Proceedings of the 4th International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2026.33431

Coordination Between National Security and International Economic Law in Cross-Border Data Flows: A Comparative Analysis Based on CPTPP and RCEP

Xiaobing Jin

Law School, East China University of Political Science and Law, Shanghai, China
Jinxiaobing66@outlook.com

Abstract. The advent of cross-border data flows has become a fundamental aspect in the digital economy era that is transforming the world economic and trade environment. Being two fundamental regional trade agreements, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Regional Comprehensive Economic Partnership (RCEP) have evolved two contrasting paradigms of regulatory approaches to cross-border data flows as one of them focuses on trade liberalization, and the other one is a balanced approach that has been accommodative to both security and development. The paper will compare the rule design, and value orientations and formation logics of the two agreements, discuss their central conflicts, such as data localization and the implementation of security exception clauses, and also expose practical dilemmas, such as governance fragmentation, over-use of national security, and lack of coordination mechanisms. In this work, four fundamental principles are proposed: value balancing, differentiated coordination, rule clarification and multilateral collaboration and develop a three-dimensional coordination trajectory with rule mutual recognition, mechanism linkage and interest reconciliation. The paper addresses the gap in the theory of in-depth comparative studies of regional data regulations, offers theoretical justification of balancing national security with international economic law and also offers practical references through which China can be in agreement with the international rules and develop a cross-border data regulatory system to coordinate security and openness.

Keywords: Cross-border data flows, national security, international economic law, CPTPP, RCEP

1. Introduction

In the era of the digital economy, data has become a new factor of production, and the growing size of cross-border flows of data is transforming the global economy and trade environment. In the meantime, the strategic essence of data has become intricately connected with national security. The threat to information security, industrial security and even national sovereignty posed by cross-border data flows has been ever more eminent, prompting nations to tighten their control over the flow of cross-border data. It is against this backdrop that the CPTPP and RCEP as the most powerful

© 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: 10.54254/2753-7048/2026.33431

regional trade agreements have evolved different regulatory paradigms. CPTPP is geared towards the so-called priority of trade liberalization and puts rigid limitations on the data localization requirements. In its turn, RCEP is much more developmentally inclusive and leaves much to be desired in terms of national security discretion of its member states. The divergences in their respective philosophies and rules have not only increased the cross-border compliance burden on enterprises but also posed challenges to the coordination of the international economic law system. Currently, the majority of theoretical research is dedicated to textual analysis of one agreement or macro discourse on multilateral frameworks, which is very limiting. Indicatively, the comparisons of data rules in the CPTPP and the RCEP by some scholars are at a surface level of the clauses without a detailed discussion of the value-balancing logic of the security and liberalism of the two agreements. A few studies grapple with over-securitization of national security and the deployment of security exception clauses, but do not consider the relevant limits of such clauses and conflict coordination systems, and the dilemmas of governance brought about by the issue of securitization overreach in practice are hard to resolve. Other researchers have discussed the ways through which China can fit the two regimes yet have not provided adequate exploration of ways to strike a balance between security and openness, and lack of working institutional design.

Against this background, this paper achieves the theoretical goals of deconstructing the regulatory logic and root causes of conflicts between the two agreements, filling survey research gaps in comparative studies on regional data rules and expanding interpretive dimensions of international economic law in a digital epoch. In practice, it can help China participate in global data governance and align with high-standard international rules to build cross-border data flow governance system that coordinates security and openness.

2. Literature review

In the era of the digital economy, cross-border data flow has become a core element in reshaping the global economic and trade landscape. Its deep integration with national security poses adaptive challenges to the international economic law system. As representative regional trade agreements, CPTPP and RCEP have developed differentiated regulatory paradigms for data, exacerbating rule conflicts and governance fragmentation. Coupled with the trend of securitization overreach in national security, how to balance the liberalization of data trade and national security, coordinate divergent rules, and resolve dilemmas in the application of security exceptions has become a core issue in the field of international economic law. Existing studies have explored this topic from multiple dimensions, and relevant findings are summarized as follows.

With regard to data rules in regional trade agreements and the application of security exception clauses, scholars have focused on regulatory defects and practical dilemmas. Guo Dexiang pointed out that the text of the general security exception clause on cross-border data flows in RCEP is overly flexible, with problems such as ambiguous key concepts and insufficient restrictions on the self-judging power of contracting parties and proposed optimizing its application through good-faith interpretation [1]. Liao Li and Wu Ziwei, by comparing the WTO, CPTPP, RCEP and other agreements, found that security exception clauses generally suffer from vague self-judging criteria, and cross-border data flows can hardly meet the traditional prerequisites for application, giving rise to legitimacy disputes [2]. Huo Junxian added that relevant agreements do not specify the scope of application of "essential security interests", which entails potential risks for China when invoking this clause for the outbound transfer of important data [3].

On the dimension of securitization overreach in national security and global data governance, scholars have analyzed its manifestations, motivations and impacts. Based on game theory, Shen

DOI: 10.54254/2753-7048/2026.33431

Wei argued that the ambiguous definition of national security has led to "securitization overreach", trapping countries in a cycle of self-protection and concerns over policy abuse by other states, which is reflected in the abuse of security exception clauses and the rise of trade protectionism [4]. Zhang Ming noted that securitization overreaches in national security is characterized by ambiguous standards and expanded scope, driven by factors including global data competition and containment by developed countries [5]. Du Ming stated that the fragmentation and securitization of data rules amid the transformation of international economic law have increased the complexity of global governance [6].

Regarding China's alignment with international rules and the construction of discourse power, scholars have put forward diversified pathways. Xie Zhuojun et al. provided references for China to integrate with regional rules by comparing the WTO, CPTPP and RCEP. Wang Huahua emphasized that China is at a disadvantage in terms of discourse in formulating data rules and needs to build discourse power with distinctive data security governance through multi-stakeholder coordination [7]. Song Yang offered references for the dispute settlement of cross-border data flows from the perspective of International Centre for Settlement of Investment Disputes (ICSID) arbitration principles [8].

Overall, existing studies have clarified the core contradictions and practical challenges in cross-border data flows, yet research gaps remain. First, comparisons between CPTPP and RCEP data rules lack depth in value balancing and neglect the operational standards of security exception clauses. Second, responses to securitization overreach lack systematic solutions. Third, discussions on China's integration pathways are relatively macro and lack operable institutional design. Future research should focus on the root causes of rule conflicts, refine the applicable boundaries of clauses, and build a governance system that balances security and openness based on China's practice, so as to provide support for global data governance.

3. Paradigm divide and formation logic of cross-border data flow regulation in the CPTPP and RCEP

Security risks arising from cross-border data flows are complex in nature, with traditional sovereign security intertwined with non-traditional sectoral risks. This characteristic determines the central position of national security in the data regulatory system [4].

Against this background, this paper deeply deconstructs the differences in regulatory paradigms between the two agreements. The CPTPP adheres to a paradigm of priority to trade liberalization, with the core objective of promoting barrier-free cross-border data flows. Its rule design centers on restricting the regulatory authority of member states, establishing a high-standard liberalized rule system by explicitly prohibiting data localization requirements and strictly limiting the application scenarios of security exceptions. Specifically, Article 14.11 of the CPTPP expressly forbids member states from imposing tariffs on digital products, while Article 14.13 strictly restricts data localization requirements, permitting exceptions only within a narrow scope on the basis of "necessity and non-discrimination." Its security exception clauses are formulated with rigorous wording, clearly defining the application scenarios of "essential security interests" and imposing constraints on the self-judging power of member states. In essence, this serves the demand for the global expansion of the digital industrial advantages of developed countries.

In contrast, the RCEP establishes a paradigm of inclusiveness of security and development, fully accommodating the divergent development levels and regulatory capacities among its member states. It does not impose a mandatory ban on data localization. Article 12.15 of the RCEP does not prohibit data localization, but merely "encourages" the free cross-border movement of data. Its

DOI: 10.54254/2753-7048/2026.33431

security exception clauses adopt ambiguous wording such as "as a Party considers necessary," reserving ample policy space for countries to adopt regulatory measures based on their essential security interests. This achieves a balance between the regulatory autonomy of developing countries and regional trade cooperation.

Such a paradigm divide is not accidental, but a concrete manifestation of the clash between the ideologies of neoliberalism and the reversion of regulatory authority in international economic law, as well as an inevitable outcome of the ongoing transformation of the global economic order [6.9].

This paper further traces the deep logic behind the formation of these paradigms. In terms of member state composition, most CPTPP parties are developed digital economies with strong competitiveness in the digital industry, and their demand for free data flows far outweighs their need for regulation. By contrast, the RCEP includes both developed and developing countries with significant disparities in the level of digital economic development, resulting in a more urgent need to safeguard national security and the right to development [10].

From the perspective of economic and trade strategic orientation, the CPTPP aims to forge a "high-standard template" for global digital trade rules, reduce compliance costs for multinational enterprises through unified norms, and consolidate the dominant position of developed countries in the digital economy. RCEP, however, focuses on promoting regional economic integration, building consensus for cooperation through inclusive rules and leaving buffer space for developing countries to adapt to the regime.

As indicated by existing research, these differences are also related to member states' strategies to address "securitization overreach": developed countries tend to curb the abuse of security exceptions through unified rules, while developing countries rely more on flexible provisions to safeguard their regulatory sovereignty [11].

4. Core dimensions of regulatory conflicts and governance dilemmas in cross-border data flows

This section focuses on the nature of rule conflicts between the two agreements, arguing that they are not mere differences in clause wording, but a superposition of multiple contradictions running through value orientations, rule design and enforcement logic. In terms of value orientation, the core divergence lies between "trade liberalism first" and "national security plus the right to development as priorities"; in rule design, it is the institutional difference between "rigid constraints" and "flexible elasticity"; in enforcement logic, it is the practical gap between "uniform standard application" and "differentiated discretion" [12]. Such multi-layered conflicts have directly plunged global data governance into a dilemma of "regional fragmentation", echoing scholar Du Ming's argument that international economic law has entered an "era of no consensus" [6].

From a practical perspective, rule conflicts have given rise to three major governance dilemmas. First, the fragmentation of the global data governance system has intensified, and enterprises face "dual compliance" pressures. Enterprises engaged in economic and trade cooperation with members of both agreements must adapt to two fundamentally distinct rule systems, leading to a sharp rise in compliance costs. Existing studies have confirmed the hindering effect of such fragmentation on the global data supply chain [6].

Second, the phenomenon of "securitization overreach" has become increasingly severe, with some member states using security exception clauses as a pretext to erect data trade barriers. The trend of "security measures shifting from exceptions to principles," as observed by some scholars, is particularly prominent in the data sector. The United States, on grounds of national security, has imposed restrictions on domestic data storage and review for platforms such as TikTok, forcing

DOI: 10.54254/2753-7048/2026.33431

relevant data to be stored and examined within its territory. This essentially instrumentalizes and politicizes data governance. India, through its Digital Personal Data Protection Act, has also invoked data security and national sovereignty to mandate the localized storage of sensitive personal data and critical data, restrict cross-border transfers and impose heavy penalties, which clearly exceed the necessary limits of reasonable security protection. Both cases essentially represent the distortion of security exceptions into tools of geopolitics and trade protectionism, seriously deviating from the basic norms of free data flows and international economic and trade rules [4].

Third, there is a lack of mechanisms for coordinating rule conflicts. Neither agreement establishes special consultation or dispute settlement provisions targeting inter-agreement rule conflicts. When a member state joins both agreements, it faces a dilemma in rule application. The absence of an effective third-party coordination mechanism further exacerbates governance chaos in practice.

In addition, the chaotic application of security exception clauses has become a focal point of conflicts. Research by Guo Dexiang points out that the ambiguous wording "as a Party considers necessary" in the RCEP grants member states strong self-judging power, and the provision that "other Parties shall not raise objections" further weakens constraints on the abuse of rules [1]. Although the CPTPP deletes the specific application scenarios in the WTO security exception clause and expands its scope of application, it still fails to clarify the definition of "essential security interests."

Research by Liao Li and Wu Ziwei further confirms that, due to the lack of uniform applicable boundaries and interpretive rules, the invocation of security exception clauses by various countries is characterized by subjectivity and arbitrariness. Cross-border data flows can hardly meet the traditional prerequisite of "emergency in international relations," leading to intense controversy over the legitimacy and rationality of clause application [2].

In practice, developed CPTPP members such as Japan, Australia and Singapore have repeatedly questioned the practices of Malaysia and Vietnam in imposing domestic storage of critical data and restricting cross-border transfers on national security grounds, citing the rigid obligation under Article 14.13 of the CPTPP to prohibit data localization. They argue that such measures exceed the scope permitted by the principles of necessity, non-discrimination and proportionality, constituting disguised digital trade barriers. Malaysia and Vietnam, on the other hand, insist on retaining data localization requirements on grounds of data sovereignty, public security and inadequate regulatory capacity, and strengthen their regulatory stance by relying on the discretionary space under RCEP security exceptions.

Such real conflicts epitomize the core divergence of interests between developed countries, which advocate restricting the abuse of security exceptions through uniform rules, and developing countries, which uphold regulatory autonomy. They place dual members in a dilemma of rule application, significantly increase the difficulty of inter-agreement coordination, and further intensify the fragmentation of global data governance.

5. Core principles and implementation paths for coordinating national security and international economic law

This section aims to resolve rule conflicts and extricate from governance dilemmas, constructing a theoretical framework and principle system for the coordination of cross-border data flows.

First, based on the basic principles of international economic law, the theoretical foundation of coordination is clarified — the coordination of cross-border data flows is not a negation of a single set of rules, but a dynamic balance of multiple values within the framework of international

DOI: 10.54254/2753-7048/2026.33431

economic law. Shen Wei's game theory analysis has shown that pursuing trade liberalization alone or overemphasizing national security will both lead to a "prisoner's dilemma"; only rule coordination can achieve Pareto optimality in global data governance [4].

Based on this, this study proposes four core coordination principles.

First, the principle of value balancing. While safeguarding the liberalization of data trade, it respects the legitimate security interests of all countries and prevents national security from being distorted into a tool for trade protection. Scholar Du Ming emphasizes that this principle is the key to resolving the current theoretical crisis of international economic law [6].

Second, the principle of differentiated coordination. It fully respects the different development stages, digital industrial levels and regulatory capacities of various countries, rejecting a "one-size-fits-all" high-standard regulation. This is consistent with the inclusive concept of the RCEP and aligns with Yin Wei's governance idea of "restricting securitization overreach through development mechanisms" [11].

Third, the principle of rule clarification. Focusing on security exception clauses, the core of conflicts, it clarifies their applicable boundaries, interpretive rules and burden of proof. By eliminating rule ambiguity, it curbs "securitization overreach". Combined with the good-faith interpretation method proposed by scholar Guo Dexiang, it provides clear behavioral guidelines for member states [1].

Fourth, the principle of multilateral collaboration. Relying on existing multilateral frameworks such as the WTO and APEC, it promotes positive interaction between regional rules and multilateral rules and constructs a multi-level governance system of "regional coordination + multilateral consensus" to resolve the dilemma of "fragmentation".

In terms of specific implementation paths, it advocates building a three-dimensional framework of "rule mutual recognition + mechanism linkage + interest coordination".

At the level of rule mutual recognition, it promotes compatible interpretation of the core rules of the two agreements, and advances "flexible compatibility" interpretation for areas of core divergence — the CPTPP recognizes transitional localization measures adopted by developing countries due to insufficient regulatory capacity; RCEP member states commit not to abuse security exception clauses and clarify the applicable period and scope of localization measures. Meanwhile, it forms "minimum consensus standards" for non-core divergence areas, including prohibiting discriminatory data restrictions in the name of security, establishing a mutual recognition mechanism for cross-border data flow security assessment, and clarifying the burden of proof for security exception clauses.

At the level of mechanism linkage, it establishes a rule coordination dialogue mechanism between CPTPP and RCEP member states to provide a communication platform for conflicts in the application of cross-agreement rules. A working group for data rule coordination among CPTPP and RCEP member states is established to hold dialogue meetings every six months to negotiate solutions to rule conflicts. Relying on the APEC Cross-Border Privacy Rules (CBPR) system, it constructs a cross-agreement dispute settlement mechanism, adopting a "mediation first, arbitration as a last resort" approach to handle rule application disputes and improve coordination efficiency.

At the level of interest coordination, it balances the interests and demands of both developed and developing countries, finding a balance between free data flow and regulatory autonomy, and avoiding a single stakeholder dominating rulemaking.

On this basis, China can align with international rules from two aspects.

First, domestic system optimization. Improve the data classification system, simplify cross-border procedures for non-sensitive data to adapt to the free flow requirements of the CPTPP; retain

DOI: 10.54254/2753-7048/2026.33431

necessary security assessment and localization measures for important data and sensitive personal information, in line with the inclusive concept of the RCEP; revise the Measures for Security Assessment of Data Outbound Transfers to clarify the applicable boundaries of security exception clauses and avoid conflicts with international rules.

Second, deepening regional cooperation. Relying on the RCEP to promote mutual recognition of data rules among member states, take the lead in reaching security assessment mutual recognition agreements with digital economic powerhouses such as Singapore and New Zealand; actively participate in CPTPP digital rule negotiations, put forward a Chinese plan of "balancing security and freedom", and enhance the discourse power in rule-making in global data governance.

6. Conclusion

This study focuses on the coordination between national security and international economic law in cross-border data flows under the frameworks of the CPTPP and RCEP. Against the backdrop of the digital economy reshaping the global economic and trade landscape, cross-border data flows have become a key carrier for the allocation of core factors. The differentiated regulations of the two agreements have triggered rule conflicts and governance fragmentation, and coupled with the securitization overreach of national security, this not only increases the cross-border compliance costs for enterprises but also impacts the coordination of the international economic law system. Conducting this research can theoretically fill the gap in comparative studies on regional data rules and expand the interpretive dimensions of international economic law in the digital era; practically, it can provide references for China to coordinate security and openness, align with high-standard international rules, and build a cross-border data flow system, which is of great significance for resolving the "security dilemma" in digital trade.

This study holds that the core of coordinating national security and international economic law in cross-border data flows lies in achieving a dynamic balance between trade liberalization, national security and the right to development within the framework of international economic law, rather than the unification of a single set of rules. There is no absolute superiority or inferiority between the CPTPP's paradigm of "priority to trade liberalization" and the RCEP's paradigm of "inclusiveness of security and development". Conflicts stem from differences in value orientations and regulatory logic, and the key to resolution lies in clarifying the boundaries of security exception clauses and constructing a differentiated coordination mechanism.

In the future, the coordination between security and the rule of law in cross-border data flows will become a core issue in global data governance, developing in the direction of diversity, inclusiveness and collaborative governance.

References

[1] Guo, D. (2025) Research on the Application of the General Security Exception Clause on Cross-Border Data Flows in the RCEP. Contemporary Law Science.
[2] Liao, L. and Wu, Z. (2024) Research on the Application of National Security Exception Clauses in Cross-Border Data Flows. International Trade, (8).
[3] Huo, J. (2025) The Predicament of Applying the Security Exception Clause to Cross-Border Data Flows and China's Countermeasures. International Trade, (08), 86-96.
[4] Shen, W. (2023) The Security Dilemma of International Economic Law — A Game Theory Perspective. Contemporary Law Science, (1).
[5] Zhang, M. (2025) The Securitization Overreach of National Security and the Restructuring of the Global Data Supply Chain: Manifestations, Motivations and China's Response. International Trade, (5).
[6] Du, M. (2025) Crisis and Reconstruction of International Economic Law. Tsinghua Law Review, (5).

DOI: 10.54254/2753-7048/2026.33431

[7] Wang, Z., Dai, C. and Zeng, Y. (2026) The Discourse Power of Security Governance on Cross-Border Data Flows: Generating Logic and Construction Pathways. Journal of Intelligence, 45(3), 62-69.
[8] Song, Y. and Gu, S. (2026) On the Autonomy of Will in ICSID International Investment Arbitration. Journal of Beijing Institute of Technology (Social Sciences Edition), 28(1), 93-105.
[9] Koremenos, B., Lipson, C. and Snidal, D. (2001) The rational design of international institutions. International Organization, 55(4), 761-799.
[10] Feinberg, R. (2012) Complex global governance and domestic policies: Four pathways of influence. International Affairs, 88(5), 1035-1053.
[11] Yin, W. (2024) The Dilemma of Securitization Overreach in International Investment Governance and Reflections. Law and Business Research.
[12] Abbott, K.W., Keohane, R.O., Moravcsik, A., Slaughter, A.M. and Snidal, D. (2000) The concept of legalization. International Organization, 54(3), 401-419.