

RCEP Basic Security Exceptions for Cross-Border Data Flows and China's Response

Chengyu Zhang

School of law, Anhui University of Finance and Economics, Bengbu 233030, China

17865276448@163.com

Abstract. With the booming development of digital economy, the cross-border activities of data are becoming more and more frequent. At present, data has become an important national strategic resource in the information age. Rational data flow plays an important role in promoting economic growth, accelerating innovation and facilitating globalization. The current global cross-border data flow regulatory system is in a critical period of formation. In the context of the continuous improvement of the current rules system at the regional level, the Regional Comprehensive Economic Partnership Agreement (RCEP), as an important regional free trade area agreement (FTA), has made new provisions on the cross-border flow of data, and the regional data flow rules represented by RCEP profoundly reflect that the rules of global cross-border data flow should not be completely dominated and formulated by developed economies, and all kinds of sovereign countries. All kinds of sovereign countries should have the right to participate and the right to speak in the system. The regulation of global data cross-border flows in the digital economy is not only motivated by economic interests, but more importantly, by the protection of national interests. Therefore, under the current data governance system, China should use RCEP as an external driving force to revise and improve the relevant domestic rules on cross-border data flows, so as to promote the benign development of the data governance system, accelerate the promotion of the free flow of data across borders, strengthen cooperation with the international community, continuously expand the intersection of rules on cross-border data flows, achieve convergence of rules, and promote the Chinese solution for the governance of cross-border data flows.

Keywords: RCEP; Cross-border data flow; Basic security exception clause.

1. Introduction

Based on the importance of digital economy and the infringement of national security and personal privacy in the process of data flow, the Regional Comprehensive Economic Partnership Agreement (RCEP) has made new provisions on cross-border data flow, which advocates the free flow of data across borders while setting "public policy objectives" and "fundamental security interests" exceptions. The RCEP provides for a "public policy objectives" and "essential security interests" exception to the free flow of data across borders. However, the scope and application criteria of the exception clause are not clear in RCEP, so there is uncertainty in its application. Moreover, China's current regulation of cross-border data flow emphasizes the maintenance of data security, which is inconsistent with the principle of free flow of data across borders under RCEP. In order to ensure the correct application of RCEP's cross-border data flow exception clause in the future, to realize the supervision and management of cross-border data flow based on the protection of vital national security interests, to strengthen the convergence with RCEP and other international rules, to enhance the level of domestic protection of cross-border data flow, and to promote the construction of unified, fair and orderly security rules for cross-border data flow is really an urgent task for China.

2. Background of RCEP Rules on Cross-border Flow of Data into the Treaty

When the RCEP was first negotiated, the cross-border flow of data was not included as a key issue, but with the rapid development of digital trade around the world, the need to include relevant rules in the RCEP has come to the fore. In terms of overall development trend, more and more countries are placing data cross-border flow provisions in bilateral or regional FTAs. The cross-border flow of data

is an important element of digital trade, but while it makes a significant contribution to global economic growth, it also raises various issues and risks. Based on policy concerns such as safeguarding national security and protecting personal privacy, maintaining public morality and public order, preventing consumer fraud, facilitating domestic law enforcement, and promoting the development of domestic industries, countries have adopted data localization measures to restrict the flow of data across borders. However, traditional economic and trade agreements such as WTO agreements lack clear rules on cross-border data flows, making it difficult to effectively regulate parties to take measures to restrict the free flow of data across borders or data localization. In order to promote further free flow of data globally, regional economic and trade agreements such as CPTPP have started to set digital trade rules to regulate parties' adoption or maintenance of measures affecting digital trade, which to a certain extent solves the problem of applying rules related to cross-border flow of data. In terms of practical needs, RCEP parties urgently need a new comprehensive, modern, high-quality, and mutually beneficial FTA to meet the development needs of their own digital economy. The Digital Economy Report 2021, published by the United Nations Conference on Trade and Development, notes that the dramatic growth in data flows is geographically concentrated between North America and Europe and between North America and Asia, but that a deep traditional digital divide still exists between the vast majority of countries. The United States and China lead the world in digital economy, with half of the world's hyperscale data centers located in these two countries. The ASEAN countries are lagging behind in terms of overall digital economy development, but ASEAN has a deep potential to develop a digital economy, with a large potential digital economy and the fastest growing Internet user base in the world; it is expected to reach \$30 billion by 2025, accounting for about 8% of ASEAN's GDP. For technical and market considerations, the Asian region also needs a high-quality FTA to regulate the cross-border flow of data and promote the sound development of the digital economy. Therefore, based on the overall trend of global economic and trade agreements and the actual needs of the development of the digital economy in the Asia-Pacific region, the negotiating parties included the issue of cross-border data flows in the RCEP e-commerce negotiations and finally reached a consensus.

3. The general rules of RCEP data cross-border flow rules

The development of communication and information technology has become increasingly sophisticated, and the heavy obstacles in the post-epidemic era have forced a shift in the realization path of trade in services. Thanks to the maturity of digital technology, e-commerce has become an important circulation method in international trade, which can not only promote the development of online trade, but also promote the transformation and innovation of business models and consumption behavior between regions, and promote rapid economic development. The relevant provisions are mainly embodied in Chapter 12 of the agreement, the section of "Electronic Commerce". This chapter contains 17 specific provisions, which provide for a series of measures to facilitate the cross-border flow of data, covering provisions related to the protection of individual rights and interests in the cross-border flow of data, and the parties have also reached consensus on key core issues such as cross-border information and data flow and local storage of data, as well as setting up a dialogue mechanism and dispute settlement mechanism for cross-border data flow. The consensus reached on these important contents has laid the foundation for further deepening the cooperation among countries in the field of e-commerce and provided institutional guarantee for establishing a favorable environment for the development of e-commerce, which has strongly promoted the development of e-commerce among regions.

RCEP's rules on cross-border data flow are mainly distributed in Chapter 8 "Trade in Services" and Chapter 12 "Electronic Commerce". Due to the large number of member countries covered and the large differences in the level and scale of development of digital economy, RCEP, with an open attitude and from the perspective of maximizing benefits, fully respects and accommodates the laws and policies of member countries, and has formulated provisions that allow the free flow of data

across borders and restrict data localization, i.e., the principle of free and secure flow of data, and takes "free flow of data" as the fundamental principle. "The RCEP does not impose mandatory obligations on member countries, but essentially embodies a concept of openness and inclusiveness, thus achieving the effect of shared governance. The balance chosen is between Europe and the United States, not just restricting the flow of data to protect personal privacy, nor just pursuing the economic benefits brought by the free flow of data, but focusing on the secure cross-border flow of data, balancing data protection and free flow.

Chapter 12 of the RCEP, "Electronic Commerce," begins with a statement of the importance of electronic commerce and sets as its primary goal "to promote electronic commerce among Parties and the wider use of electronic commerce on a global scale. Under this principle and objective, Article 15(1) first recognizes that Parties may have their own regulatory requirements for the transmission of information by electronic means, while paragraph 2 provides that "a Party shall not prevent the electronic cross-border transmission of information by a covered person for the purpose of conducting business." This provision does not specify the type of "data," and thus may include both personal and non-personal information. In addition, the cross-border flow of data regulated here includes only the purpose of "commercial conduct"; cross-border flows of data led by government or judicial authorities (e.g., cross-border forensics) are not regulated by this provision. The above two paragraphs indicate that the parties shall not restrict the cross-border transfer of data and shall follow the principle of free flow. This is also the core obligation set by RCEP for member countries. Although RCEP does not provide a clear definition of whether electronically transmitted information contains personal information, the principle of free flow of data across borders established by it follows the trend of development of cross-border data flow rules in the new generation of free trade agreements.

4. Basic Security Exceptions to RCEP's Data Cross-Border Flow Rules

The exception principle of data cross-border flow established by RCEP is essentially a conditional restriction on data localization storage, i.e. data transmission restriction requirement, which imposes certain conditions on data flowing across borders under some specific circumstances. The implementation of localized data storage mainly stems from the traditional territorial protectionism, and each RCEP member country has different national conditions and development status, and different legal policies in implementing data localization, and the degree of localized data storage also varies. The degree of localized data storage can be divided into the following three categories: first, there is no data localization requirement; second, a copy of the data must be stored in the territory before the relevant act can transmit and process the data outside the territory, which is mainly for telecommunications metadata and business financial data, usually to ensure regulatory needs; third, the data can only be accessed, stored and processed in the territory and is strictly prohibited from leaving the country. The RCEP fully respects the development and regulatory differences of different countries by allowing the free flow of data while making exceptions for the secure flow, which is unprecedented in previous e-commerce agreements.

While Article 15(2) of the RCEP prohibits in principle restrictions on the free flow of data across borders, paragraph 3 of the RCEP provides for two exceptions to balance this, namely the "public policy objectives exception" and the "essential security interests exception". Paragraph 3 provides that a Party may adopt or maintain: "(i) any measure that is inconsistent with paragraph 2 but that the Party considers necessary to achieve its legitimate public policy objectives, provided that the measure is not applied in a manner that constitutes arbitrary or unjustifiable discrimination or a disguised restriction on trade; or (ii) any measure that the Party considers necessary to protect its essential security interests. Such measures may not be challenged by other Parties." The two exceptions confer greater self-rule on the parties.

First, with respect to the public policy objectives exception, the article does not specify the specific content of the objectives, effectively allowing a country to pursue additional objectives, such as the "data sovereignty objective," for its data cross-border flow regulation measures, thereby granting

greater discretion to the parties. In addition, the RCEP specifically states after the first "necessary measures" that "Parties recognize that the need to implement such legitimate public policy shall be determined by the Party implementing it", thus emphasizing the "self-judgment" nature of the public policy objective exception. This emphasizes the "self-adjudicative" nature of the public policy objective exception and increases the likelihood that a Party will successfully invoke the exception to prove the legality of the measure at issue.

Second, with respect to the essential security interest exception, RCEP does not strictly limit the exception to the circumstances listed in the article, as in Article 21 of the GATT and Article 14 bis of the GATS, but adopts an open-ended approach, fully guaranteeing the regulatory autonomy of the parties. It can be seen through the above provisions that RCEP takes into account the security of data flow and makes exceptions, such as a contracting party may take necessary measures to restrict data flow in order to safeguard the basic security interests of the country or to protect public policy objectives, and the necessary measures shall be decided by the country from which the data flows, and other contracting parties shall not raise any objection to such measures. In other words, a Party may take measures such as restricting data out of the country and implementing localized storage in order to achieve legitimate public policy objectives or to protect the basic security interests of the country, as well as to protect users' personal information. As can be seen, the RCEP parties still take security as the primary principle, which not only gives the parties a certain degree of discretion in taking measures, but also emphasizes respect for data sovereignty and network sovereignty of the country where the data is located, as well as the autonomy of each member state in data governance, and the financial regulators of the parties have the regulatory power to store data and retain copies of records, provided that they comply with the relevant obligations. It should be noted that the security exception clause is a special institutional arrangement that allows contracting parties to be exempted from obligations under free trade agreements in order to maintain national security and public policy objectives, but the RCEP only provides a general description of the meaning of "fundamental security interests" and "public policy objectives. However, RCEP has only made a general statement on the meaning of "basic security interests" and "public policy objectives" without clear and definite explanation, which is vague and discretionary, making it a "dynamic" rule of international law, which requires member states to exercise discretion based on the principle of goodwill; in addition, RCEP takes into account the differences in the development of member states, which is conducive to achieving the dual objectives of cross-border data flow and digital trade development. In addition, RCEP takes into account the differences in the development of each member country, which is conducive to achieving the dual objectives of cross-border data flow and digital trade development, and reduces the conflicts between the domestic laws of each member country and RCEP rules to achieve compatibility between them.

In summary, RCEP expands the regulatory space for cross-border data flows by emphasizing the self-judgment attribute of the public policy objective exception and adding the fundamental security interest exception, allowing parties to adopt more regulatory measures for cross-border flows to protect individual interests, public interests and national security. However, the scope and application criteria of "public policy objectives" and "essential security interests" are not clear in the exceptions to the RCEP data flow rules, which may lead to disputes in the process of treaty implementation. Therefore, who and how to judge and interpret the scope and conditions of application of the exceptions is the key to whether the parties can successfully invoke the exceptions to exempt the free flow of data across borders.

5. Measures for the Convergence of China and RCEP Cross-border Data Flow Exceptions

5.1 Current status of legislation on the regulation of cross-border data flow

In the era of digital economy, the scale of data in China is growing rapidly, the significance of data to economic development, people's life, national and social governance is becoming increasingly

important, and China is paying more and more attention to the legal regulation of cross-border flow of data. Since the adoption of the Cybersecurity Law in 2016, China has further strengthened its domestic regulation and legislation on cross-border data flows. After joining RCEP, China should first consider the convergence of relevant regulatory measures with RCEP rules on data cross-border flow.

In the field of cross-border data flow, China has initially formed a system of data cross-border flow regulation with the Network Security Law, Data Security Law and Personal Information Protection Law as the core and special regulations in key areas. As the basic law of China's cyberspace governance, the Cybersecurity Law regulates the cross-border flow of data at the legal level for the first time.

Article 37 of the law provides that "operators of critical information infrastructures in the People's Republic of China operations collected and generated in the personal information and important data should be stored in the territory. For business needs, it is necessary to provide outside the country, should be in accordance with the national network information department in conjunction with the relevant departments of the State Council to develop a security assessment; laws and administrative regulations otherwise provided, in accordance with its provisions." The "Data Security Law" passed on June 10, 2021 further regulates the rules of cross-border data flow, indicating that China's promotion of the safe and free flow of data across borders. The law provides that Article 31 of the law provides that "the outbound security management of important data collected and generated by operators of critical information infrastructures in their operations in the People's Republic of China shall be governed by the provisions of the Network Security Law of the People's Republic of China; the outbound security management of important data collected and generated by other data processors in their operations in the People's Republic of China shall be governed by the State Network Information department in conjunction with the relevant departments of the State Council." This article of the Data Security Law clarifies the important data exit management system and also provides a legislative basis for further regulation of important data exit in other areas.

In China's practice, the concept of "other fields" is mostly found in administrative regulations and departmental rules, such as Article 34 of the Map Management Regulations, which stipulates that Internet map service units shall locate servers for map data in China and develop a security management system and safeguard measures for Internet map data. Article 24 of the Credit Industry Regulations also states that "the collation, preservation and processing of information collected by credit agencies within China shall be conducted within China." Article 7 of the Network Security Review Measures requires that "operators with personal information of more than one million users who go public abroad must declare their network security review to the Network Security Review Office." Article 21 of the "Automotive Data Security Management Provisions (for Trial Implementation)" also requires that automotive data processors should be "important data should be stored within the territory in accordance with the law, and business needs do need to be provided outside the country, should pass the security assessment organized by the State Network Information Department in conjunction with the relevant departments of the State Council." Given the important role of cross-border flow of personal information data in the development of the digital economy, the Personal Information Protection Law, adopted on August 20, 2021, establishes a special chapter to regulate the cross-border flow of personal information and protect the rights and interests of personal information. Article 38 stipulates that if a personal information processor provides personal information abroad for business and other needs, it shall pass the security assessment of the state Internet information department, be certified by a professional institution for personal information protection, or clarify the rights and obligations of the overseas recipient in accordance with a standard contract formulated by the state Internet information department. Article 39 stipulates that if a personal information processor provides personal information abroad, it shall inform the individual about the information leaving the country and obtain his or her "separate consent". Article 40 stipulates that operators of critical information infrastructures and personal information processors that handle personal information up to the amount prescribed by the state network information

department shall store personal information collected and generated in China within the territory; if it is necessary to provide it outside the country, it shall pass the security assessment organized by the network information department, unless the law, administrative regulations and the state network information department stipulate otherwise. In general, the Personal Information Protection Law distinguishes between ordinary personal information processors, operators of critical information infrastructure and operators of personal information that process personal information up to a certain amount, puts forward special requirements for data localization and outbound security assessment for the latter two, and specifies the requirements to be met by ordinary personal information processors to transmit personal information outside of China.

The above provisions can be found in several of China's laws, regulations and departmental rules that address China's right to regulate the cross-border flow of data. Although the principle of safe and free cross-border data flow has been established, important data domestic storage and outbound security assessment have been emphasized, so overall China's current stage of data cross-border flow regulation focuses more on maintaining data security, especially national security issues, and the legislative attitude is more conservative and prudent. Therefore, the existing data cross-border flow regulation measures are inconsistent with the principle free flow of data implemented by RCEP across borders. The legitimacy of the regulatory free flow measures adopted or maintained by China under RCEP should be based on the ability to invoke the RCEP exceptions.

5.2 Strategies for Linking China and RCEP Cross border Data Flow Exception Provisions

How to balance the cross-border data flow and national data security is a problem that countries all over the world are trying to solve. China should base on its national conditions, follow the development trend of cross-border digital trade, and adapt to the relevant requirements of international rules, including the economic and trade agreements to which it has acceded, on the premise of ensuring that the relevant agencies have sufficient regulatory capacity for data cross-border. Under the RCEP agreement, China should shape the concept of coordinating data security and promoting flow, unify relevant concepts and establish important data catalogs internally, expand legal data exit channels and strengthen regional cooperation externally, and promote the improvement of rules for cross-border data flow.

5.2.1. Shaping the concept of data security and promoting the flow of rules

"If law is a painting, then its base color must be the right to freedom." The reshaping of the concept of China's data cross-border flow rules can try the regulation model of "principle + exception", that is, the principle of free flow of data across the border and the prohibition of localization of data storage, and the exception of the realization of legitimate public policy objectives and the need to protect basic security interests, to restrict the flow of data across the border and the requirement of localization of data storage.

On the one hand, the rules of cross-border data flow in China should be based on the principles of free flow of data across borders and prohibition of localization of data storage, so as to manifest the concept of rules to promote the flow. First, the establishment of the principle of free flow of data across borders needs to interact with Article 15(2) of Chapter 12 of the RCEP Agreement. This provision emphasizes that data cross-border conduct as a result of commercial conduct shall not be prevented, and its elements include two parts, namely, commercial conduct and data cross-border conduct. Therefore, in the design of the provision, China can consider the principle of "general network operators may provide relevant commercial data information to foreign countries for commercial purposes" to establish the principle of free flow of data across borders. Secondly, the requirement of prohibiting localization of data storage also needs to interact with Article 14(2) of Chapter 12 of the RCEP Agreement, i.e., "data information collected and generated by general network operators may be stored outside of China" to establish the principle of prohibiting localization of data storage. The establishment of the two principles will enhance the alignment of China's data flow rules with the RCEP Agreement and shape the concept of China's data flow rules to facilitate the flow.

On the other hand, China's data cross-border flow rules also need to restrict the cross-border flow of data with the exception of the need to achieve legitimate public policy objectives and to protect basic security interests, and to propose data storage localization requirements. China's Cybersecurity Law proposes that critical data of critical information infrastructures should be stored locally, and also proposes the requirement of security assessment. For what is critical information infrastructure, combined with the RCEP Agreement, Chapter 12, Article 14, paragraph 3 and Chapter 12, Article 15, paragraph 3 to review this, China should focus on "based on the achievement of legitimate public policy objectives, and the need to protect the basic security interests of the parties", rather than directly enumerate the relevant industries. This can be fully dovetailed with the RCEP agreement, but also to avoid criticism by other countries. In general, China's existing legal provisions, after appropriate improvement and complementary, can well cope with the requirements of the "exception" norms. In addition, if the restriction of cross-border data transfer is to maintain constitutional values, it should not be regarded as data protectionism in general. The localization of data storage in China is a fundamental value established by the Constitution, such as national security, and should be covered by the "exception". On this basis, the exception is necessary to achieve legitimate public policy goals and to protect basic security interests, which will effectively establish the concept of the rule that we value data security.

5.2.2. Unification of related concepts and establishment of important data catalog

Combined with the interpretation and practice of the exception clauses of WTO series agreements, China's measure of "localization of data storage + exit security assessment" to restrict data exit can basically be supported by the exceptions of basic security interests and public policy objectives of RCEP agreement. However, due to the sensitivity and natural uncertainty of data control measures, the implementation process is prone to ambiguity and disputes, so it is necessary to clarify and unify the concept internally and provide domestic law guidelines for the interpretation of related disputes. Exceptions to public policy objectives require flexibility in the relevant measures, and need to improve the relevant measures based on the data classification system and the important data catalog as a means to improve the relevant measures.

On the one hand, when the measures of China's data flow rules are challenged by other countries and resorted to RCEP dispute settlement, the RCEP Joint Committee or expert group will review the relevant measures to determine whether they are in compliance with the exceptions of the RCEP agreement. Establishing the link between the relevant measures and the exceptions relies on the interpretation and reasoning of the relevant legal concepts to reach a relatively consistent understanding and application. "A legal concept is an authoritative category formed by generalizing various legal implementations and abstracting their common features." Among the measures to regulate the cross-border flow of data, the Cybersecurity Law requires the localized storage of information generated by critical information infrastructures based on the concepts of "national security, national livelihood and public interest", which can be included in the categories of "basic security interests" and "public policy objectives". "Public policy objectives". The Data Security Law emphasizes "the development of international rules and standards related to data security" and proposes "the establishment of a data security review system" on this basis, while the Personal Information Protection Law stipulates that personal information leaving the country In the Personal Information Protection Law, "security assessment shall be conducted". It can be seen that within the rules of China's cross-border data flow, there is already a situation of inconsistency in the relevant legal concepts. The exceptions to the RCEP agreement for cross-border data flows are limited to "essential security interests" and "legitimate public policy objectives". If the Joint Committee or the Expert Group reviews China's invocation of the "fundamental security interest exception" and the "public policy objective exception," it will inevitably examine the definition and application of the relevant legal concepts in China's domestic law. In this regard, the legal concept of measures to restrict data exit in China should be unified with the expression of the RCEP agreement, and the measures and systems to restrict the cross-border flow of data should be constructed on the grounds of "fundamental security interests" and "public policy objectives". At the same time, the relationship

between "data security review" and "exit security assessment" should be clarified, so as to clarify the security assessment as a specific review measure for data exit, and thus build internal rules to meet the requirements of the RCEP Agreement's data cross-border flow framework.

On the other hand, a sound catalog of important data can help clarify the application of cross-border security assessment and related alternative measures. The Data Security Law, on the other hand, establishes a "top-down" hierarchical protection system based on the value of data to the state and society and the consequences of harm caused by security incidents, with the State as the main body. However, the definition of important data is still determined by the source subject. Since important data is naturally linked to basic security interests and has dynamic and evolutionary characteristics, its connotation criteria, determination conditions, and determination procedures are not suitable to adopt a relatively fixed definition. In this regard, China can adopt the "important data catalog" proposed by the Data Security Law, which includes data vital to national security and social public interest, and control them in combination with data storage localization and exit security assessment, so as to improve the operability and transparency of China's data cross-border flow rules. At the same time, the "Important Data Catalogue" should be regularly updated to meet the needs of data cross-border and national security for economic and trade development in the RCEP region.

5.2.3. Expanding Channels for Legal Data Exit and Regional Cooperation

RCEP, as an advocacy agreement to promote the development of cross-border e-commerce in the Asia-Pacific region, is committed to reaching widely applicable e-commerce rules in the Asia-Pacific region. China is relatively absent in the international participation of data cross-border flow, and is more concerned about data protection and security issues. China should actively promote RCEP parties to collaborate in the governance of cross-border data flows, and externally promote the landing of richer channels for legal data exit and regional cooperation.

China's existing data legal exit channels are all adequate safeguards, of which personal information protection certification by professional organizations can be expanded to a third-party certification mechanism for data security certification. Third-party certification is to prove the safety and reliability of the information network by proving that network services, data products, management systems, etc. comply with the relevant legal norms, technical standards, industry guidelines assessment by certification bodies. In terms of personal information protection certification for data exit, China can actively construct personal information data exit relying on third-party data security certification, and guarantee the safety and compliance of personal information data exit through this measure. In terms of the construction of the standard contract, China's "Personal Information Exit Standard Contract Provisions (Draft for Comments)" has been introduced in 2022, the draft clarifies the data security protection responsibilities and obligations that the data exit implementation subject and the recipient subject should take the initiative to adopt, and the next step is that China should actively promote the introduction of this assessment method as soon as possible. On the basis of the above two improvements, China can also increase the channel of binding group enterprise rules. This rule is derived from the EU BCR rules, which means that the data exporter and receiver belong to the same group, although the data flow across national borders, but the group as a whole follow the rules of China's data flow across borders, then the whole group can be regarded as a "safe harbor", general commercial data can flow freely across borders without security assessment. China can actively learn from and incorporate the adequacy safeguards to improve the legal exit of data, and gradually promote them through pilot projects to accumulate experience in cross-border transmission of specific types of data.

In addition to the adequacy safeguards, China can actively carry out intra-regional cooperation in RCEP and establish a regional whitelist mechanism for cross-border data flow. The whitelist mechanism refers to assessing the political and legal links of data outbound and inbound countries, and if their data protection level meets the minimum requirements of data outbound and outbound countries, the data cross-border behavior is legal and transparent, and there are no negative reports about data cross-border flow, the data outbound and inbound countries can be included in the countries with free flow, forming a whitelist of data cross-border flow. As there are both developed

and developing countries in the RCEP region, the level of data security protection varies greatly from country to country. Therefore, China can make use of the RCEP platform to negotiate with developed countries such as Japan and Australia on the cross-border flow of data first, balance the data security protection level of each country, reach a minimum level of data protection, and establish a whitelist mechanism for the cross-border flow of data in the RCEP region. The developing countries in the region can also join the consultation and deliberation to promote the free and secure flow of data across borders in the RCEP region after they have continuously improved their own data security protection level. Of course, the whitelist mechanism for cross-border data flow is not static, and China can promote the RCEP member countries to hold regular reviews and remove from the whitelist those countries that no longer meet the minimum level of data protection, so as to guarantee the safety and reliability of the whitelist mechanism for cross-border data flow in the RCEP region. Adequacy safeguards, whitelist mechanism and security assessment are not clear-cut states, and the national network information department should enjoy the power to assess and restrict the cases of cross-border data flow that meet the adequacy safeguards and whitelist mechanism on the premise that security risks exist in the implementation process, and effectively guarantee the realization of data security while continuously expanding data outbound and regional cooperation.

To sum up, the improvement path of China's data cross-border flow rules under RCEP agreement mainly starts from three aspects: First, the "principles + exceptions" regulatory model, shaping the concept of China's rules that attach importance to security and promote the flow. Second, the internal unification of relevant legal concepts, so that China's measures to restrict the flow of data to better align with the RCEP agreement, the establishment of an important data directory to enhance the operability and transparency of measures. Third, the external improvement of the adequacy of the security measures and white list mechanism to expand the channels of data exit and regional cooperation.

6. Conclusion

In the context of rapid development of digital economy, the rules of cross-border data flow have become an important element of national participation in global data governance, and the concept of cooperative governance reflected by RCEP will lead the pursuit of global data governance values, which is a breakthrough and innovation to the existing regulatory pattern and also provides a brand-new idea to the negotiation of WTO related rules. In addition, the signing and entry into force of RCEP is only a new starting point for China to actively participate in the construction of global rules. As a major data resource country, China should take this opportunity to enhance the level of cross-border data flow and realize a win-win situation of data flow and data protection while adhering to the basic national security concept. In the future, various sovereign countries should work together to provide the international community with sufficient and efficient data governance public goods, build secure and orderly global data governance rules, promote the opening and sharing of global digital resources, and push the global cross-border flow of data toward a more inclusive, coherent and open international rule of law.

Acknowledgment

This paper is the research achievement of the graduate scientific research and innovation fund project of Anhui University of Finance and Economics (Project approval number: ACYC2022220). We thank Anhui University of Finance and Economics very much for its support and funding.

References

- [1] Wang Yafei. Construction of coordination mechanism of cross-border data flow rules among RCEP member countries [J]. China Telecom Industry, 2023, (03):18-21.

- [2] Li Y. Review and improvement of China's data cross-border flow rules under the RCEP agreement [J]. Science, Technology and Law (in English), 2023, (01):119-128.
- [3] Xu Weigong; Jia He. Comparative study on the rules of cross-border data flow governance in the context of RCEP and China's solution [J]. Guangxi Social Science, 2022, (12):62-69.
- [4] Li Xuejiao. Study on the exception clause of cross-border data flow under the framework of RCEP [J]. Journal of Dalian University, 2022, 43(06):44-50.
- [5] Wang Yan; Liu Danxia. RCEP cross-border data flow regulation and China's response [J]. Journal of International Law, 2022, (03): 154-155.
- [6] Zhang Xiaojun; Qu Xiaomeng. The RCEP data flow exceptions and China's response [J]. Political Law Series, 2022, (03):109-119.
- [7] Yang Xuekun. China's response to the RCEP e-commerce rules: a perspective on the governance of cross-border data flows [C]. Jilin University, 2022.
- [8] Hong Zhigang; Huo Junxian. RCEP regulation of cross-border data flows and its important impact [J]. Southwest Finance, 2022, (04):83-94.
- [9] Zhao Haile. Application of RCEP dispute settlement mechanism to the issue of cross-border flow of data and China's response [J]. WOU International Law Review, 2021, (06):39-55.
- [10] Wu Qiwei. RCEP protection of cross-border flow of personal data and China's response path [J]. Foreign trade and economic cooperation, 2022, (10):29-32.