Journal of Commercial Law Review
2025, VOL. 9, NO. 3, 27-31
DOI: 10.47297/wspjclrWSP2516-249705.20250903

Legal Conflicts in China-US Cross-border Data Governance - A Case Study of Data Localization Policies and the Game of Extra-territorial Jurisdiction

Jiale Ying

Xiamen University, Xiamen, Fujian, 361005, China

ABSTRACT

With the deepening of the globalization of digital trade, cross-border flow of data has now become one of the core issues in international trade, and the legal conflicts between China and the United States in the field of data governance have become more and more prominent. The Chinese side advocates strengthening data localization requirements with the Data Security Law and the Personal Information Protection Law, upholding the principle of "security first",while the US side relies on the Cloud Act to expand its extraterritorial jurisdiction and advocate the "free flow of data", which creates a double constraint in the rules. This constitutes a certain sense of double constraint within the rules. This conflict is essentially a game of national sovereignty and jurisdiction in the digital age. This game not only plunged multinational enterprises into a double predicament, but also exposed the limitations of traditional international law in the digital domain. In order to solve the problems shown above, this study adopts more than two solution methods, such as the literature research method, the comparative research method, and the case study method, to systematically sort out the manifestations and causes of the legal conflicts of data governance between China and the United States, to analyze the inadequacies of existing studies in various aspects, and finally to propose different reconciliation paths from various aspects. This research aims to provide relevant references for multinational enterprises, thereby promoting the reconstruction of the international law framework and effectively offering theoretical support for the reform of the global data governance system.

KEYWORDS

US-China cross-border data governance; Conflict of laws; Cdata localization policy; Extraterritorial jurisdiction; Data sovereignty

1 Introduction

1.1 Research background

In today's digital economy, the cross-border flow of data as a core production factor has reshaped the global trade landscape. However, the differences between China and the United States in terms of data governance concepts and legal practices have gradually widened: China has established the obligation of local data storage through legislation. Moreover, it is required that critical data be retained domestically to achieve the purpose of safeguarding national security. However, the United States has expanded its jurisdiction globally through the Cloud Act, authorizing relevant law enforcement agencies to retrieve overseas data. This dichotomy has led to the "fragmentation" of legal rules: multinational enterprises need to meet the conflicting requirements of China's "data not to leave the country", while the United States allows "data accessibility", it also faces high costs and legal risks, and the compliance costs and legal risks are also very high. For instance, Microsoft once got embroiled in a serious legal dispute because it refused to submit data on its servers in Ireland to the US government. This kind of conflict not only hinders the development of digital trade, but also reflects the structural contradictions in the global data governance system.

1.2 Research significance

1.2.1 Theoretical significance

Traditional international law is centered on territorial sovereignty, which is difficult to adapt to the characteristics of "intangibility" and "transnationality" of data. By analyzing the conflict of jurisdiction between China and the United States, this paper injects the profound connotation of international law adapted to the digital era so as to promote the transformation of global data governance rules from "territorial-oriented" to "function-oriented" and provide a doctrinal reconstruction of the jurisprudence of sovereignty and jurisdiction in the digital era. In order to promote the transformation of global data governance rules from "territory-oriented" to "function-oriented", and to provide academic support for the reconstruction of sovereignty and jurisdiction in the digital era.

1.2.2 Practical significance

From the enterprise level, the study of this topic can provide enterprises with relevant hierarchical compliance strategies (e. g., classification management of core data and general data) and technical solutions (e. g., application of privacy computing), which can effectively reduce the operational risks of multinational enterprises; from the international

level, it can provide a variety of paths of reference to the multilateral negotiation mechanism and break the barrier of U.S.-U.S.-America sovereignty and jurisdiction with the method of "data sovereignty and equality." At the international level, it can provide various paths for multilateral negotiation mechanisms to break the monopoly of rules dominated by the U.S. and Europe for many years so as to enhance the discourse power of developing countries in global data governance.

2 Literature review

2.1 Current status of domestic and foreign research

2.1.1 Conflict between international rules' docking and China's localization paths

Academics are generally concerned about the fitness conflict between international rules (e.g., RCEP, CPTPP, DEPA) and China's governance model. Wang Shaohui et al. (2025) pointed out that RCEP, CPTPP, and DEPA because of the dominant countries, have difference in the level of digital economy , and in the data classification and grading , as well as cross-border flow of different core issues , such as the existence of obvious differences. And nowadays China's existing governance system and the core issues of the above still exists in different gaps, and we still need to take the FTZ as a testing ground for the program to We still need to use the FTZ as a testing ground to balance openness and security. Kai Zhang and Qiuhui Su (2024) take DEPA as an entry point and emphasise the need for China to differentiate between the criteria of "public policy objectives" when interfacing with international rules, but unfortunately there is no time to propose a concrete path to reconcile the security review of data with the free flow of data.

In international studies, Jiayue Yan (2024) advocates the use of bilateral agreements to improve China's data governance rules but has not yet addressed the compatibility of localized and globalized standards. For example, when China is interfacing with CPTPP, how to balance the data localization requirements with the freedom of cross-border flow is another big problem.

2.1.2 Data sovereignty game and security and openness balance

In today's academic world, most scholars generally believe that the essence of the conflict between China and the United States is the confrontation between "equal data sovereignty" and "long-arm jurisdiction". Zhang Xiaojun (2025) points out that the conflict of data jurisdiction is rooted in the opposition between the legal logic of sovereignty and extraterritorial jurisdiction, in which the principles of traditional international law can hardly achieve the role of reconciliation and therefore need to rely on the global governance system and mechanism, but has not yet put forward a more specific program for the game between China and the United States. Wu, Changhai and Huang, Jingyi (2024) compare the expansiveness of the EU's General Data Protection Regulation (GDPR), suggesting that China should guard against the infiltration of the idea of the "EU standard", and at the same time, can learn from its data intermediary system to effectively balance security and openness.

Lu Lu and Qi Meijuan (2025) propose a framework of "benign government-business interaction" and advocate soft law governance to reconcile security and market-related needs. In practice, the plight of some SMEs that are forced to withdraw from the cross-border market due to the lack of technological capabilities to meet compliance requirements (e. g., privacy computing deployment) has not yet been adequately covered by existing research.

2.2 Research gaps and future directions

Existing research still suffers from three major limitations:

Insufficient rule compatibility and lack of dynamic adaptation tools (e. g., transition clauses) for localization of international rules; lagging technological enablement and no synergistic standards have been formed between technologies such as privacy computing and legal frameworks; and SMEs have been neglected, and SMEs' compliance costs and the discourse of emerging economies have yet to be systematically included in the solution. Therefore, future research still needs to take the US-China conflict as an entry point to build a "system-technology-diplomacy" trinity reconciliation framework.

3 Research methods

This paper adopts a combination of three research methods to ensure that the analysis is systematic and practical: the first is the literature research method. This paper analyzes the legal literature on data governance of the two countries as well as related scholars' theses to clarify the background of the legal conflict between China and the U. S. on data governance, the progress of the existing research and the shortcomings. The second is the case study method, which can

be reflected in the article when enterprises face the contradiction between China's data localization requirements and the US Cloud Act's data access instructions as a case study and analyze the impact of the legal conflict on the practice through the case study method in order to provide a realistic basis for proposing the path of reconciliation.

4 The performance and causes of cross-border data governance legal conflicts between china and the united states

4.1 Core performance of conflict

4.1.1 Confrontation between data localization policy and extraterritorial data access

Article 31 of China's Data Security Law stipulates that "the core data of critical information infrastructure operators shall be stored within the country and shall not be taken out of the country without approval"; the Personal Information Protection Law further details the security assessment requirements for the cross-border provision of personal information, forming a governance model in which "local storage is the principle, and the exception is taken out of the country". The Personal Information Protection Act further details the security assessment requirements for cross-border provision of personal information, forming a governance model in which "local storage is the principle and exit is the exception". The Cloud Act of the United States authorizes relevant federal law enforcement agencies to access data outside the country. As long as the data controller is an American company or there is a "minimum connection" between the data and the American case, it is possible to skillfully bypass the laws of the data storage location and directly request the relevant data. However, this essentially denies the sovereignty of other countries over the localization of their data.

This approach has put the company in a dilemma: complying with China's localization requirements might violate the US data access directives, but cooperating with US law enforcement agencies might conflict with China's national security review system.

4.1.2 Conflicting Jurisprudence of Jurisdictional claims

Based on the principle of "territorial sovereignty", China adheres to exclusive jurisdiction over data within its territory and emphasizes the "territorial jurisdiction priority" in data governance. However, the United States advocates the principles of "effect" and "interest jurisdiction". The United States, on the other hand, based on the "principle of effect" and "jurisdiction of interest", extends its jurisdiction to the whole world, forming the expansion mode of "personal jurisdiction + jurisdiction of interest". For example, the U.S. Federal Court ruled in the Microsoft case that the extraterritorial effect of the Cloud Act applies to data outside the control of U.S. enterprises, directly challenging the sovereignty of the country where the data is located.

4.2 Analysis of the causes of conflict

4.2.1 Differences in the concept of data sovereignty

China believes that data is an extension of national sovereignty and regards data localization as a necessary means to safeguard national security and relevant public interests, which coincidentally reflects the value orientation of "sovereignty over efficiency". The US, on the other hand, views data flow as a core driver of the digital economy and maintains its dominant position in the global digital market by expanding its jurisdiction, and its essence is the practice of the concept of "efficiency over sovereignty".

4.2.2 Path dependency of legal system

China's data governance legal system is mainly centered on "security review" and focuses on the interception of data before its exit or use and the elimination of hidden dangers through administrative supervision, which is closely related to the progressive legislative logic of the Cybersecurity Law and the Data Security Law, while the US relies on the "long-arm jurisdiction" in judicial practice.The United States, relying on the principle of "long-arm jurisdiction" in judicial practice, advocates institutionalizing the application of extraterritorial jurisdiction in domestic law through the Cloud Act, in order to continue their expansion path of "legal hegemony".

4.2.3 The game of global governance discourse

The U. S. and Europe have long dominated the formulation of global data governance rules (e. g., the "long-arm jurisdiction" model of the GDPR), and China, as a digital economy power, needs to safeguard its own interests through the

export of rules, and the essence of the conflict is the change in the discourse of global data governance from unipolar dominance to multi-polar dominance. The nature of the conflict is the inevitable product of the transformation of global data governance discourse from "unipolar dominance" to "multipolar balance".

5 Path to reconcile the conflict of laws

5.1 Institutional level: constructing a docking mechanism for dynamic adaptation of rules

5.1.1 Establishment of a hierarchical and classified list of cross-border data flows

According to and with reference to China's Measures for Security Assessment of Data Exit, data can be classified into three categories, namely, "core data" , "important data" and "general data". "The State strictly restricts the export of core data. The country strictly restricts the exit of core data, and general data simplifies the cross-border process and reduces the ambiguity of the application of rules.

5.1.2 Introduction of transitional provisions

In docking international rules (e.g. DEPA), a transitional period of 3-5 years is set, during which enterprises are allowed to gradually meet the compliance requirements, and SMEs' transition costs are reduced.

5.2 Technical level: promote synergy between technical standards and legal frameworks

5.2.1 Promote the scenario-based application of privacy computing technology

Achieve data "availability and invisibility" through technologies such as federated learning and secure multi-party computing, which not only meets China's localized storage requirements but also provides US law enforcement agencies with a compliant channel for data retrieval.

5.2.2 Establishment of a mutual recognition mechanism for technical certification

China and the United States can jointly formulate technical standards for data encryption and data anonymisation, and exempt enterprises that meet the standards from some of the scrutiny so as to reduce technical barriers.

5.3 Diplomatic level

Strengthening multilateral consultations and regional cooperation.

5.3.1 Promote bilateral data governance dialogue between China and the U.S

Drawing on the experience of the U.S.-EU Data Privacy Framework, establish a judicial coordination mechanism for intergovernmental data access, and clarify the review procedures and remedies for cross-border data requests.

5.3.2 Participate in global rule-making with emerging countries

Based on the BRICS countries and countries along the Belt and Road, promote the incorporation of the principle of "data sovereignty and equality" into the rules of global governance under the framework of the United Nations, so as to strike a balance between the U.S.-European-dominated rule system and the U.S.-European-dominated rule system.

6 Research innovations and shortcomings

The article is partly innovative in terms of research perspective and solutions, focusing on the specificity of the US-China game, breaking through the generalized discussion of "global governance" in existing research, and proposing a targeted "system-technology-diplomacy" reconciliation path. The article also links technical tools (such as privacy computing) with legal rules to form a "technology-enabled compliance" solution, which can effectively make up for the deficiencies of existing research. However, the selection of cases in this article is overly limited and lacks microdata on internal compliance practices, which may affect the relevance of the solutions. In addition, the idea of establishing a multilateral mechanism also needs to rely on the support of the international political environment, and its feasibility remains to be further verified.

7 Conclusion

The legal conflict of cross-border data governance between China and the United States is a concentrated manifestation of the concept of sovereignty, institutional logic , and the game of global discourse in the digital era, the core of which is the confrontation between the two governance modes of "security priority" and "free flow". Although existing research has revealed the mechanism of the conflict, there are deficiencies in the adaptation of rules, technological synergy and protection of small and medium-sized subjects.

The "system-technology-diplomacy" framework proposed in this paper can provide new ideas for the reconciliation of the conflict through the specific paths of hierarchical data flow, mutual recognition of technical standards, and multilateral consultation mechanisms. In the future, it will still be necessary to further combine the empirical data of enterprises and international political dynamics to optimize the feasibility of the solution and to promote the development of the global data governance system in a more inclusive and balanced direction.

References

[1] Zhang Xiaojun. On the Conflict and Coordination of Data Jurisdiction[J]. Politics and Law Series, 2025(01):95-109.

[2] WANG Shaohui, WANG Fanghong, LIU Gang, et al. Comparison of International Rules on Digital Trade and China's Suggestions for Docking - An Analysis Based on RCEP, CPTPP and DEPA[J]. Southwest Finance, 2025(01):39-50.

[3] Lu Lu, Qi Meijuan. Security Governance Regulation of Cross-Border Data Flows[J]. Jianghuai Forum, 2025(01):145-152.

[4] Wu Changhai, Huang Jingyi. The Expansion of the EU Data Governance Model and China's Response[J]. Technology and Law, 2024(06):34-43.

[5] Zhang Kai, Su Qiuhui. Data Exit Governance for Digital Enterprises under DEPA: Clarifying the Public Policy Objective Criterion[C]//Journal of Legal Studies 2024, Vol. 2, 2024:30-37.

[6] Xu W, Wang S, Zuo X. Global data governance at a turning point? Rethinking China-U. S. cross-border data flow regulatory models[J]. Computer Law & Security Review, 2024, 55:106061.

[7] Yan J. Improvement Path for Cross-Border Governance Rules of Personal Data from an International Perspective[J]. International Journal of Frontiers in Sociology, 2024, 6(1).

[8] YikChan C, Jingwu Z. Governing Cross-Border Data Flows: International Trade Agreements and Their Limits[J]. YikChan C, Jingwu Z. Governing Cross-Border Data Flows: International Trade Agreements and Their Limits.