Analysis of Challenges and Compliance Pathways for China's Data Regulation in Alignment with RCEP Data Flow Rules

Ke Shi *

Law School, Shanghai University of Political Science and Law (SHUPL), Shanghai, China

* Corresponding Author Email: Archerdec19@outlook.com

Abstract. With the rapid development of the digital economy, cross-border data flows have become a central issue in global economic and trade competition. The study utilizes the Security Exceptions Clause of the Regional Comprehensive Economic Partnership (RCEP) and China's Data Outflow Security Assessment System as entry points, examining the challenges and compliance pathways associated with flow regulations. Core issues. The study finds that there are two dilemmas in aligning China's data regulations with RCEP rules. At the regulatory level, RCEP is based on the principle of free movement with security as an exception, while China prioritizes security and constrains free movement through evaluation. At the institutional level, issues such as unclear scope of "important data", lack of facilitation mechanisms, and insufficient regulatory coordination have resulted in high compliance costs for enterprises. In response to these issues, the national level should promote consensus on the interpretation of RCEP security exception clauses, clarify the leading department for data export, and improve the directory of "important data". At the enterprise level, it is necessary to establish an internal compliance system, strengthen communication with regulatory authorities, and proactively apply for compliance certification. This study aims to provide a theoretical reference and practical guidance for enhancing the regulation of cross-border data flow in China and supporting enterprises in participating in international competition in compliance.

Keywords: cross-border data flows, RCEP, security exception clauses, enterprises' compliance.

1. Introduction

As the digital economy becomes the core engine of global economic growth, cross-border data flows have also become a focus of global economic and trade competition. The issue of "solving cross-border data flow and other problems" was included in the government work report in 2024 and clearly identified as one of the important measures to increase efforts to attract foreign investment. Based on it, some scholars have found through surveys on the five major sectors of e-commerce, cloud computing, logistics platforms, third-party payments, and software services that cross-border data flow directly affects the business activities of enterprises, affecting their costs and benefits, and even determining whether they can successfully integrate into and even dominate the global supply chain [1].

As the world's largest free trade agreement, the entry into force of the RCEP marks a new stage in the digital trade rules of the Asia Pacific region. Among them, the chapter on e-commerce also sets international obligations for the cross-border flow of data in China, and in principle allows the free flow of data for commercial purposes. At the same time, China has also successively promulgated relevant laws and regulations, such as the Data Security Law of the People's Republic of China, implementing data flow based on security assessments. There is a natural contradiction and a natural tension between freedom and security, which poses a dual compliance dilemma for Chinese companies seeking to "go global" and "bring in". Companies need to meet both strict domestic data export security assessments and timely responses to overseas transactions. Therefore, promoting China's data regulation and RCEP data flow rules has profound significance, not only for the interpretation and application of the treaty, but also for providing operational compliance path guidance for Chinese enterprises. Based on this, this study aims to explore a cross-border compliance path for enterprise data that is both in line with international legal obligations and based on China's institutional conditions, taking into account the actual deficiencies of China's data regulation.

2. Literature Review

The existing literature on the regulation of cross-border data flows mainly focuses on international rule schemes, challenges in domestic legal integration, compliance with special provisions such as security exception clauses, and China's response strategies.

In terms of international rules, scholars generally believe that the current international community has formed two main programs. Many scholars pointed out that the plan is unilaterally dominated by Europe and the United States, among which the United States emphasizes freedom of data flow, while the European Union pays more attention to privacy protection [2]. Huang systematically analyzed the provisions of Articles 12.14 and 12.15 of RCEP on the prohibition norms and exceptions for data localization and pointed out that the interpretation of the "legal public policy objectives" and "basic security interests" clauses should refer to the WTO case law and be defined by the parties according to their own actual situation [3]. There is a plan represented by RCEP and facilitated by China and ASEAN. Hong Zhigang and Huo Junxian further explained that the core of the RCEP program is to seek a balance under the premise of respecting national data sovereignty, which not only supports the free flow of data across borders but also establishes basic security exceptions [4].

In terms of the challenge of connecting with domestic laws, most scholars have pointed out a significant conflict between the high-standard rules dominated by Europe and the United States, and China's security-based domestic regulatory system. In terms of institutional impact, some scholars believe that this conflict allows China to participate in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). High-standard agreements, such as the Digital Economy Partnership Agreement (DEPA), have brought external pressure. In addition, some scholars further pointed out that the scope of "important data" in China's "Data Exit Security Assessment Measures" is unclear, the burden of risk self-assessment is too heavy, and the evaluation procedure is lengthy, which may lead to conflicts between China and international rules such as CPTPP, but justification can be sought through exception clauses [5]. From the perspective of enterprises, some scholars point out that rule conflicts lead to the serious "two-way compliance" dilemma of "going out" and "introducing" enterprises, increasing operating costs and legal risks [4].

In the discussion of key provisions, the relevant research mainly focuses on the interpretation of the "Basic Safety Exception Clauses" in RCEP. Most scholars pointed out that the clause has the problem of ambiguity of key concepts and gives the party the right to self-adjudication. Although it provides a legal basis for China's implementation of data localization measures, it still needs to be bound by the "goodwill principle" and also requires a "minimum correlation" between the measures and security interests. This ambiguity leads to uncertainty in compliance practice and brings compliance obstacles to enterprises [6].

In terms of coping strategies, most scholars have formed a consensus that internal agreements and external initiatives should go hand in hand. Externally, scholars emphasize that people should actively participate in the formulation of international rules, enhance the institutional right to speak, and vigorously promote the formation of a more inclusive situation of pluralistic co-governance [2]. Internally, people should first improve the domestic rule of law guarantee, including fine data classification to clarify the scope of the important concept of "important data", and learn from the United States, the European Union, and other countries to establish independent regulatory agencies, optimize security assessment procedures, and build a unified governance system to solve the problem of legal fragmentation [4].

Overall, the existing research has clarified the conflict between international obligations and domestic rules and provided direction for China's approach. However, how to form a more operational and concrete compliance path between adhering to basic national security and connecting high standards of international rules still needs to be further studied.

3. The Practical Challenges of China's Data Regulation in Aligning with RCEP Rules

3.1. Conflict Dilemma at the Rule Level

The primary challenge in aligning China's data regulations with RCEP rules lies in the fundamental institutional tension between the broad interpretation of RCEP security exception clauses and the mandatory requirements for China's data export security assessment. Article 15 (3) of Chapter 12 of RCEP provides for a "fundamental security exception clause" that allows contracting parties to take measures they deem necessary to protect their fundamental security interests. However, the two core concepts of "basic security interests" and "they think it is necessary" are not clearly defined in the agreement, which gives the contracting parties more room for independent interpretation [6]. At the same time, according to the Data Security Law and relevant supporting regulations, China has established a data exit control system based on security assessment, requiring that important data collected and generated during operations in China should be stored in China in principle. If it is really necessary to provide it overseas, it should pass the security assessment organized by the national network information department. This creates fundamental institutional tension: on the one hand, RCEP tends to promote the free flow of data, and the broad interpretation of its security exception clauses may be used in a more relaxed regulatory environment; On the other hand, China's current system emphasizes security priority and sets rigid pre-examination requirements for data export.

Behind data sovereignty is a practical issue: whoever controls the core nodes of global data flow has the potential to influence or even threaten the security of other countries by controlling data. Farrell and Newman's research suggests that countries occupying the core nodes of the network can use their structural advantages to monitor or block other countries, which explains why China adheres to a security-first stance in data flow regulation [7]. Gao summarized this different value orientation into three modes. China stands for the "national sovereignty" mode, and its core is security priority, which is in sharp contrast with the modes of the United States and the European Union [8]. RCEP tends to reserve a large policy space for member countries in design, and its definition of "basic security interests" clearly covers key public infrastructure such as communications and electricity, which provides a basis for China to invoke security exception clauses when docking RCEP rules [9]. However, the underlying logic of RCEP is free flow priority, and security exceptions are only exceptions. However, the basic principle of the current system in China is safety first, and free movement is subject to safety assessment.

3.2. The Dilemma of Missing Positions in Mechanism Design

First of all, the most important thing is that the scope of "important data" is unknown. Although China's Data Security Law has established an important data protection system and clearly proposed the establishment of a data classification and grading protection system in Article 21, the definition of "important data" has only made principled provisions, and a unified national catalogue of important data has not been issued so far. There are differences in the identification standards of important data in the competent departments of various industries, such as the identification of customer transaction data in the financial field, the division of health and medical data in the medical field, the definition of infrastructure operation data in the energy field, etc., which lack unified norms. This unclear scope also makes it difficult for enterprises to accurately judge whether the data they process is important data in practice, and then it is impossible to determine whether it is necessary to declare a security assessment for the data.. Enterprises either dare not carry out cross-border business normally because of excessive caution, or face the risk of violation due to misjudgment, and the uncertainty of compliance increases significantly.

Another important flaw is the lack of a facilitation mechanism. The current data exit security assessment system does not clearly stipulate the validity period of the assessment results. In practice, after an enterprise completes a security assessment, if it needs to carry out cross-border business for

a long time, it often needs to face problems such as duplicate applications and repeated evaluations. This not only increases the compliance cost of enterprises, but also has a certain gap with the free flow of data advocated by RCEP [4]. RCEP is relatively binding on the free flow of data, which not only provides policy flexibility for member states but also increases the uncertainty of corporate compliance [9]. The degree of institutionalization of data flow rules directly affects the compliance expectations of enterprises, and the lack of a clear facilitation mechanism will increase the uncertainty of cross-border business [10]. Especially under the RCEP framework, trade between member countries is frequent, and the cross-border data flow of enterprises is characterized by continuity and a long-term nature. The lack of a protection mechanism to facilitate the long-term stable data exit has put enterprises in a dilemma between fulfilling international obligations and complying with domestic regulations.

Finally, the supervision and coordination of various departments are insufficient. The supervision of data outbound involves many competent departments, including the national network information department, the industry and information technology department, the public security department and the competent departments of various industries. At present, there is a cross-overlap in the regulatory responsibilities of various departments, and the regulatory standards cannot be unified as much as possible. Enterprises often need to make multiple declarations and be reviewed repeatedly when handling data outbound business, and the communication and time costs have increased significantly. The lack of a regulatory coordination mechanism affects the compliance efficiency of enterprises.

4. Institutional Improvement of China's Data Regulation Integration with RCEP Rules and the Response of Enterprisess

4.1. National-Level Institutional Improvement

The country should promote consensus on the interpretation of RCEP security exception clauses. To alleviate the conflict dilemma at the level of rules, China can actively rely on regional cooperation platforms such as the RCEP Joint Committee and work with ASEAN and other contracting parties to jointly promote the interpretation and consensus of the "basic security interests" clause. Through a multilateral dialogue mechanism, the applicable boundary of security exception measures should be clarified, so as to prevent individual member States from abusing security exception clauses to hinder normal data flow, and at the same time ensure that member States enjoy the necessary space in safeguarding national security [9].

The government should make clear the lead department of data exit and establish an inter-departmental coordination mechanism. In order to solve the problem of insufficient supervision coordination, it is suggested that the national network information department should be the lead unit in the supervision of cross-border data flow, establish a cooperation mechanism between the network information department, the industrial information department, and the public security department, and unify the supervision standards and review process. By establishing a "one-stop" reporting window and information sharing platform, people can provide more convenient compliance services for enterprises and effectively reduce the communication cost brought by multi-head law enforcement.

Relevant departments should improve the dynamic adjustment mechanism of important data catalogs. To solve the problem of the unclear scope of "important data", it is recommended to quickly introduce a unified national identification standard for important data, and the competent departments of various industries should formulate a special catalog of important data in their respective fields in accordance with the Data Security Law. At the same time, establish a dynamic adjustment mechanism for the directory, update it in a timely manner according to technological development, security situation, and changes in international rules, to ensure the scientific and timely scope of important data.

4.2. Corporate Compliance Response Strategies

Enterprise should construct a reasonable internal data compliance system. Enterprises should set up a special data compliance department, systematically sort out the cross-border data categories involved in their own business, draw up a data classification and grading list, and cross-border transmission process according to the standard RCEP rules and Chinese legislation. By establishing a normalized compliance training mechanism, people will enhance the awareness of data compliance of all employees and embed compliance requirements into business processes.

All departments should strengthen communication and feedback with the regulatory authorities and promote system optimization. Enterprises should establish regular communication channels with regulatory authorities and provide timely feedback on outstanding problems encountered in compliance practice, such as a vague definition of important data and complicated evaluation procedures. Through industry associations and other platforms, people can reflect the demands of enterprises, promote the improvement of the system, and form a governance pattern of benign interaction between government and enterprises.

Enterprises should actively apply for compliance certification. Enterprises should actively connect with the domestic data exit facilitation mechanism and take the initiative to apply for "one-time assessment" or "green channel" qualification. Reduce the cost of repeated evaluation through compliance certification, improve the efficiency of cross-border data flow, and win institutional convenience for participating in international competition.

5. Conclusion

Against the background of the coexistence of the globalization of digital trade and the game of digital sovereignty, China's data security assessment mechanism and the RCEP data cross-border flow mechanism present a complex situation of tension and mutual coordination. This study focuses on the institutional conflict in the process of docking between the two and the dilemma of Chinese enterprise compliance and explores a feasible path to find a balance between maintaining national security, promoting the free flow of data, and protecting enterprise trade.

The study found that there is a double dilemma between China's data regulation and RCEP regulation: first, the conflict dilemma at the rule level, and there is tension at the rule level between the broad interpretation of basic security exceptions and the rigid requirements of China's data control; second, the gap dilemma of mechanism design, specifically manifested in the "important data" model The encirclement is unknown, the validity period of the safety assessment results is short, the supervision of long-term law enforcement, and the existing system has not established a protection mechanism to facilitate the exit of long-term stability data. The deep-root cause of the above dilemma lies in the institutional conflict between data sovereignty and trade liberalization in the field of cross-border data flow.

In response to the above difficulties, this study puts forward a response plan from the national and enterprise levels. At the national level, people should promote the consensus on the interpretation of RCEP security exceptions, rely on the RCEP Joint Committee and ASEAN and other parties to clarify the definition standards of "basic security interests"; clarify the leading departments of data exit, and establish a cross-departmental coordination mechanism for network information, industry and information, public security and other departments; accelerate the introduction of national unified First, the important data identification standard is to establish a dynamic adjustment mechanism for the catalogue. At the enterprise level, people should build an internal data compliance system, set up a special data compliance department, formulate a data classification list and cross-border transmission process; strengthen communication and feedback with regulatory departments, and centrally reflect the demands of enterprises through industry associations; take the initiative to apply for compliance certification, strive for "one-time evaluation" qualifications, and reduce duplication compliance costs.

In the future, China's cross-border data flow system needs to be continuously optimized in the background of parallel development and security. On the one hand, with the help of regional cooperation platforms such as RCEP, people will continue to improve the practical understanding and application of basic security interest clauses. On the other hand, the improvement of the domestic system should focus on the refinement of the "important data" catalogue, the rationalization of the evaluation procedure, and the coordination of the supervision system. Only by finding a balance between adhering to international rules and adhering to the bottom line of security can people provide a stable and predictable guarantee of the rule of law for Chinese enterprises to participate in global digital competition.

References

[1] Hui Zhaobin. Risk management of cross-border data flow for enterprises in the era of data economy. Social Sciences Academic Press, 2018: 102-107.

[2] Feng Jinhui, Zhou Meng, et al. Regulation of cross-border data flows: Core issues, international schemes, and China's responses. Journal of Shenzhen University (Humanities and Social Sciences Edition), 2021, 38(4): 88-97.

[3] Hong Zhanggui, Huo Jianxing, et al. Regulation of cross-border data flows under RCEP and its significant impacts. Southwest Finance, 2022, (4): 83-94.

[4] Xu Duoqi. On the legal safeguards for enterprises' two-way compliance in cross-border data flow regulation. Eastern Journal of Law, 2020, (2): 185-197.

[5] Liu Junchao. China's security assessment measures for outbound data transfers. Journal of East Asia and International Law, 2023, 16(2): 267-282.

[6] Guo Duanxi. Study on the application of the basic security exceptions for cross-border data flows under RCEP. Contemporary Law Review, 2025, 39(4): 149-160.

[7] Andrew D. Mitchell, Neha Mishra, et al. Data security and trade agreements: The security exceptions. World Trade Review, 2023, 22(2): 201-218.

[8] Gao Henry. Data sovereignty and trade agreements: Three digital kingdoms. In: Anupam Chander, Haochen Sun, Eds. Data sovereignty: From the digital Silk Road to the return of the state. Oxford University Press, 2021: 213-239.

[9] Andrew D. Mitchell, Vrinda Gyanchandani, et al. Convergence & divergence in digital trade regulation: A comparative analysis of CP-TPP, RCEP, and EJSI. South Carolina Journal of International Law and Business, 2023, 19(2): 98-150.

[10] Mira Burri. Data flows and global trade law. In: Mira Burri, Ed. Big data and global trade law. Cambridge University Press, 2021: 1-44.