# International Legal Regulation of Cross-Border Data Flows in Digital Trade

Zhuangzhuang Jin
*Civil, Commercial, and Economic Law School, China University of Political Science and Law, Beijing, China*

Keywords: Cross-Border Data Flow, International Regulation and Governance, Data Sovereignty.

Abstract: This paper examines the international legal regulation of cross-border data flows in digital trade, focusing on the fragmented nature of the current global regulatory framework and its core controversies. By analyzing provisions in key free trade agreements (FTAs), the study highlights the role of the "principle + exception" model in reconciling tensions between trade liberalization and data sovereignty. It further explores the governance logic of regional frameworks and their implications for global rules. The research identifies three distinct governance models: the U.S. prioritizes free data flow, the EU emphasizes human rights protection, and China balances security with development. Conflicts among these models complicate international coordination. The paper argues that China should construct a new global digital governance paradigm by refining domestic legislation, aligning with high-standard international rules, and conducting regional innovation experiments.

## 1 INTRODUCTION

The disruptive innovations brought about by current digital technologies are reshaping the global economic and trade system. A new generation of information and communication technologies, underpinned by big data, cloud computing, 5G networks, and artificial intelligence, is sweeping across the world. This has led to the rapid development of a data-centric global digital trade ecosystem. While cross-border data flows serve as the foundation for global digital trade growth, countries around the world currently hold divergent stances on this issue. For instance, the United States advocates for unrestricted cross-border data flows, whereas the European Union maintains reservations about complete freedom in this regard, emphasizing that data should flow under secure conditions and prioritizing data regulation and protection. Within the evolving architecture of multilateral trade governance, novel transnational regulatory frameworks are crystallizing to enable seamless circulation of digital assets across jurisdictions. Contemporary trade pacts increasingly incorporate dedicated digital economy modules that pioneer innovative governance mechanisms for transboundary information exchange paradigm shift redefining the contours of global data governance. This institutional transformation intersects with China's escalating strategic requirements for international data interoperability, positioning the establishment of secure and efficient transnational data transfer protocols as a pivotal institutional challenge in the digital transformation era.

China formally applied to join the CPTPP in September 2021 and applied to join the Digital Economy Partnership Agreement (DEPA) in November 2021. This paper employs comparative research, case studies, and literature review methodologies to focus on the international regulatory framework for cross-border data in digital trade agreements. It analyzes how current international regulations govern cross-border data in digital trade and explores a potential "third way"-a "Chinese approach"-between the U.S.-EU-led "free flow" model and the "sovereign control" path advocated by developing countries.

## 2 REGULATORY FRAMEWORK UNDER INTERNATIONAL AGREEMENTS

With the continuous globalization of digital trade, cross-border data flow has become a key issue in the



Jin, Z.
International Legal Regulation of Cross-Border Data Flows in Digital Trade.
DOI: 10.5220/0014394100004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 619-624
ISBN: 978-989-758-785-6

field of international trade. However, due to conflicting national interests such as data sovereignty among different countries, international legal rules exhibit a characteristic of multi-track parallelism. The current international regulatory framework primarily involves countries embedding their own cross-border data rules into trade agreements, resulting in a "fragmented" landscape of global cross-border data governance. Among different trade agreements, there exist both competitive clauses and a gradual trend toward integration.

## 2.1 The "Principle + Exception" Model in Free Trade Agreements (FTAs)

The World Trade Organization (WTO) currently lacks specialized regulations addressing cross-border data flows. Over the past few decades, Free Trade Agreements (FTAs) have gradually emerged as a key platform for discussing data governance issues. By establishing new rule frameworks for emerging topics in digital trade, FTAs have to some extent alleviated many of the contradictions faced by the WTO's multilateral trading system (Burri, 2017). Currently, FTAs attempt to reconcile the tension between trade liberalization and sovereign regulation through a balanced design of “the free flow of data principle” and “exception clauses”. The varying emphases of different agreements also reflect the strategic intentions of the dominant countries involved.

The U.S.-Korea Free Trade Agreement (KORUS FTA) is the world's first free trade agreement that explicitly incorporates rules on the free flow of data in its e-commerce chapter. In contrast, the CPTPP elevates the language on cross-border data flow rules from the shall endeavor phrasing in KORUS FTA to the legally binding "shall," thereby increasing the mandatory nature of these obligations. Article 14.11 of the CPTPP clearly articulates the obligation of free data flow, prohibiting parties from restricting cross-border data transfers and stipulating that signatory states are obligated to permit transboundary data flows via digital channels, with specific provisions for sensitive personally identifiable data, provided such transmissions align with authorized commercial operations of registered entities. These binding obligations codify prohibitions against data territorialization mandates and other measures that hinder foreign digital services.

CPTPP’s cross-border data provisions also incorporate exceptions to obligations, permitting member states to implement restrictive measures for achieving "legitimate public policy objectives," provided they meet the two conditions of "non-discrimination" and "necessity." It treats "essential security interests" as non-justiciable exceptions, granting contracting parties’ greater autonomy. The innovation is reflected in Article 14.13, which explicitly prohibits data localization requirements through a "negative list" approach while allowing sensitive sectors like finance to retain certain regulatory flexibility. Although CPTPP's soft dispute settlement mechanism limits the enforceability of its rules, compared to other agreements addressing cross-border data disputes, CPTPP has already established relevant provisions that can be submitted to its dispute resolution mechanism.

The USMCA’s digital trade provisions (Chapter 19) establish robust frameworks for enhancing cross-jurisdictional data interoperability, while its counterpart in the CPTPP (Article 14.13.1) affirms the sovereign right of member states to develop localized technical compliance frameworks for critical information technology assets-particularly addressing communication security and sensitive information protection protocols.

In contrast, Article 19.12 of the USMCA explicitly abolishes the exception in the CPTPP that allows parties to impose ‘computing facility localization’ requirements, permitting only central banks to retain data storage requirements for financial regulation. However, the USMCA exhibits prominent characteristics of data hegemony. Article 19.16 imposes restrictions on algorithmic transparency obligations, prohibiting member states from demanding the disclosure of source code or algorithms. This essentially represents the U.S. exporting rules of data hegemony to maintain the competitive advantage of its technology firms. Under such a model, Latin American countries may be forced to relinquish their digital sovereignty and become subordinate to the U.S. data economy.

Chapter 12 of the RCEP core provisions demonstrates an inclusive approach toward the developmental disparities among member states. Article 12.15 requires contracting parties to endeavor to avoid imposing unnecessary restrictions on cross-border data flows, though it does not establish mandatory standards. Meanwhile, in addressing disputes over cross-border data flows under RCEP, the actual resolution proves challenging, as RCEP merely stipulates that disputing parties should engage in consultations to resolve the issue (Lando, 2022). Paragraph 3 of Article 12.14 further expands the scope of security exceptions, permitting unilateral measures based on "essential security interests," with other contracting parties barred from raising objections. RCEP's flexible framework makes it the

first data flow regulation encompassing China, Japan, South Korea, and ASEAN. However, its relatively low common standards have raised concerns about weak enforceability. For instance, Indonesia has reinforced localization requirements through its Personal Data Protection Law, creating potential conflicts with RCEP provisions.

Although the Digital Economy Partnership Agreement shares similarities with the CPTPP in terms of cross-border data flow rules, it adopts a modular architecture that allows countries to selectively join specific modules, thereby reducing the difficulty of rule adoption. Moreover, DEPA actively promotes the establishment of a standardized framework for digital trade technical exchanges and advances the application of standardized API interfaces.

## 2.2 Clashes among Regional and Plurilateral Agreements

Regional governance agreements attempt to strike a balance between data sovereignty and trade liberalization by establishing shared values and mutual recognition mechanisms for rules. However, in their practical implementation, prominent institutional competition conflicts have emerged among different regional agreements.

The EU's General Data Protection Regulation (GDPR) exemplifies a human rights-first approach, requiring non-EU countries to demonstrate "adequate" data protection standards for cross-border transfers. However, GDPR's stringent compliance costs have driven small and medium enterprises (SMEs) out of European markets. The invalidation of the EU-U.S. "Privacy Shield" in the Schrems II case underscored fundamental conflicts between U.S. surveillance laws (e.g., the Foreign Intelligence Surveillance Act) and EU privacy principles. Despite adjustments under the 2023 Privacy Shield 2.0, the 2024 FISA amendments re-expanded U.S. surveillance powers, further destabilizing transatlantic trust.

In the Pacific region, APEC stands as a highly representative regional framework. Its APEC Cross-Border Privacy Rules (CBPR) system achieves mutual recognition of privacy protection through voluntary participation mechanisms, enabling enterprises to reduce compliance costs by obtaining dual certification under both CBPR and GDPR. The CBPR system does not seek to overturn domestic legislation on personal data protection across nations, but rather acknowledges differences in legal systems, social values, and development paths among countries, given their diverse national conditions and the inherent complexity of privacy protection. The CBPR system emphasizes interoperability of data governance mechanisms among nations, aiming to facilitate cross-border data flows while safeguarding privacy rights.

Nevertheless, specific regulatory obligations embedded in these agreements—notably the mandate for participating nations to implement proactive measures minimizing non-essential barriers to cross-border digital transmissions-demonstrate substantive alignment with American data governance paradigms when analyzed through the prism of transnational data exchange objectives.

This is particularly evident in recent years as U.S.-China competition in the digital value chain has intensified. The U.S. being a global leader in digital technology and the digital economy, faces minimal impact on its data sovereignty security from the growth of cross-border data flows worldwide. Leveraging its advantages in digital trade, the U.S. advocates for free and open digital trade internationally, opposing data localization policies. It even enforces long-arm jurisdiction through agreements like USMCA to suppress and exploit the growth of digital trade in other countries, while adopting unequal openness strategies toward nations whose cross-border data flows might threaten its digital hegemony. In September of the same year, the U.S. Department of Commerce announced sweeping restrictions barring domestic enterprises from engaging in commercial interactions with WeChat and TikTok, with additional prohibitions targeting financial infrastructure integration specifically forbidding American businesses from operating payment platforms leveraging WeChat's ecosystem. Subsequently in January 2021, the Trump administration escalated these measures through an executive order outlawing financial engagements with eight Chinese digital payment systems, notably encompassing Alipay and WeChat's financial services arm. When digital enterprises from other countries expand internationally, the U.S. imposes restrictions under the pretext of national security threats. Such practices challenge the CBPR system's goal of secure and efficient free data flows and cast a negative impact on global digital trade.

# 3 RULE CHARACTERISTICS OF MAJOR COUNTRIES AND REGIONS

The United States adopts a model that prioritizes free flow with supplementary exception-based restrictions.

It has consistently advocated for the free flow of data by promoting cross-border data flow agreements it champions, such as the CBPR and USMCA, leveraging its technological advantages to maximize benefits during the rapid development of the global digital economy. However, the cross-border data free flow promoted by the U.S. is not entirely liberalized; in practice, it employs diverse exception clauses and restrictive measures like negative lists. For instance, Chapter 19 Digital Trade of the USMCA establishes horizontal exceptions and negative list annexes for cross-border data flow. By leveraging its domestic technological edge in the international digital market, the U.S. secures a dominant position, extracting profits from developing countries through cross-border data flows. It also exploits its technological superiority to penetrate developing markets, disrupting local industries and reinforcing its monopolistic dominance (U.S. Department of Commerce, 2025). Additionally, the U.S. imposes stringent controls on the export of core technologies in the digital economy supply chain and on foreign acquisitions of domestic internet companies. The discrepancy between its international advocacy and domestic policies reflects a degree of double standards (Xia & Zhang, 2024).

The EU model demonstrates characteristics of prioritizing human rights protection, with both internal safeguards and extraterritorial jurisdiction. The EU places significant emphasis on human rights protection, which is linked to Europe's tradition in this regard. The foundational framework for European human rights protections traces its origins to 1953, when the intergovernmental organization enacted its seminal human rights charter-formally titled the Convention for Safeguarding Fundamental Liberties and Human Dignity-now universally acknowledged as the ECHR. Article 8 of this convention stipulates the right to respect for private and family life. The EU actively employs legislative measures, such as the 1995 EU Data Protection Directive, to establish standards within the Union that prohibit member states from restricting the free flow of personal data within the EU on grounds of data protection, thereby reducing the costs of intra-EU data transfers. However, for transfers of personal data to regions outside the EU, the EU imposes restrictions, requiring non-EU governments to provide adequate data protection before allowing their operations within the EU. This adequacy protection measure, in practice, creates barriers to cross-border data flows, hindering the development of digital trade and, to some extent, constraining the full growth of the digital economy.

The China model emphasizes digital sovereignty while balancing security and development. In 2016, China clarified its data localization measures of local storage and outbound assessment for cross-border data flows through Article 37 of the Cybersecurity Law, highlighting data sovereignty and security. Facing increasingly intense international data market competition, China has adopted tiered and classified management based on the Data Security Law and the Personal Information Protection Law. In 2020, China joined RCEP and formally applied for CPTPP/DEPA in 2021, gradually aligning domestic cross-border data management measures with international high-standard rules (Wang, 2024).

# 4 CHALLENGES AND RESPONSES IN INTERNATIONAL COORDINATION

## 4.1 Challenges

First, the boundary between security exceptions and public policy exceptions (Li, 2025). Most agreements permit restrictions on data flows based on national security or public policy grounds. However, the specific scope remains contentious, as exemplified by RCEP's explicit stipulation that "essential security interests" shall be determined by each contracting party, whereas CPTPP requires restrictive measures to comply with the principle of proportionality.

Secondly, the legitimacy of data localization requirements (Tan, 2022). Most countries with digital technology advantages advocate restrictions on data localization, aiming to establish an open and free international order for cross-border data flow. By leveraging their technological or economic strengths, these countries seek to enhance their position in global cross-border data flow regulations, dominate upstream industries, and reap the dividends of the digital era. In contrast, countries with relatively weaker digital market competitiveness tend to adopt data localization strategies, restricting foreign enterprises from entering their domestic digital markets and prioritizing the security of national digital sovereignty. According to credible data, by 2021, 62 countries worldwide had implemented 144 restrictive measures related to data localization (Cory & Dascoli, 2021). To this day, the conflict between free data flow and data localization remains unresolved.

Third, there is a conflict between privacy

protection and the liberalization of data flow. The divergence between the GDPR and U.S.-style regulations clearly reflects the tension between safeguarding privacy rights and pursuing economic benefits from data. In the global development of cross-border data flow, both free data movement and data privacy protection are indispensable. However, how to reconcile free data flow with data privacy protection remains an unresolved issue.

### 4.2 Responses

Although the Chinese approach has achieved certain results thus far, when facing the challenges and opportunities brought by cross-border data, China still needs to actively and deeply participate in the international institutional framework, carefully examine its own institutional status quo, and proceed with optimization from the following aspects.

First, accelerating the process of improving domestic legislation. As the nation places greater emphasis on cross-border data, the number of relevant domestic regulations has been increasing. However, it must be clearly recognized that China is still in the initial stages of legal governance for cross-border data, with imperfections in areas such as jurisdictional scope and enforcement design for cross-border data governance. The Data Security Law should explicitly stipulate "ensuring the orderly and free flow of data in accordance with legal provisions," while the Personal Information Protection Law should refine provisions on outbound security assessments, certification, and contractual mechanisms. Open pilot programs should be established, developing Hainan Free Trade Port as a "data special zone" and the Yangtze River Delta as a "data hub," while creating a negative list for cross-border data. Permits should be granted in areas such as game exports and data processing to reduce corporate compliance costs.

Second, China must actively promote alignment with international rules. Currently, China has joined the RCEP and has applied to join the CPTPP and DEPA. China needs to immediately begin organizing domestic regulations to align with relevant provisions of DEPA and CPTPP, making preparatory efforts in advance to prevent conflicts between domestic and foreign regulations and facilitating a smooth transition between domestic rules and the "principle + exception" model. China should also enhance its international discourse power, firmly opposing long-arm jurisdiction and vigorously advocating a governance model based on consultation and joint development.

Third, regional innovation experiments should be conducted. China can explore a classified regulatory system for full-process cross-border data governance in the Shanghai Free Trade Zone or the Guangdong-Hong Kong-Macao Greater Bay Area, establishing offshore data centers and international data-specific channels. Leveraging these advantages, China should propose initiatives from its own perspective on digital development, security governance, and mutual recognition of standards, gradually testing fairer, safer, and more sustainable dispute resolution mechanisms, improving arbitration technology, and establishing compensation funds.

## 5 CONCLUSION

This paper analyzes the fragmented international regulatory system governing cross-border data flows and its core controversies. Key challenges include ambiguous exceptions, data localization disputes, and unresolved privacy-free flow conflicts. To counter Euro-American dominance, China must adopt an "internal-external linkage" strategy: improving legal adaptability domestically while promoting multilateral cooperation. This approach will help establish a secure, efficient, and inclusive global digital governance paradigm, critical for advancing China's digital economy and fostering global equity.

## REFERENCES


Bradford, A. 2012. The Brussels Effect. *Northwestern University Law Review* 107(1): 1–68.

Burri, M. 2017. The regulation of data flows through trade agreements. *Georgetown Journal of International Law*, 48(1). Available at SSRN.

Cory, N. & Dascoli, L. 2021. How barriers to cross-border data flows are spreading globally. *ITIF*.https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/.

Data Guidance. 2020. Berlin commissioner issues statement on Schrems II case.

Lando, M. 2022. Enhancing conflict resolution 'ASEAN Way': The dispute settlement system of RCEP. *Journal of International Dispute Settlement* 13(1): 98–120.

Li, Y. 2025. Balancing template clauses for cross-border data flows in international trade law. *Journal of International Economic Law* (1): 58–80.

Tan, G. 2022. International legal regulation of cross-border data flows in digital trade. *Comparative Law Review* (3): 169–185.

U.S. Department of Commerce. 2025. *Global cross-border privacy rules declaration.*

Wang, A. 2024. Cyber sovereignty at its boldest: A Chinese perspective. *SSRN*.
Xia, J. & Zhang, Y. 2024. Regulatory dilemmas and pathways for cross-border data flows in digital trade. *Economic Review* (4): 39–46.