China's Response to Enterprise Cross-Border Data Flow Rules from the RCEP Perspective

Kaiyun Shi*

School of International Law, Shanghai University of Political Science and Law, Shanghai, 201701, China

*Corresponding author. Email: 1329581867@qq.com

Abstract. Under the current social context, the importance of enterprise cross-border data flow has grown significantly with the increasing development of information technology and the deepening of globalization. However, to ensure the more comprehensive applicability and coherence of enterprise cross-border data flow under the RCEP treaty framework, more specific rule-making and policy implementation are required. First, an analysis of the relevant rules on enterprise cross-border data flow in RCEP reveals that the current framework on enterprise cross-border data flow presents a compatible relationship between general rules and exception clauses. Meanwhile, a study of domestic legal norms on enterprise cross-border data flow indicates that China's current legal system for cross-border data circulation is structured with the *National Security Law* as the overarching principle, sectoral laws as the main body, and normative documents as supplementary provisions. Nevertheless, numerous issues persist in China regarding enterprise cross-border data flow, including the inherent limitations of RCEP at its current stage, as well as legal conflicts and coordination barriers between domestic laws and RCEP. Consequently, specific measures must be implemented to address these challenges. On one hand, refinement can be achieved by targeting RCEP's exception clauses, including updating and optimizing legal provisions while thoroughly improving and clarifying the standards. On the other hand, efforts must also focus on strengthening the reform and implementation of domestic rules governing enterprise cross-border data circulation.

Keywords: Cross-Border Data Flow, RCEP, Enterprise Data, Data Rights Confirmation

1 Introduction

In the current era of rapid advancements in information technology and deepening globalization, data as a factor has acquired significant economic value. Simultaneously, with the accelerated pace of enterprise internationalization, the importance of enterprise cross-border data flow has been increasingly amplified.

However, enterprises inevitably encounter legal issues related to cross-border data circulation during overseas operations. In addressing legal legal issues concerning

© The Author(s) 2026
J. Rak et al. (eds.), *Proceedings of the 2026 11th International Conference on Social Sciences and Economic Development (ICSSED 2026)*, Advances in Economics, Business and Management Research 391,
https://doi.org/10.2991/978-94-6239-701-9_2

cross-border data flow, domestic legal norms such as the *Cybersecurity Law and the Data Security Law, as well as the Regional Comprehensive Economic Partnership Agreement (RCEP)* that China has joined, have established relevant rules governing cross-border data flow. This paper will first examine the rules pertaining to enterprise cross-border data flow under RCEP, focusing on its general rules and exception clauses. Subsequently, the paper will systematically analyze domestic legal norms on enterprise cross-border data flow. Following this, the paper will concentrate on the current challenges faced by China regarding enterprise cross-border data circulation. Finally, based on an in-depth analysis of the aforementioned aspects, specific measures to address these issues will be proposed, seeking reasonable and effective approaches to the governance of enterprise cross-border data flow.

2 RCEP Rules on Enterprise Cross-Border Data Flow

The *Regional Comprehensive Economic Partnership Agreement (RCEP)* stands as one of the world's largest free trade agreements. To foster an open and mutually beneficial global economy while accounting for the varying stages of economic development among member states, RCEP adopts a more inclusive approach in reaching consensus on digital trade regulations (Rui, Z. 2024) [1]. Section 4, "Facilitating Cross-Border E-Commerce", provides a relatively systematic framework for enterprise cross-border data flow.

2.1 General Rules on Cross-Border Data Flow in RCEP

2.1.1 Freedom Clauses of Cross-Border Data Flow in RCEP.

The original text of RCEP explicitly advocates and supports the free cross-border flow of data among member states, recognizing it as a core element of digital economic development. Clause 15.2 stipulates that a Party shall not prevent cross-border transfer of information when such transfer serves the business operations of a covered person, establishing the principle that cross-border data flow should be governed by freedom. This provision transcends the frameworks of other traditional trade agreements by treating data as a production factor of equal status to goods and services. Thus, the relevant clauses under RCEP aim to reduce compliance costs for enterprises dealing with cross-border data circulation issues while promoting the integration of regional digital economies and trade.

In addition to Clause 15, RCEP Clause 14 also addresses contents related to cross-border data flow among member states, with its second paragraph forming the core of the prohibition on computing facility localization for cross-border data circulation. It stipulates that no party is permitted to demand a covered person to utilize or place computing facilities within its territory as a requirement for conducting business in that territory. This clause is designed to prevent member states from erecting trade barriers through computing facility localization (e.g., data storage, server placement, etc.), thereby ensuring that enterprises across nations can freely choose methods for cross-border data storage and processing (Guo, D., Zhang, J. 2024) [2].

2.2 Exception Clauses on Cross-Border Data Circulation in RCEP

2.2.1 Public Policy Objective Exception Clause.

Although RCEP adopts a supportive and encouraging stance toward enterprise cross-border data circulation, considering the diverse development models and varying economic and trade needs among member states, situations may arise where full compliance with the general principle of unrestricted cross-border circulation becomes unfeasible. Therefore, in addition to the general rules, RCEP has incorporated multiple exception clauses.

Both Clause 14 and Clause 15 of RCEP permit contracting parties to adopt measures inconsistent with the principle of free flow based on "public policy objectives". However, this exception clause is subject to stringent conditions. On one hand, the exception clause must satisfy the necessity requirement stipulated in the clause, meaning that the measures taken to achieve the "public policy" objective must be "necessary". On the other hand, the exception clause is also required to obey the legal requirements set forth in the clause, which includes that the measures must not count as arbitrary or unjustified discrimination, nor as a disguised restriction on trade. Thus, if the public policy objective exception clause is invoked to restrict cross-border data circulation, it must simultaneously meet the legality and necessity requirements prescribed in the provisions.

2.2.2 Essential Security Interests Exception Clause.

In addition to the public policy objective exception clause, RCEP also includes an essential security interests exception. Clauses 14 and 15 allow member states to take necessary measures based on "essential security interests", even if such measures contravene the principles prohibiting computing facility localization and restricting cross-border data flow, and other contracting parties may not raise objections. This clause does not impose restrictive conditions, nor does it require the measures to meet necessity or legality criteria. Furthermore, it explicitly prohibits recourse to dispute settlement mechanisms. Compared to the "legitimate public policy objective" exception, its application is more lenient—as long as a contracting party deems the measures necessary to safeguard its essential security interests, it may be exempt from RCEP's provisions on the free flow of cross-border data.

3 Domestic Legal Norms for Enterprise Cross-Border Data Flow

Against the backdrop of rapid global digital economic development and deepening cross-border data circulation, China has progressively established a legal system for cross-border data flow, with the *National Security Law* as its overarching framework, sectoral laws as the main body, and normative documents as supplementary components, in order to comply with the requirements of RCEP and other multilateral agreements regarding enterprise cross-border data circulation. This legal framework emphasizes both safeguarding national security and accommodating the need for rational data flow as a production factor.

3.1 National Security Law: Foundational Provisions for Enterprise Cross-Border Data Flow

As a fundamental law, the *National Security Law* establishes the principle of data sovereignty and a national security review mechanism. Clause 25 incorporates information security into the scope of national security, requiring the protection of core network technologies, critical infrastructure, and the security of important information systems and data, while preventing cyberattacks, intrusions, and other illegal activities to uphold national sovereignty and security in cyberspace. For cross-border transfers of data involving critical information infrastructure operators, a national security review must be conducted to ensure the security and controllability of core data resources. Cross-border data circulation must comply with national security requirements and strictly adhere to relevant legal provisions. The *National Security Law* serves as the cornerstone for cross-border data flow regulations, providing the legal basis for supervision.

3.2 Other Sectoral Laws: Detailed Provisions for Enterprise Cross-Border Data Flow

Sectoral laws regulate and oversee enterprise cross-border data flow from different perspectives. Currently, China has established a legal framework in the field of cross-border data circulation, with the *Cybersecurity Law*, the *Data Security Law*, and the *Personal Information Protection Law* at its core, forming a regulatory system that balances security and development. These three laws establish data governance rules from distinct dimensions.

The *Cybersecurity Law* imposes explicit data localization requirements. Clause 37 stipulates that "operators of critical information infrastructure" must store "personal information and important data" collected during operations within China in principle. This provision applies to all enterprises operating in China. Such data is now regarded as one of the most critical production factors. To prevent potential leaks and secondary risks during cross-border processing, this law prioritizes security in cross-border data circulation, making data exit security a core aspect of cross-border circulation.

Building upon the relevant rules of the *Cybersecurity Law*, the *Data Security Law* further clarifies and mandates security management for data. First, it innovatively sets up a system for data classification and hierarchical protection, identifying data linked to "national security and the lifelines of the national economy" as being subject to special protection. It stipulates that all localities and departments must, based on the data classification and hierarchical protection system, work out specific lists of important data for their own regions, departments, and related industries or fields, and give priority to protecting the data included in these lists. Second, it introduces a data security assessment mechanism, mandating that important data must undergo a security assessment by the cyberspace administration before data exit. Additionally, it establishes a data security emergency response mechanism and a data security review system, which, in conjunction with Clause 25, significantly supplements the *Cybersecurity Law*'s provisions on the review and supervision of cross-border data circulation.

Chapter 3 of the *Personal Information Protection Law* details the rules for cross-border circulation of personal information. Clause 38 states that cross-border circulation of personal information may be conducted in accordance with agreements or treaties to which China is a party. Clause 39 requires that cross-border flows must obtain separate consent from individuals to protect their rights. Clause 40 supplements the *Cybersecurity Law* by stipulating that operators of critical information infrastructure and large-scale personal information handlers must store personal information collected within China domestically, forming the legal basis for personal information localization. At the same time, it provides exceptions for cross-border flows: where it is truly necessary to provide personal information overseas, a security assessment by the national cyberspace administration must be conducted, unless exempted by laws and regulations. Overall, China's legal provisions on cross-border circulation of personal information are relatively comprehensive and well-developed.

3.3 Regulatory Documents: Operational Provisions for Enterprise Cross-Border Data Flow

China's regulatory documents provide more detailed supplements to the aforementioned sectoral laws through specific implementation rules, thereby enhancing the enforceability and operability of the legislation to a certain extent.

The *Opinions of the Central Committee of the Communist Party of China and the State Council on Building Basic Systems for Data to Maximize the Role of Data Elements* (hereinafter referred to as the "Twenty Data Measures") further specifies the classification and hierarchical management of data and proposes corresponding governance approaches. It requires more refined classification, categorization, and rights confirmation and authorization for enterprise data, personal data, and public data, respectively defining the legal rights at each stage of data processing. Additionally, the "Twenty Data Measures" actively promotes the construction of cross-border digital trade infrastructure by establishing a "mechanism for secure, compliant, and orderly cross-border data circulation", encouraging the exploration of cross-border data flow methods that are both secure and open for development.

On the other hand, the issuance of the *Measures for the Security Assessment of Outbound Data Transfer* clarifies the procedures and requirements for security assessment declarations related to data exits, stipulating the legal obligations of data processors to declare security assessments. It details the assessment process, required materials, and key assessment content, serving as a comprehensive management measure for data exits. Meanwhile, the *Guidelines for Filing the Standard Contract for Outbound Transfer of Personal Information* provides comprehensive regulations on the procedures and requirements for the cross-border circulation of personal information.

Furthermore, the *Provisions on Promoting and Regulating Cross-border Data Flow*, promulgated and implemented in 2024, also supplements the norms for cross-border data flow. This regulation explicitly classifies and manages "data collected and generated in activities such as international trade, cross-border transportation, academic cooperation, transnational manufacturing, and marketing" separately from important data

and personal information, adopting a more relaxed process management for cross-border data circulation that does not involve important data or personal information. It also implements classified management for personal information, exempting qualified cross-border flows of personal information from "declaring security assessments for data exits, entering into standard contracts for cross-border circulation of personal information, or obtaining personal information protection certification".

The aforementioned series of regulatory documents, through their interconnected and coordinated provisions, construct a framework system for data supervision. From data classification and identification to risk assessment and export approval, they form a complete institutional loop encompassing ex-ante prevention, in-process control, and ex-post accountability. Simultaneously, with the continuous improvement of China's domestic laws and regulations, policies on cross-border data circulation have become increasingly open and scientific. Corresponding to RCEP, these laws and regulations not only fulfill the obligations for data security protection under the RCEP framework but also reserve necessary institutional space for the development of the digital economy.

4 Challenges in Aligning Domestic Legal Rules with RCEP

4.1 Limitations Inherent in RCEP

As the world's largest free trade agreement, RCEP has established a fundamental framework for cross-border data circulation rules that primarily consists of general provisions supplemented by exception clauses. However, significant limitations exist in the practical operation and application of RCEP rules. These limitations stem not only from the agreement's limited binding force but also from the overly broad nature of its content.

4.1.1 Limited Binding Force of RCEP Rules.

As a regional trade agreement comprising both developed and developing countries, RCEP aims to promote common development and build an open world economy. Considering the uneven development of digital trade among member states and their varying practical needs, RCEP's cross-border data flow rules emphasize principles, encouragement, and advocacy rather than mandatory requirements, distinguishing it from more detailed and specific multilateral agreements such as CPTPP and USMCA (Zreik, M. 2024) [3]. Furthermore, RCEP's dispute settlement mechanism is incomplete. According to Clause 17 of the RCEP E-Commerce Chapter, contracting parties involved in disputes shall engage in consultations in good faith. If consultations fail, the matter may be submitted to the Joint Committee for further resolution, but it cannot be referred to the dispute settlement procedures under Chapter 19. This demonstrates that, in principle, enterprise cross-border data circulation disputes are not subject to RCEP's dispute settlement mechanism, and no specialized data dispute mechanism has been established. The absence of an effective dispute resolution mechanism results in limited binding force for the rules, making it difficult to effectively resolve disputes related to cross-border data circulation.

4.1.2 Overly Broad Content of RCEP Rules.

The limitations of RCEP are also reflected in its overly broad content. As mentioned earlier, RCEP includes corresponding exception clauses for cross-border data circulation. However, due to the excessively concise wording of the treaty itself, significant controversies arise in its practical application (Li, S. 2024) [4]. For example, the definition of "necessary measures" under the public policy objective exception clause is based solely on what a contracting party "considers" to be lawful conduct. Similarly, measures related to essential security interests rely on the subjective judgment of contracting parties, lacking objective standards. This impedes dispute resolution. RCEP's vague definitions of core concepts related to cross-border data circulation may affect the discretionary power of countries in regulating such flows. On one hand, the concept of public policy objectives is prone to overgeneralization, potentially enabling some countries to prohibit cross-border data transfers on national security grounds. On the other hand, expansive interpretations of the concept of essential security interests increase the risk of abuse, thereby weakening the normative effectiveness of the clauses.

In summary, given RCEP's weak binding force and ambiguous definitions of core concepts, enterprises may face difficulties in fully applying its provisions when addressing issues related to cross-border data circulation due to the RCEP Agreement's inherent limitations.

4.2 Misalignment Between Domestic Regulations and RCEP

4.2.1 Ambiguous Overall Stance of Domestic Regulations on Cross-Border Data Circulation.

First, based on the practical needs of national development, national policies and legal regulations often prioritize emphasizing national sovereignty and security. Such a tendency is directly reflected in the fundamental attitude toward cross-border data circulation. On one hand, the state actively participates in international multilateral organizations to promote trade openness, yet its emphasis on national security becomes a constraint on cross-border circulation for digital trade. Although the *Data Security Law* proposes "balancing security and development", the prioritization of "security" and "development" lacks clear guidance in the legal provisions. On the other hand, different legal documents exhibit divergent stances on cross-border data flow. For instance, Clause 37 of the *Cybersecurity Law* mandates that critical information "shall be stored within the territory", while the *Provisions on Promoting and Regulating Cross-border Data Flow* encourages cross-border data circulation. Such inconsistencies in laws and policies reflect the ambiguity in the state's stance on this issue.

4.2.2 Low Legal Hierarchy of Provisions on Enterprise Cross-Border Data Flow.

Currently, China's legal norms related to cross-border data are scattered across sectoral laws such as the *Cybersecurity Law* and the *Data Security Law*, as well as various regulatory documents like the *Measures for the Security Assessment of Outbound Data Transfer*. While these sectoral laws contain diverse and complex provisions, there is a lack of comprehensive and systematic legislation specifically governing enterprise

cross-border data flow. Although the *Personal Information Protection Law* serves as a dedicated sectoral law for the protection and regulation of personal data, its regulatory objectives are fundamentally different from those of enterprise data exit compliance. The *Personal Information Protection Law* primarily focuses on safeguarding personal privacy, whereas enterprise data exit compliance aims to promote the free flow of digital trade. Consequently, the relevant provisions of the *Personal Information Protection Law* cannot be analogously applied to enterprise data (Huang, Q. 2025) [5].

As a result, most provisions related to enterprise cross-border data flow appear in the form of departmental rules or regulatory documents, which occupy a lower level in the legal hierarchy. For example, although the *Provisions on Promoting and Regulating Cross-border Data Flow* relaxes certain restrictions, its legal status is inferior to that of the *Data Security Law*, making it difficult to override the constraints imposed by higher-level laws.

Moreover, due to the fragmentation of rules, enterprises must simultaneously comply with multiple laws and hundreds of departmental regulations. When multinational corporations handle user data, they may need to meet the security assessment requirements of the *Personal Information Protection Law*, the localization storage requirements of the *Cybersecurity Law*, and the declaration requirements of the *Measures for the Security Assessment of Outbound Data Transfer*. This sharply increases compliance costs, forcing some small and medium-sized enterprises to abandon cross-border operations due to their inability to bear multiple compliance pressures, thereby stifling the development of the digital economy.

4.2.3 Lack of Clarity in Core Terminology and Assessment Standards.

The current regulations on cross-border data circulation in China suffer from vague definitions of key terms, creating structural obstacles to implementation and leading to inconsistent legal application standards. For example, although the *Data Security Law* defines "important data" as "data related to national security, the lifelines of the national economy, and critical industries and fields", it lacks specific identification criteria. This ambiguity may invite challenges from other countries when invoking RCEP's exceptions for cross-border data flow. Additionally, terms such as "necessary circumstances" in legal texts can also lead to interpretive disputes. Clause 5 of the *Provisions on Promoting and Regulating Cross-border Data Flow* exempts "genuinely necessary" transfers of employee personal information overseas from assessment, but the term "genuinely necessary" lacks quantifiable indicators or operational guidelines, resulting in divergent legal interpretations and hindering dispute resolution.

Furthermore, the ambiguous definitions of core terms such as "important data" and "necessary circumstances" may lead to unclear assessment standards during specific security evaluations of enterprise data [5]. The unclear division of responsibilities among regulatory and assessment bodies, coupled with inadequate mechanisms for protecting rights related to assessment outcomes, leaves enterprises without effective administrative procedural support. Although China has specified regulatory authorities—Clause 6 of the *Data Security Law* designates the national cyberspace administration as the lead agency, with other departments cooperating in supervision—in practice, mul-

tiple entities, including the cyberspace administration, public security agencies, and industry regulators, participate in oversight. This results in fragmented and uncoordinated regulation, undermining the effective implementation of data security assessments and supervision.

5 China's Countermeasures for Cross-border Data Flow of Chinese Enterprises from the Perspective of RCEP

5.1 Formulating Detailed Provisions Targeting RCEP Exception Clauses

Since the content of RCEP regarding cross-border data flow is too broad, and the current relevant contents of China's *National Security Law* and *Cybersecurity Law* only emphasize and clarify national security and national sovereignty, there is a lack of definitions for "public policy objectives" and "essential security interests" involved in RCEP clauses. Therefore, it is possible to update and optimize legal provisions, comprehensively refine the definitions of the above-mentioned contents, and at the same time improve and clarify the standards. Thus, when Chinese enterprises face legal disputes arising from RCEP cross-border data flow, since China has refined and clarified such exception clauses domestically, they can directly apply domestic laws and regulations for connection and application. Therefore, the construction of domestic laws and regulations on RCEP-related rules can, to a certain extent, make up for the problem that the corresponding rules of RCEP are too broad.

5.2 Strengthening the Rule Transformation and Implementation of Cross-border Data Flow for Domestic Enterprises

5.2.1 Establishing the Legal Concept of Parallel Data Security and Free Flow.

In the context of the globalization of the digital economy, China's legislation on cross-border data flow urgently needs to achieve a clear positioning of value orientation and systematic reconstruction. The ambiguity of the current legal system between "security first" and "economic development orientation" has led enterprises to face the practical dilemma of unclear compliance directions. Therefore, efforts should be made to balance national security and economic interest development. First of all, China should adhere to and clarify the maintenance of national security, and further take the consolidation of national security as the core basic position. Restricting and regulating issues related to data sovereignty and data flow involving national security is not a manifestation of data protectionism. Such data related to the country's core fundamental interests do need reasons and necessity for protection (Li, W., Wu, J. 2023) [6]. Secondly, a clear and affirmative attitude towards cross-border data flow should be adopted. Due to the further strengthening and influence of the globalization of the digital economy, although a conservative cross-border data flow policy may ensure data security and stability in the short term, it will eventually be unable to comprehensively and systematically promote the development of digital economy and trade. Therefore,

on this basis, China should take supporting the free flow of cross-border data as a principle, comply with the relevant rules stipulated by RCEP, and clearly support the cross-border flow and transmission of data related to various commercial activities. In addition, since RCEP also stipulates the right to store data information overseas, in the design of rules involving data storage, it should comply with the relevant provisions of RCEP, allow and recognize the overseas storage of general enterprise data, so as to reflect the basic principle of free data flow and better connect with the content of RCEP treaties. At that time, when Chinese enterprises encounter possible cross-border data flow problems, the clear attitude of domestic data free flow will also provide legal basis and support for enterprises.

5.2.2 Unifying and Integrating Various Documents in the Form of Departmental Laws.

As mentioned above, various cross-border data laws and regulations are complex and diverse, and there is a lack of clear and specific superior laws. These problems will make the specific content of cross-border data too fragmented and some regulations too simplistic, which will greatly increase the operational cost of enterprise data compliance. Therefore, it is necessary to unify and integrate the scattered clauses of these departmental laws and normative documents, and centrally formulate specific departmental laws focusing on enterprise cross-border data flow rules, and systematically stipulate aspects such as enterprise data right confirmation, enterprise data classification, enterprise cross-border data processes, and enterprise data sovereignty protection, so as to achieve the situation of reducing costs and increasing efficiency in enterprise cross-border data compliance and having laws to abide by.

In addition, while integrating the relevant clauses of various normative documents and departmental laws, attention must also be paid to the clarity of the definitions of core terms. At present, China has adopted a relatively clear attitude towards the classification of data itself. However, as mentioned above, the definition of terms such as "important data" is still unclear and needs to be solved. Therefore, in order to conduct cross-border data security assessment and ensure that such data are fully protected during cross-border transmission, "important data" should be clearly identified.[5] In order to more accurately grasp its scope and nature, reference can be made to the content related to the catalogue of "important data" in the *Data Security Law*, by disclosing the catalogue of important data and its judgment standards, such as setting the threshold range for important data related to national security interests or public interests, and specifying the specific application scenarios of important data that meet national security needs, so as to carry out relatively precise screening and control of data content, and regularly analyze and update the catalogue of important data, so as to meet the needs of cross-border data flow under RCEP rules and achieve the dual goal of maintaining national security (Zhang, C. 2023) [7].

5.2.3 Further Optimizing the Data Evaluation and Supervision System.

The accurate screening of 'important data' and the clear provisions of laws and regulations can be used as specific standards for data security assessment and classification, which can greatly promote the evaluation and identification of cross-border data flow of Chinese enterprises. However, relying only on data definition standards is not enough for the evaluation system; the evaluation framework system also needs to be optimized. First of all, it is necessary to stipulate and clarify the subject of data circulation security assessment. At present, the departments responsible for data security assessment in China are not clear, and there is a lack of clear division of functions and responsibilities for evaluation and supervision departments. A series of steps in enterprise cross-border data operations need to be coordinated through various government functional departments, which will lead to insufficient cooperation between departments. Therefore, it is necessary to clarify the subjects and their terms of reference of cross-border data security assessment institutions and supervision departments, establish independent data security assessment institutions and data export supervision departments, and carry out efficient overall coordination and communication between departments. Secondly, it is necessary to build a data security protection mechanism. When enterprises are assessed to have data related to public policy objectives or essential security interests in data security assessment, in order to safeguard their own legitimate rights and interests, the protection mechanism for enterprise data rights should be improved, and administrative procedures such as reconsideration and litigation for enterprises to appeal against the results of relevant cross-border data security assessments should be provided to effectively protect the basic rights of enterprises. In addition, the supervision procedures should also be reasonably simplified. At present, the *Provisions on Promoting and Regulating Cross-border Data Flow* have simplified the procedures for data collected and generated in activities such as international trade, cross-border transportation, academic cooperation, transnational manufacturing, and marketing. The specific scope of the above categories can also be listed in a list, so as to reduce the possibility of inconsistent understanding of specific project supervision.

6 Conclusion and Outlook

Cross-border data flow of enterprises is of great significance in the current digital economy system, but it still faces multiple challenges in the application of laws under the RCEP framework and the connection with domestic laws. Although RCEP has established general rules and exception clauses under the treaty, due to its broad clauses and limited binding force, enterprises find it difficult to directly apply them to complex real situations. On the other hand, although China has initially established a cross-border data governance framework led by the *National Security Law*, there are still problems such as unclear policies, scattered rules, and ambiguous terms in the connection with RCEP. In order to effectively respond to the pressure of institutional adjustment brought by RCEP, it is urgent to create regulations targeting RCEP exception clauses, strengthen the guidance of the legal concept of parallel data security and free flow, integrate various legal rules and clarify them, and optimize the assessment mechanism

and supervision system, so as to achieve the institutional balance between enterprise data security and free flow under the RCEP framework and create a clearer and more feasible compliance environment for cross-border data flow for enterprises.

Reference

1. Rui, Z. (2024). China-ASEAN Bilateral Digital Trade under the RCEP Digital Trade Framework: Current situations, Challenges, and Responses. *Frontiers in Business, Economics and Management*, *14*(2), 196-205.
2. Guo, D., Zhang, J. (2024). RCEP's Regulation on Financial Data Localization Measures and China's Response, *Credit Reference*, *42*(09), 44-52.
3. Zreik, M. (2024). The Regional Comprehensive Economic Partnership (RCEP) for the Asia–Pacific region and world. *Journal of Economic and Administrative Sciences, 40*(1),57-75.
4. Li, S. (2024). Research on Security Exception Clauses for Cross-Border Data Flow in RCEP, *Investment and Cooperation*, (06), 46-48.
5. Huang, Q. (2025). On the Compliance Dilemmas and Optimization Paths for Enterprise Data Exit, *Wuhan University International Law Review*, *9*(01), 36-52.
6. Li, W., Wu, J. (2023). Legal Regulation of Cross-Border Flow of Financial Data and China's Solution, *Journal of Nantong University (Social Sciences Edition)*, *39*(05), 80-88.
7. Zhang, C. (2023). RCEP Basic Security Exceptions for Cross-Border Data Flows and China's Response. *Journal of Education, Humanities and Social Sciences*, *14*, 36-45.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.