

An Analysis of China's Rules for Cross-border Data Flows under RCEP Framework

Xin Huang, Jiahao Li*

SILC Business School, Shanghai University, Shanghai, China

**corresponding author*

Abstract

In recent years, the improving value of data has led to enthusiasm for the establishment of data management regulations in various countries, but the rules worldwide data flow have not been created, and data flow is still problematic. The contradiction of cross-border data flow is the conflict between its economic value and security risk. As a data power, China is pushing forward the improvement of its rules. The establishment of RCEP has positive implications for the unification of rules. This paper will further explain the improvement and progress of China's cross-border data rules under the influence of RCEP through comparative study and literature analysis, and gain a deeper understanding of the changes and development of rules.

Keywords

Data Cross Border, RCEP, Flow Rules, Data Governance

Date of Submission: 09-04-2023

Date of Acceptance: 23-04-2023

I. Introduction

With the continuous development of digital technology and the Internet, cross-border e-commerce and international digital trade with the character of data flow have become an important part of world trade, and the value and significance of data are constantly highlighted, becoming an important strategic resource with profound economic value. According to "Data Globalization: A New Era of Global Flows" released by McKinsey Global Institute in 2016, compared with traditional international trade, data flow between countries has played a more important role in promoting the development of the world economy.^[1]

In such a digital era, the importance of data to the country cannot be overstated, and data security is seen as a new type of national security. It is worth noting that if data is allowed to flow freely, the various information contained in the data can be analyzed and processed to accurately know the personal information of almost all citizens, which also means that other countries can precisely control all the information of the country, including important strategic information of military, economic and politics which are visible to other countries, that is undoubtedly terrible. The arbitrary flow of data will pose a serious threat to national security.

Therefore, no country will let its data flow unrestrainedly. However, this also makes some companies suffer a lot and limit their development. For example, the U.S. government decided to block tiktok for national security reasons, believing that tiktok, a Chinese app, has the ability to manipulate public preferences through algorithms and tweets and the ability to influence political and policy stability in the U.S. This undoubtedly reflects the importance of data to the country and the economic value and security risks in the flow of data divergence.

Along with the emergence of the theory of data sovereignty, countries have started to consider how to establish a reasonable and sustainable set of rules for the cross-border flow of data. The EU has promulgated the General Data Protection Regulation (GDPR), which sets different security aspects and a series of prerequisites for the cross-border flow of personal data, trying to guide the safe use of data. China, as an important country in digital technology development and a major country in digital trade, has also introduced corresponding policies and regulations on data flow. For example, the E-Commerce Law and the Data Security Law fully reflect the country's emphasis on data and its mindset to actively address this contradiction.

However, for security reasons, each country has imposed restrictions on its own data, and the restriction rules are complicated, which seriously hinders the normal flow of data and has an extremely negative impact on economic development, and how to regulate their own rules and establish uniform standards has become the focus of public and governmental attention. In 2022, with the entry into force of the Regional Comprehensive Partnership Agreement (RCEP), the relevant regulatory powers and obligations on cross-border data flow in the agreement provide a good rule for the parties, and China, as one of the first countries to enter into force, has also learned from such an agreement to further improve the relevant legal system to further

achieve the harmony and unification of data security and economic benefits.

II. Method

In this paper, I mainly use literature collection and comparative methods to qualitatively analyze the contradictory nature of data flow and the development of rules for cross-border data flow in China in the context of RCEP, and to compare data governance in China and extraterritoriality, from which I draw corresponding conclusions.

2.1 Literature induction method

Using databases such as China Knowledge Network (CNKI) and China Outstanding Master's Degree Thesis, we searched for content related to data flow rules across borders and RCEP data flow. The corresponding search terms are data cross-border, data restriction, data security, RCEP data flow, RCEP information security, from which several relevant authoritative articles were found, and I read them, took their essence and summarized them to draw his own relevant conclusions.

2.2 Comparative method

The comparative research method refers to the research and investigation of a certain number of objects according to certain criteria, to discover the similarities and differences among them, and to draw universal and special regular conclusions from them. In this paper, the author mainly compares the current situation of data governance between China and extraterritorial countries, aiming to find out the different focus and details of rules among different geographical countries, as well as the common rule norms, and find out the universal rule requirements and the improvement direction of China's data cross-border rules from these similarities and differences.

III. Analysis

3.1 Status of Data Governance in China and Extraterritoriality

Wei, Chengfei et al.(2023) point out that the dramatic increase in the influence and volume of data has triggered a high level of attention to it in various countries, and China and other countries or organizations outside the region have built their governance models for data at multiple levels, including strategies, laws and regulations, industry norms, and technical regulations, encouraging the free flow of data on the one hand and controlling the flow of data through explicit or implicit approaches on the other. ^[2]However, different countries have their own practices and strategies, which will be analyzed in detail in the following text.

The countries and organizations that are indicative and influential on data governance rules extraterritorially are the U.S. and the EU. The US focuses on an ex post remedy approach, while the EU tends to use an ex ante defense approach. ^[2]The U.S. is a significant data power and actively encourages the cross-border flow of data, using a less clear system of evaluation and interpretation, but this does not mean that the U.S. does not regulate data. The U.S. has adopted the Clarifying Lawful Overseas Use of Data ACT, the Executive Order on Protecting Americans' Sensitive Data from Foreign Adversaries' Sensitive Data from Foreign Adversaries), etc., to categorize data involving interstate control and enhance penalties in the event of a violation. In the case of the former act, its introduction not only gives the U.S. government greater access to cross-border data itself, but also makes it difficult for foreign companies in the U.S. to mobilize data within the U.S. For the EU, in contrast to the U.S., it has changed from ex post to ex ante by adopting the General Data Protection Regulation to conduct ex ante reviews of agencies and organizations involved in the use of such data to ensure that they have a sound data protection approach and system, and to include a white list of the free flow of data, with only the subjects of the list entered having freer access to the relevant data. For a multinational joint organization like the EU, its data cross-border rules also reflect this feature, i.e., countries within the EU region are free to transfer data across borders, while strict restrictions are implemented for all areas outside the region.

China is a major data resource country, and its total data volume is expected to account for nearly one-third of the world's data by 2025. ^[3]The rapid rise in the total amount of data brings increased economic benefits, but also comes with greater data security risks and threats to national security. According to Wei Chengfei et al.(2023) , in general, the data governance system adopted by China implements the idea of full governance. ^[2]Through the Data Security Law, the Data Exit Security Assessment Measures, and the Security Assessment Measures for Personal Information and the Most Important Data Situation (Draft Opinion), China has built a prudent whole-process management system specific to the localized use of data and advance security assessment to further safeguard national security and protect data information. Among the more prominent laws are the Personal Information Protection Law, which contains a complete elaboration of the data protection system, and the Data Security Law, which contains the identification methods and security assessment strategies for important data, and contains the idea of graded data protection, which has certain commonalities with the graded control in the United States.

It is clear that the management of data across borders is distinctive in different countries, but the commonalities are also extremely evident. The management of data outflow is uncommonly important across countries, and a prudent approach to data is common to all countries. However, the U.S. manages from an ex post relief approach, the EU uses ex ante, and China strictly manages the whole process. Moreover, the EU, as an interstate organization, also provides some exemplary role in the harmonization of data cross-border rules for the proposal of a uniform cross-border management system in the world. Data cross-border management is a new management issue that has emerged only in recent years, and it is difficult for any country to establish an extremely perfect approach in this regard. For China, it is of positive significance to learn from the strengths of other countries for the soundness of its own data cross-border management system.

3.2 RCEP regulations on data flow

RCEP is the largest free trade agreement in the Asia-Pacific region, and its influence and development potential are unmatched by most international organizations. In the e-commerce chapter of the agreement, the flow of data has already been stated, which further proves the importance of cross-border flow of data. As a huge inter-state organization, its recommendations are of great importance to the establishment of world rules.

Jiehan Feng et al.(2021) point out that the RCEP agreement not only takes care of the e-commerce interests of developed countries, but also equally takes into account the data security issues of developing countries, and has a differentiated approach to data protection for different countries. ^[4]Pluralistic governance, free flow and restricted flow are the core elements of the RCEP agreement for data flow. ^[5]Therefore, based on the concept of equality and protection, while encouraging the free flow of data to meet the needs of developed countries, a certain grace period is also given to the more backward developing countries to provide a buffer time for the improvement of the system and industrial development of these countries. At the same time, in response to the different sensitivities of different countries to data security, the parties to the agreement are considered to have a certain degree of autonomy to decide, reflecting the concept of shared governance, which not only respects the differences between countries, but also makes the docking of national rules more smooth. Free flow is an important manifestation of the value of the data economy. In order to promote the cross-border flow of data and better promote economic development in Asia, RCEP has adopted a clause prohibiting the localization of facilities while encouraging the flow of data, i.e., the governments of the contracting parties are not allowed to restrict the development of e-commerce based on such industry standards as whether the data facilities are localized, and RCEP is strongly opposed to the obstruction of data. But such a restriction does not mean that RCEP encourages complete free flow, and it also incorporates an exceptional interpretation of the above prohibition based on the achievement of public policy objectives and the requirement of maintaining fundamental security interests. And, in terms of data categories, certain controls may be imposed on financial and telecommunications data.

3.3 The main contradiction of data circulation - economic value and security risk

A wealth of information proves that the government is encouraging the flow of data while at the same time restricting it, a seeming contradiction that is essentially between the government's need for economic progress and the protection of national security.

Peng Yu et al.(2022) clarify that data has been the new engine for economic development in the digital age, and the value generated by cross-border data flows has been greater than the overall value of goods in cross-border trade. The economic value of data is huge, and no country will give up on the economic boost of cross-border data utilization. The analysis of cross-border data can also effectively maintain the stability of international trade and maintain financial security. For example, in cross-border e-commerce, through the analysis and utilization of massive data from various countries, the transaction behavior and trust index of subjects in different jurisdictions can be accurately assessed, which makes cross-border trade more reliable and efficient.^[2]

However, large-scale data cross-border, especially the data cross-border that contains strategic significance of homeland security, will raise serious national security issues. For example, DDT, with its Class A mapping of high precision maps, which contains a large amount of personal information, geographic coordinate data, etc., has a huge impact on homeland security and military security, and is therefore subject to regulation by the relevant authorities in its listing in the United States.

Economic value and security risk may seem to be the main contradiction that is difficult to reconcile in data cross border, but it is possible to maximize the economic value of data under certain conditions while maintaining national security through perfect data cross border management rules.

IV. Improvement of China's data cross-border rules under RCEP

Comparing RCEP's data cross-border flow provisions with China's data management system, one can still find points of difference between the two.

Faced with the RCEP concept of pluralistic governance and advocating cross-border free and secure flow, China prefers security above all and does not show an active supportive attitude towards the concept of free flow.^[5] Although in the Data Security Law, China clearly writes that data security and free flow go hand in hand, as far as the specific management system is concerned, China focuses more on protecting data security and emphasizes the localization and security assessment of data storage devices, while the feasible scope of free flow, etc., is not clearly stated. There is a contradiction between the localization requirement of storage devices and RCEP, and China's unilateral emphasis on this is a great restriction on free movement. Although this is of great significance for national security, the inflexible and unclear character of its measures will undoubtedly cause further loss of the economic value of data flow.

Faced with such a difference in rules, China, as a party to RCEP, has also made certain relaxations in the measures for data cross-border. China has clarified the necessity of cross-border data flow, and gradually allowed conditional cross-border data flow while insisting on localization of data storage, which also demonstrates that China is keeping pace with the times and conforming to the world development trend. As for the inflexibility of our rules, we have shifted from a complete government assessment to a combination of self-assessment and security assessment, while the security assessment measures are reviewed, and its review is whether there is a conscious neglect of a part of the assessment measures, resulting in the final assessment processing with rigid characteristics. At the same time, China has also extended some exemptions to data exit restrictions, namely personal information protection certification, data cross-border standard contract approach, which is the result of learning from the relevant experience of the United States and the European Union, and also makes China's cross-border flow of data more effective, and more in line with the concept of RCEP free flow.

In summary, China's adjustment strategy basically meets the relevant requirements of the RCEP for data cross-border, and has made certain enhancements to its own legal system. However, Li Ye (2023) points out that although China's flow restriction measures have basically been able to be harmonized with the RCEP agreement, there are still differences in the wording of the rules expressed therein, which may lead to inconsistent interpretation of the provisions, and there is still room for improvement.^[5]

V. Summary

As the scale of data continues to expand and its influence continues to rise, data has become an important strategic resource as well as an important factor that affects national security. Excessively free data activities can easily make military, political and other strategic information leaked, infringing on national security and social stability.

Therefore, realizing the importance of data, all countries have enacted certain laws and regulations on the cross-border flow of data to safeguard national interests. While China adopts a strategy of full governance to manage data, not only assessing the storage and transmission of data in a secure manner *ex ante*, but also imposing strict controls during the dissemination process, the EU only carries out the former, with only *ex ante* security assessments and lower restrictions on *ex post* data transmission. However, it is worth noting that the EU provides for the free flow of data within the EU region and restrictions outside the region, and this regionalized free data flow also serves as a guide for worldwide data transfer regulation. The U.S., on the other hand, adopts an *ex post facto* remedy to regulate and manage data transfer issues by focusing on the strength of *ex post facto* penalties. Clearly there are differences in the legal systems of each country, which seriously affects the free flow of data and poses a negative impact on the development of the digital economy.

RCEP, the largest inter-state organization in Asia, has also addressed the issue of cross-border data flows in its agreement. In the agreement, it points out the need for pluralistic governance, free flow and security restrictions in parallel, which not only takes care of the interests of developed countries, but also concerns the digital status of developing countries, giving a certain buffer. At the same time, while promoting the free flow and prohibiting countries from requiring data localization, it also explains the prohibition order and gives certain exceptions.

The main contradiction of data flow can be attributed to the contradiction of economic value and security risk, but it is not an irreconcilable difficulty, and countries are making useful attempts. Facing the RCEP agreement, China's legal system is undoubtedly contradictory to the relevant provisions of RCEP, which also points the way to the progress of China's data cross-border regime. In response to its overly strict controls and look down on free flow, China is gradually loosening its controls on data, expressing more clearly its support for free flow of data, while adopting a flexible approach to *ex ante* assessment and extending some of the exemptions to enhance the level of freedom of data crossing borders. However, the wording of China's rules still differs somewhat from the RCEP, so Chinese legal improvements should continue to be implemented .

References

- [1]. Kinsey Global Institute (MGI). Digital globalization: The new era of global flows. <https://www.mckinsey.com/~media/mckinsey/business%20functions/mckinsey%20digital/our%20insights/digital%20globalization%20the%20new%20era%20of%20global%20flows/mgi-digitalglobalization-full-report.pdf>, accessed on February 28, 2023
- [2]. Wei Chengfei, Jiang Jie. Multidimensional logic of global cross-border data security governance and China's response[J/OL]. *Books and Intelligence*:1-8[2023-03-01]. <http://kns.cnki.net/kcms/detail/62.1026.G2.20230221.1533.001.html>.
- [3]. Zhang, Malnan. Cross-border data flows: global dynamics and Chinese countermeasures[J]. *Open Herald*,2020,No.209(02):44-50.DOI:10.19625/j.cnki.cn44-1338/f.2020.0025.
- [4]. Feng Jiehan, Zhou Meng. Cross-border data flow regulation: core issues, international solutions and China's response[J]. *Journal of Shenzhen University (Humanities and Social Sciences Edition)*,2021,38(04):88-97.
- [5]. Li Y. Review and improvement of China's data cross-border flow rules under RCEP agreement [J]. *Science, Technology and Law (in English and Chinese)*, 2023, No. 13(01):119-128. doi:10.19685/j.cnki.cn11-2922/n.2023.01.013.
- [6]. Peng Yu,Ding Bai Lin,Yang Bi Zhou.Simulation of the impact of RCEP cross-border data flow rules on China's economy[J]. *Quantitative Economic and Technical Economics Research*,2022,39(12):69-89.DOI:10.13653/j.cnki.jqte.2022.12.004.

Xin Huang, Jiahao Li. "An Analysis of China's Rules for Cross-border Data Flows under RCEP Framework." *IOSR Journal of Business and Management (IOSR-JBM)*, Vol.25, No. 04, 2023, pp. 24-28.