Improvement of China's System on Security Assessment of Outbound Personal Data Flow under the Background of CPTPP

Bolin Wang *

Department of Law, Ningbo University, Ningbo, China

* Corresponding Author Email: 2311020125@nbu.edu.cn

Abstract. With the development of cross-border e-commerce's integration with the global economy, the cross-border data flow is playing an increasing important role in international economy and trade, and the smoothness of it directly or indirectly affects the improvement of the digital economy. Many countries or regions have established their own legal regulation systems for outbound data. Now China is the largest retail export economy in cross-border electronic commerce in the world, it application to join the Comprehensive and Progressive Trans-Pacific Partnership Agreement (CPTPP) is not smooth, and its data cross-border rules are quite different from CPTPP clauses, so it is difficult to align with them. Among them, the security assessment of outbound personal data flow system currently implemented in China is a major factor that makes connecting the cross-border personal data flow rules of China with CPTPP cross-border personal data flow clauses more difficult. By comparing this system in China with the cross-border personal data flow regulation system in the United States and the European Union, as well as the relevant provisions of CPTPP, this paper points out that there are some problems in this system in China, such as vague definition of the basic concept "important data" and excessive burden on data processors, and puts forward some legislative improvement measures to solve these existing problems, such as clarifying "important data", constructing a classification and grading system for cross-border data flow, and reshaping the distribution system of compliance responsibility for safety assessment.

Keywords: Security Assessment of Outbound Personal Data Flow, CPTPP, Cross-border E-commerce, Cross-border data flow, International economic and trade.

1. Introduction

On September 16th, 2021, a written letter of China's formal application to join the CPTPP was submitted by Minister of Commerce of China to the New Zealand, the one of the member countries of the Comprehensive and Progressive Trans-Pacific Partnership Agreement (hereinafter referred to as CPTPP) which held the original text of CPTPP. As for China's application to participate in CPTPP, every member country posed different reactions. Some member countries do not support China's membership, and even the United States, which has been not the member country of CPTPP, has been accused by many politicians of China's disqualification, and China has not yet joined CPTPP [1]. In sharp contrast, Britain, as a non-Pacific country, joined in July 2023 and became the first European contracting party to join the agreement. Undeniably, China's delay in joining CPTPP was influenced by international relations, but China's provisions on intellectual property rights, e-commerce and market access are different from those of CPTPP, adjusting the rules has become a necessary measure to help China join CPTPP. Among them, a big gap between China's regulations on cross-border data flow and the high standards of CPTPP's provisions on cross-border data flow exists, and the currently implemented security assessment of outbound personal data flow system is a major obstacle to the docking of CPTPP's provisions in the China Rules. The purpose of this paper is to compare the current safety assessment system in China with the relevant provisions of Typical Regions and CPTPP, point out the existing problems of this system, and put forward the improvement measures to meet the high standards of CPTPP.

2. Comparison of Related Regulations of China, Representative Regions and CPTPP

The orderly flow of international data, being a crucial aspect of international economic and trade exchanges, is facilitated by the promotion and regulation of national data, which in turn promotes the development of a country's international economy and trade. Consequently, numerous countries have adopted various forms of regulation pertaining to the cross-border flow of national data [2]. In addition, CPTPP, RCEP, and USMCA are all agreements that regulate the cross-border flow of data among their member countries. In this section, the differences between China's Security Assessment of Outbound Personal Data Flow regulations and the data cross-border regimes of the Representative Regions and the relevant rules of the CPTPP, which China wants to join, by comparing them with each other, will be analyzed [3].

2.1. China's Rules on Security Assessment of Outbound Personal Data Flow

The main regulations pertaining to the security assessment of outbound personal data flow in China can be traced to the "Provisions on Security Assessment of Outbound Personal Data Flow" (hereinafter abbreviated as "Security Assessment Provisions") and the "Provisions on Promoting and Regulating the Cross-border Flow of Data" (hereinafter referred to as "Cross-border Flow Provisions"). Additionally, some related concepts and terms are stipulated in the Network Security Law of the People's Republic of China which stipulates the concept of "important data", as well as in the Data Security Law of People's Republic of China. Among them, the Provisions on Security Assessment stipulate the outbound data that need to be assessed, key assessment items, materials needed for assessment and other safety protection responsibilities and obligations. The Provisions on Cross-border Flow stipulate that the types of data subject to security assessment, the exemption of certain data types from assessment, the validity period for passing security assessment, and the relationship between these regulations and other relevant regulations are to be **observed. There** are even other official documents such as the Cybersecurity Standard Practice Guidelines -- Guidelines for the Classification and Hierarchy of Network Data, which also stipulate rules related to the outbound personal data. Thus, different types and levels of normative documents form China's current system of security assessment of 0utbound personal data flow.

2.2. Representative Regions'Rules on Outbound Personal Data Flow

The "Representative Regions" mentioned here mainly refer to countries or regions other than CPTPP member countries that have relatively representative regulations in the field of personal cross-border data flow, mainly including the United States and European Union countries. There are gaps between them in many aspects of personal data cross-border flo regulation. Though the establishment of a comprehensive federal law addressing data issues in the U.S. has failed, it has formulated special data protection legal documents for different kinds of data in different fields, and these legal documents contain relevant provisions on the cross-border flow of personal data [4]. In addition, as the lead country of TPP, the predecessor of CPTPP, the concept of data flow in the United States is "emphasizing freedom and neglecting security" [5]. However, at present, A fact confronting U.S. data legislation lies in cross-border data transfers, as other nations remain cautious in permitting American corporations to transmit individuals' data to the U.S., for instance, HIPAA, falls short in sufficiently safeguarding personal data [6]. Conversely, a rigorous regulation system for cross-border personal data flows has been instituted by the European Union, it regulates the Cross-border Flow of personal data mainly according to the General Data Protection Regulation (hereinafter referred to as GDPR), and attaches great importance to the safety of personal data, benefiting the EU significantly, promoting better data hygiene practices enhances data quality and security, fostering trust in digital transactions and fostering economic growth [7]. By constantly improving the path rules of cross-border data flow, it gradually formed a hierarchical system to standard cross-border data flow, taking

into account the safety and free mobility of personal data, and constructing an extremely complete personal cross-border data flow regulation system.

2.3. CPTPP's Provisions on Outbound Personal Data Flow

CPTPP is a multilateral trade agreement, which goes beyond the traditional market access negotiation. Its existence provides a new multilateral paradigm for the realization of global FTA (Free Trade Agreement). In addition, because CPTPP was originally an American trade rule led by the United States, it advocates and even requires parties to promote cross-border data flow, while reducing localization of data to encourage free cross-border data flow, which largely reflects the pursuit of "data flow freedom" [8]. CPTPP rules adopt a normative form of "principle+exception" for personal data leaving the country, which stipulates the general principles of personal data leaving the country and also stipulates the exceptions. Specifically, CPTPP's provisions in this field are based on the second paragraph of Article 11 in Chapter 14, "Cross-border transmission of information by electronic means shall be allowed" as the principle, with the exception of regulatory requirements in the first paragraph of Article 11 of Chapter 14, the exception of public policy in the third paragraph, and the exception of general and security as stipulated in Chapter 29, a complete personal cross-border data flow legal regulation system has been formed [9].

2.4. Comparative Analysis

Under the concept of attaching importance to data security, China has established a security assessment system for personal data leaving the country. Compared with China, the idea of pursuing "data freedom" in the United States is consistent with CPTPP (This is typified by the fact that the CPTPP provides for a “security carve-out” that does not encompass security interests based solely on commercial economic purpose), however, there exists no documented regulation pertaining to restrictions on cross-border data flows. In addition, many countries have been worried about cross-border data flow with the United States, so American regulations or practices cannot bring much help to the improvement of personal cross-border data flow system in China. However, the complete and strict cross-border data flow restrictions of the European Union are contrary to the CPTPP that China wants to join, so the EU system cannot provide China with enough positive reference. In order to make China's personal security assessment of outbound personal data flow system successfully connect with CPTPP standards, we should return to the comparative analysis with CPTPP standards, which are different in many aspects from macro to micro. First of all, there are significant differences in the conceptual level between the two regarding the cross-border flow of data. Safety assessment system in China is the embodiment of its concept of "emphasizing safety and neglecting freedom", while CPTPP pursues a completely opposite concept. Secondly, there are differences in the regulatory system between the two. CPTPP’s “principle+exception” regulatory system for personal data leaving the country has actually formed a classified and hierarchical legal system, while China's Data Security Law and the Provisions on Cross-border Flow point out that a classified and hierarchical system should be established, but it is still in the conceptual stage (even though many provisions of the Provisions on Cross-border Flow involve the classified and hierarchical planning of data leaving the country, it is not clear). In addition, in terms of specific provisions, compared with CPTPP's practice of clearly stipulating restrictions such as "general exception" and "safety exception", although China's "Regulations on Safety Assessment" stipulates that "important data" is restricted from leaving the country, this regulation and other laws have not given a clear scope of "important data", which is ambiguous and increases the compliance burden of data processors [10].

3. Current Problems on China's Security Assessment of Outbound Personal Data Flow

It is evident that there exist some notable differences between China's provisions in this area and the relevant provisions of the CPTPP. The objective of enhancing China's Security Assessment of

Outbound Personal Data Flow is to align with the standards set forth by the CPTPP, so it is necessary to identify the existing problems of China's outbound personal data flow in light of the differences between China's Security Assessment of Outbound Personal Data Flow and the CPTPP standards.

3.1. Conservative Attitude towards Outbound Data Flow

As mentioned above, in general, China's lawmakers are still in the greater emphasis on the safety of cross-border data flow, and even China's Data Security Law mandates the localization of relevant data in order to provide close protection for national interests in cyberspace. This is contrary to the CPTPP's concept of "freedom over security" for data flows. The Provisions on Security Assessment of Outbound Personal Data Flow is also a concrete embodiment of China's concept of "emphasizing security" of data flow. Although the Provisions on Security Assessment and the Provisions on Cross-border Flow are both aimed at promoting the free flow of data, these two laws still set a few restrictions on the cross-border flow of personal data, and even still presuppose the "necessary" principle. The premise is even "necessary". A conclusion can be drawn that China's concept of data flow is still relatively conservative, and the Provisions on Security Assessment and the Provisions on Cross-border Flow provide for the Security Assessment of Outbound Personal Data Flow regime as a means of restricting the free flow of data [11]. The Security Assessment of Outbound Personal Data Flow regime, which is regulated by the Provisions on Security Assessment and the Provisions on Cross-border Flow, compared to the CPTPP standard, is too strict.

3.2. Vague Concept and Scope of ''Important Data''

The Provisions on Security Assessment and the Provisions on Cross-border Flow, the two main laws regulating the export of personal data in China, both stipulate restrictions on the export of "Important Data". Among its provisions, Article 19 of the Provisions on Security Assessment outlines the definition and scope of "Important Data", encompassing information that, upon tampering, damage, leakage, or unauthorized acquisition or use, has the potential to compromise national security, economic stability, societal harmony, public health and safety, among other critical aspects. This article only qualifies the nature of the so-called "Important Data" without stipulating what types of data are included in "Important Data" or mentioning the difference between "Important Data" and "Ordinary Data". Although the Provisions on Cross-border Flow stipulate that data that is not declared as "Important Data" by the relevant authorities can be exempted from security assessment, the entire Provisions do not contain any limitation on the concept and scope of "Important Data".

In conclusion, there is not an accurate definition the concept and scope of "Important Data" in Provisions on Security Assessment and the Provisions on Cross-border Flow, or such a definition is too vague and general. With such vague concept and scope criteria and concerns about the security of outbound data, security assessment enforcement agencies and data processors tend to recognize data that is difficult to identify as "Important Data", and the pssibility of conducting a security assessment of outbound data if a data is recognized as "Important Data" increases the probability that the security assessment system will be triggered. assessment system is triggered, making data exports more restrictive.

3.3. Excessive Compliance Responsibility of Data Handler

The Provisions on Security Assessment stipulate that data processors bear the compliance responsibility of preventing digital risks when processing personal data out of the country, and Article 3 of the Provisions stipulates that a risk assessment system combining "risk self-assessment and security assessment" shall be established in respect of personal data out of the country.

Although the newly introduced the Provisions on Cross-border Flow does not explicitly mention the concept of "risk self-assessment" in its legal text, Article 11 of the Provisions essentially requires data processors to carry out security risk assessment of the data in question, which is related to the concept of "risk self-assessment". Article 11 of the Provisions on Promoting and Regulating Cross-border Flow of Data stipulates that: "If a data security incident occurs or is likely to occur, it shall

take remedial measures and promptly report the incident to the net information department at or above the provincial level and other relevant competent authorities."

The "risk self-assessment" system in fact imposes a heavy compliance burden on data processors. Although the necessity of data processors conducting security risk assessments for outbound data is only vaguely stipulated in the relevant laws and regulations, with no explicit provisions, in practice, on the one hand, data processors need to assess multiple matters such as the type of outbound data, the mode of cross-border data flow, and the data receiver's security capability with their own assessment capability, and on the other hand, as data processors are mainly enterprises, the data security assessment capability varies from enterprise to enterprise, and the data security assessment capability varies among different enterprises. On the other hand, since data processors are mainly enterprises, the data security assessment capabilities of different enterprises vary, and it is difficult for enterprises to ensure their own data outbound security risk assessment capabilities. Since data processors have to bear unfavorable legal consequences in case of cross-border data flow risks, the existence of the "self-assessment of risk" system will undoubtedly make data processors worry about cross-border data flow compliance and hinder the free data flow.

4. Proactive Measures to Align China's Rules with CPTPP's Provisions

In order for China to successfully join the CPTPP, it is imperative that it aligns with the rules stipulated in the CPTPP. Upon comparing China's regulations with the CPTPP's provisions, it can be seen that a series of problems are existing in the current framework of China's Security Assessment. To streamline the convergence between China's regulations CPTPP's provisions, it is necessary to address the existing problems, change the attitude, and make legislative improvements.

4.1. Adjust the Conservative Attitude towards Outbound Data Flow

The difference in the concept of cross-border data flow is the most macroscopic and fundamental difference between China's rules and CPTPP's provisions, and also the reason for other differences between the two. Guided by the legislative spirit of paying more attention to data security, Chinese legislators have formulated a series of more conservative rules, which in turn has led to the formation of a system of data cross-border rules in China that is more restrictive relative to the CPTPP rules.

In order for China's cross-border data flow system, including the personal cross-border data flow security assessment system, to successfully interface with the CPTPP standards, the first step should be to change the conservative attitude. An attitude that attaches more importance to the free flow of data should be held by Multiple subjects involved in personal cross-border data flow. Legislators should promote the concept of promoting the free flow of personal data in the legal provisions and further reduce the restrictions in the relevant legal provisions; they should reduce the risk self-assessment responsibility of the personal data processors and the unnecessary security review of the cross-border data flow by the enforcement authorities, and reduce the restrictions by the relevant enterprises and organizations [12].

4.2. Clear the Concept and Scope of Data of Different Levels

The mere characterization of the concept of "Important Data" without a clearer definition of its concept and scope will inevitably lead to an unnecessary increase in the probability of triggering the cross-border data flow security assessment system. In order to connect China's personal data security assessment system with the CPTPP standards, clarifying the concept and scope of Important Data is necessary. To clarify the concept and scope of Important Data, lawmakers can make a list of specific categories and form a reasonable classification and grading system of data departure.

In order to clarify the concept and scope of Important Data, reduce unnecessary security assessments and improve the efficiency of data export, the following legislative work can be carried out:

First, the types of "Important Data" can be listed directly in the legislation, so that the legislator can improve the accuracy of the legislation by specifying which data outbound may jeopardize which specific aspects in different fields of the country, society and economy, and also be more conducive to the identification of data processors and executive agencies; Secondly, the legislator can emphasize the qualities of "Important Data" in the legislation in terms of the difference between "Important Data" and "ordinary data", so as to reduce the ambiguity that may arise when data processors and executive agencies identify the level of data. In addition, the construction of the classification and grading system for personal data exportation should be speeded up by the legislator, who should as well as stipulate different regulation methods for different important levels and types of data, so that data processors and executive agencies can have a reliable reference standard when handling data exportation, and make more standardized data exportation behaviors, taking into account both security protection and data exportation. This will enable data processors and enforcement agencies to have a reliable standard of reference when handling data export and make more standardized data export behaviors, balancing security protection and data export efficiency.

4.3. Remodel the Allocating System of Compliance Responsibility

Excessive compliance responsibilities imposed on data processors during the risk self-assessment not only increase the burden on them, but also greatly reduce their motivation on promoting the freedom of data flow [13]. To facilitate the seamless flow of data and reinforce the standards set by the CPTPP, the burden of data processors should be reduced and the compliance responsibility allocation system should be reshaped. The following approaches can be taken to reshape the Allocating System of Compliance Responsibility in China.

First, more risk assessment responsibilities should be assumed by the data outbound enforcement department. Due to the varying security assessment capabilities of enterprises, many enterprises do not have sufficient risk assessment capabilities, while cross-border data flow enforcement authorities, including local net information departments, often have more professional risk assessment personnel and systems, with stronger risk assessment capabilities, and should assume more responsibility for cross-border data flow security assessment. A specialized cross-border data flow security assessment organization can also be set up, employing relevant professionals to be in charge of the organization can also set up a specialized data outbound security assessment organization, hire relevant professionals to be responsible for security risk assessment work, and be uniformly responsible for the security assessment of outbound data or at least undertake part of the assessment work, so as to reduce the assessment pressure on enterprises and local net information departments, and at the same time, avoid the relevant stakes and step up the freedom. Finally, no matter which subject is responsible for the main assessment and compliance, no matter what division of labor is involved in the cross-border data flow security assessment, in the actual operation of the security assessment, the focus should be highlighted, with emphasis on reviewing the legality and necessity of the cross-border data flow, maximizing the freedom of data flow under the premise of guaranteeing data security, and promoting the convergence of China's personal cross-border data flow with the CPTPP standards.

5. Conclusion

The cross-border flow of personal data refers to the processing, storage and retrieval of personal data across national boundaries, and the free flow of it has emerged as a crucial impetus for the development of cross-border e-commerce and international economy and trade, as advocated by CPTPP. China strives to join CPTPP, but its existing security assessment of outbound personal data flow system has some problems, such as conservative concept of data exit, vague definition of related concepts, and excessive compliance burden of data processors. In order to solve these problems, legislators can adjust the concept of data exit, clearly define related concepts, and reshape the risk distribution system of safety assessment. However, the analysis of the above problems and the corresponding solutions are mainly at the legislative level, and there is no in-depth analysis of the

problems in the practice of China's security assessment of outbound personal data flow, and no corresponding improvement measures are put forward for the problems in practice. Future endeavors by researchers could involve exploring the practical realm of China's security assessment of outbound personal data flow system, thereby enhancing China's system both legislatively and practically, aligning it with CPTPP provisions, pushing China to participate CPTPP successfully.

References

[1] Ajibo, Collins C., Nwatu, Samuel I, Ukwueze, Festus O., Adibe, Emeka; Lloyd, Chidi, Richards, Newman. U. RCEP, CPTPP and the Changing Dynamics in International Trade Standard-Setting. Manchester Journal of International Economic Law, 2019, 16 (3): 425 - 440.

[2] Jin Li, Wanting Dong, Chong Zhang, Zihan Zhuo. Development of a risk index for cross-border data movement. Data Science and Management, 2022.

[3] Jiayue Yan. Improvement Path for Cross-Border Governance Rules of Personal Data from an International Perspective. International Journal of Frontiers in Sociology, 2024.

[4] Bertaut, Carol C. Understanding U.S. Cross-Border Securities Data. Federal Reserve Bulletin, 2006.

[5] Ajibo, Collins C. TPP Objectively: Legal, Economic, and National Security Dimensions of CPTPP. Manchester Journal of International Economic Law, 2021, 18 (1): 152 - 155.

[6] Joshua M. Wilson. Cross-Border Data Transfers: A Balancing Act through Federal Law. Business, Entrepreneurship & Tax Law Review, 2022, 6 (2): 150 - 180.

[7] Voss, W. Gregory. Cross-Border Data Flows, the GDPR, and Data Governance. Washington International Law Journal, 2020, 29 (3): 485 - 532.

[8] Burri, Mira. The Regulation of Data Flows through Trade Agreements. Georgetown Journal of International Law, 2017, 48 (2): 407 - 448.

[9] Qian Xu. Phoenix from the Ashes: CPTPP Meaning for Asia-Pacific (and Global) Investment. Asian Journal of WTO and International Health Law and Policy, 2022, 15 (2): 567 - 652.

[10] Michell Andrew D, Mishra Neha. Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute. Journal of International Economic Law, 2019, 22 (3): 389 - 416.

[11] Liu Junchao. CPTPP Compliance of China’s Measures for the Security Assessment of Outbound Data Transfer. Information Security and Communications Privacy, 2023 (11): 37 - 45.

[12] Dayday, Czar Matthew Gerard T. Cross-Border Data Flows and Data Regulation under International Trade Law. Philippine Law Journal, 2023, 96 (1): 33 - 81.

[13] Lin Zihan. Research on the Rules of Cross-border Data Flow in Major Global Economies. China Information Security, 2023 (10): 53 - 57.