 2024). In addition, Some scholars have also proposed that technological and scientific breakthroughs is one of the several cores of cross-data flow, enhancing digital technology and understanding the technological foundation of the digital economy, while at the precise same duration, increasing the establishment of legal system experts and teams, which is in line with the development needs of today's digital industry, in order to realize the combination of core technology and legal system regulation (Du & Liu,2023).

Based on this, this study argues that by exploring the conflict and coordination between Europe and the United States on cross-border data protection, it can be possible to thoroughly comprehend the underlying differences between both of them, which in turn allows this paper to shed new light on how China can explore a better long-term cross-border data protection strategy and better integrate into international digital trade. In the era of prevalent digital economy, China should emphasize the inclusiveness and cooperation of international cross-border data security and share the dividends of the era with the international community. At the same time, it should take into account the development and protection of its own cross-border data and strengthen expert supervision of cross-border data flows, so as to realize long-term governance of cross-border data protection along with grasp the key issues facing growth in the era of digital economy.

3 STATUS OF CROSS-BORDER DATA SECURITY GOVERNANCE IN VARIOUS COUNTRIES

3.1 Status and Challenges of China's Cross-Border Data Security Governance Landscape

3.1.1 Current Institutional Status of Cross-Border Data Security Governance in China

China's cross-border data security governance structure is based on three laws: the Network Security Law, the Data Security Law, and the Personal Information Protection Law. These rules clearly explain the core requirements and principles of cross-border data transfer within China. China has issued a variety of operational measures to help implement cross-border data flow control. Initially, China has created a rather flawless cross-border data flow mechanism that provides a compliance path for cross-border data flow (Guo & Li, 2025).

In terms of supervision, China has now formed a multi-body, systematized system of coordinated supervision by the national net information department, the national data management department and the national security agency, which has greatly improved supervision and efficiency.

3.1.2 Judicial Practice of Cross-Border Data Security Governance in China

When faced with jurisdictional difficulties, the infringement of cross-border data often faces difficulties in obtaining evidence and jurisdictional difficulties, and in response to this problem, Chinese courts have adopted the principle of territoriality as the primary jurisdiction, supplemented by personal and protective jurisdiction. For example, they assert jurisdiction over data within the territory according to China's Criminal Law, followed by data sovereignty through judicial interpretation. Typical cases, such as the security review of DDT in 2021, when DDT was in the stage of listing in the U.S., its illegal collection of users' photo albums and road data for travel, the existence of data processing activities seriously affecting national security, the judicial authorities to national security reasons, requiring enterprises to cooperate with the localization of data to rectify the situation, highlighting the priority of the protection of the public interest. In terms of international judicial collaboration, China has also improved cross-border data security regulation cooperation through multilateral as well as bilateral agreements.

3.2 Current Situation and Experience of Cross-Border Data Security Governance in Europe and America

3.2.1 Current Status and Theoretical Foundations of Cross-Border Data Security Governance in the EU

The European Union's regulatory system is becoming increasingly sophisticated, and the enforcement of the law is becoming increasingly stringent. In recent years, the EU has strengthened cross-border data security governance through a number of regulations. Centered on the General Data Protection Regulation (GDPR), the jurisdiction covers the entire EU and requires strict protection of user privacy (Yan, 2023). Meanwhile various regulations enacted in recent years have further imposed higher requirements on important industries such as energy and medicine. The EU promotes policy dialogue by organizing symposiums on cross-border data flows with China and other countries, but enforcement is still dominated by unilateral measures. Continuously promoting international cooperation and policy harmonization. The theoretical basis of cross-border data security governance in the EU has become firstly data altruism and data sharing, which is reflected in the EU Data Governance Act, and this vigorously promotes the public sector and data holders to share data in the public interest without compensation, while taking into account data security. Second, the EU prioritizes the protection of individual rights, the GDPR will protect the citizens' right to govern their private information as a basic right, as a foundation for data governance to balance the economy and security, data security as the core of the economy, requiring enterprises to bear the risk and management responsibility, while building trade barriers through high-standard legislation to enhance the power of global discourse. It is because of the EU's strong protection of citizens' privacy rights, the previous Privacy Shield and Safe Harbor agreements signed by Europe and the United States were both due to two appeals filed by Austrian privacy activist Schrems against the U.S.-based Facebook Inc. for allegedly transferring EU user data to the United States (Rubinstein & Margulies, 2022). The underlying reason was that the U.S. surveillance of EU citizens' privacy was too extensive and lacked transparency, falling short of the EU's minimum standards (Rubinstein & Margulies, 2022). Despite the restrictions on U.S. surveillance in the privacy framework of the European Union-U.S. Data Agreement that was later reached between the two sides, the EU still cannot manage to fully constrain the activities of U.S. intelligence agencies.

3.2.2 Current Status and Theoretical Foundations of Cross-Border Data Security Governance in the US

In terms of the legal system, the U.S. builds a governance framework for cross-border data flows through several laws (Jiménez-Gómez, 2021). The Cloud Act, for example, emphasizes that data sovereignty belongs to businesses and that the government only enjoys the power to access data across borders, and also restricts sensitive data from leaving the country in the name of national security. In terms of international cooperation, the U.S. recently adopted the U.S.-U.S. Framework Agreement on Data Privacy with the EU, which builds new rules on data flows, restricts the scope of access to data by intelligence agencies and complies with the principle of necessity and proportionality, and establishes a two-tier relief mechanism and a data protection review court to meet the EU's privacy protection demands. On the other hand, the U.S. tries to promote self-interested data flow rules through multilateral and regional agreements such as the U.S.-Canada-Mexico agreement and excludes developing countries such as China. In terms of industrial practices, the U.S. has been encouraging enterprises to adopt self-regulatory mechanisms such as "Safe Harbor" certification through technological advantages, and adopting mandatory restrictive measures against foreign apps related to national security (e.g., TikTok), reflecting the governance logic of "prioritizing national security". Logic. The United States actively supports the open movement of data as one of the major foundations of cross-border data security governance, arguing that it should be used to strengthen the United States' dominant position in the world's digital economy by emphasizing the financial significance of data, encouraging the inflow of foreign data, and limiting the outflow of sensitive data from the country. At the very same time, the U.S. focuses on prioritizing national security and sovereignty, and uses data security as a tool to maintain its hegemony in the world, for example, empowering the government to access data across borders through the CLOUD Act and restricting the access of foreign firms to critical data on the grounds of national security, as well as advocating for the expansion of jurisdiction extraterritoriality through the U.S. domestic law by resorting to the long arm of jurisdiction (Murthy, 2022). For example, on March 21, 2025, the U.S. placed a Chinese oil refinery in Shandong on the sanctions list through long-arm jurisdiction because of its procurement of crude oil from Iran. Its essence is still to compete for the dominance of international rules, to construct an international rule circle dominated by itself, and to weaken the discourse power of other countries. The United States in cross-border data security regulation mainly relies on enterprise industry self-regulation and self-regulation, reduces government intervention, many large enterprises such as Facebook, Apple, etc. have developed their own internal data protection regulations.

3.2.3 Lessons Learned from Cross-Border Data Governance in Europe and the US

Europe and the United States have accumulated a great deal of experience in cross-border security of data governance, and both sides emphasize the classification and management of data and promote international cooperation and the improvement of regulatory mechanisms. Data classification and management is the foundation, the U.S. will classify data according to its value and adopt different management modes, and the EU has also designated relevant laws and regulations, such as the GDPR, to classify and manage data. Regulatory tools are the fundamental guarantee to ensure cross-border data security. The U.S. implements two regulatory measures during and at the end of the project, focusing on real-time monitoring of market themes and risk prevention, as well as reviewing and evaluating the results of the project; and the EU has set up a diversified rights redress mechanism. Finally, international cooperation is an important data protection tool. The EU's unique adequacy determination method has helped it grow its international impact on data security, whereas the United States has promoted data freedom through various international trade policies and multilateral agreements. The lessons learned in Europe and the United States are helpful models for global cross-border data security governance.

4 LOCALIZED CONSTRUCTION OF CHINA'S SOLUTIONS

4.1 Core Challenges

Chinese enterprises are facing compliance problems. With the huge differences in global governance systems today, enterprises are facing multiple compliance pressures in cross-border transmission, especially in the face of the U.S. Cloud Act's long-armed jurisdiction, through which they are forced to acquire data outside the country, which contradicts with China's principle of data sovereignty. Influenced by geopolitics, some countries led by the United States have passed the Countering Distrust in Foreign Telecommunications Act to restrict Chinese companies, such as TikTok, Huawei data disputes and ZTE and other related equipment and services, on the grounds of data security (Chen, 2022). China's influence in global data rulemaking does not match the strength of its digital economy, and now that China has joined DEPA and CPTPP, which set high standards for cross-border flow of data, data localization, and other rules, the challenge is how China can adjust its domestic regulations and optimize its data situational management system by joining these agreements to counter the U.S.-European-dominated rule system.

4.2 Solutions

In order to improve China's cross-border data security governance, China has actively responded to international data cooperation agreements, and has now joined RCEP, DEPA and other high-standard economic and trade agreements to establish a whitelisting and data mutual recognition framework for data interoperability, and to jointly promote the internationalization of rules for cross-border data flows (Chen, 2024). While joining international agreements, China should seek to innovate and propose international data security cooperation agreements with itself as the main body, and participate in the formulation of international rules, such as the implementation of the Digital Belt and Road under the framework of the Belt and Road, in order to further safeguard the security of cross-border data. At the same time, on the basis of the existing negative list of data outbound, we should strengthen the clarity of the types of data that are restricted and prohibited from going out of the country, simplify the process of approval, help the free flow of data outside the list, and promote enterprise exchanges and cooperation. In the face of compliance difficulties, enterprises are encouraged to build "China-US dual systems" and "China-EU dual systems" to segregate the management of domestic and foreign data and avoid cross-border risks by controlling domestic equipment and teams.

5 CONCLUSION

This paper systematically examines the experiences of Europe and the United States in cross-border data security governance and the implications for China's localization strategy through the case study method, comparative research method and literature review method. This study will first review the existing state and issues of cross-border data security governance in China, which has constructed a relatively perfect data security governance framework but has insufficient discourse power in the current international rule-making system and faces serious corporate compliance dilemmas and geopolitical pressures. Afterwards, the current situation and experience of Europe and the United States in cross-border data security governance are explored, and it is pointed out that the EU concentrates on data protection, safeguards individuals' privacy through GDPR and other high-standard rules, and fosters international collaboration and policy adjustments; while the United States focuses on the free flow of data, emphasizes on economic interests and national security, and builds up a data flow system through the Cloud Act and other laws, and defends its own rights and interests through its long-arm jurisdiction. Both sides in the classification and management of data, international cooperation and regulatory mechanisms provide a good governance model for the world. The article then suggests that China should learn from the lessons of Europe and the United States and explore a new governance strategy that suits its own situation. In conclusion, this article argues that China should enhance its right to speak in international rule-making, promote the inclusiveness and cooperation of data sovereignty, optimize its domestic governance strategy, take into account data security and economic development, and explore its own cross-border data security governance path, so as to better integrate into the international digital trade system and grasp the opportunities for development in the era of digital economy.

REFERENCES

Chen, M. 2024. Developing China's Approaches to Regulate Cross-border Data Transfer: Relaxation and Integration. Computer Law & Security Review 54: 105997.

Chen, S. 2022. Application of US Long-Arm Jurisdiction in Cross-Border Data Flows and China's Response. US-China Law Review 19: 65.

Du, X., & Liu, A. 2023. Security and Openness: China's Cross-Border Data Flow Scheme. Pacific International Journal

Guo, S., & Li, X. 2025. Cross-border Data Flow in China: Shifting from Restriction to Relaxation? Computer Law & Security Review 56: 106079.

He, D. 2023. Regulation of Cross-Border Flow of Personal Data in Europe and the United States: Conflict and Harmonization – An Examination Based on the Case of Safe Harbor and Privacy Shield Invalidated by the Court of Justice of the European Union (CJEU). China-Arab Science and Technology Forum (in Chinese and English) (11): 158-162.

Jiang, S.H. 2024. Research on Data Governance Suggestions Based on Comparing Data Cross-Border Demand between China and the United States. Frontiers of Data and Computing 6(5): 57-65.

Jiménez-Gómez, B.S. 2021. Cross-Border Data Transfers between the EU and the US: A Transatlantic Dispute. Santa Clara Journal of International Law 19: 1.

Lessig, L. 2009. Code 2.0: Law in Cyberspace. Tsinghua University Press, 299-333.

Li, Y. 2023. The Establishment of International Rules for Cross-Border Data Flow under Major Country Competition. Contemporary World (3): 13-17.

Murthy, M.S. 2022. Data Protection Law and Policy in the USA: An Overview. Indian Journal of Law and Legal Research 3.

Rubinstein, I., & Margulies, P. 2022. Risk and Rights in Transatlantic Data Transfers: EU Privacy Law, US Surveillance, and the Search for Common Ground. Connecticut Law Review 54: 391.

Wang, J.Y., & Wang, Z.Y. 2022. The European and American Game of Personal Data Cross-Border Flow Rules and China's Response – Based on the Double Externality Perspective. E-Government (5): 99-111.

Xu, W., Wang, S., & Zuo, X. 2024. Global Data Governance at a Turning Point? Rethinking China-US Cross-Border Data Flow Regulatory Models. Computer Law & Security Review 55: 106061.