ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

The Influence of RCEP on the Regulation of Cross-Border Data Flow and China's Response

Ziyi Xu

Hebei University of Economics and Business, Shijiazhuang, 050000, China

Abstract: *The Regional Comprehensive Economic Partnership Agreement (RCEP), as an important regional Free Trade Area agreement (FTA), provides for new provisions for cross-border data flow. RCEP focuses on the security, which allows cross-border data flow basis on respecting national data sovereignty while setting up basic security exceptions. This respect-based cooperation and co-governance model is different from the "zero-sum game" in Europe and the United States.In addition, the RCEP cross-border data flow clause plays a great significant role in promoting regional digital governance and improving the global data flow rules when the WTO related rules lag behind.As the RCEP contracting party, China should be as the external driving force, on the fundamental of the national security concept to expand the level of open cross-border data flow, form data governance "Chinese template", contribute to digital development and data governance wisdom and Chinese solutions, promote a more inclusive, more open digital pattern of international law.*

Keywords: *cross-border data flow; RCEP; regional trade agreement; data regulation; data security; data sovereignty; digital economy*

1. Introduction

The performance of cross-border data flow can be traced back to the time when human beings began to carry out transnational business activities. People transfer all kinds of domestic business information to another country through transnational trade activities, forming the most primitive "cross-border data flow phenomenon". Research on "cross-border data flow" in modern society can back to the rapid growth of international trade brought by the advances in computer and communication technologies in the 1970s.The concept of cross-border data flow was first proposed at the Organization for Economic Co-operation and Development (OECD) meeting in the 1980s, The OECD's subsequent Guide to Privacy Protection and the Cross-border Flow of Personal Data, released in 1980, defined it as "personal data movement across borders"[1]The EU General Data Protection Regulation (GDPR), coming into force in 2018, specifically describes the cross-border flow of data as "the transmission of personal data to third countries or international organizations". [2] China's information security standardization technical committee also stipulates the definition, namely data exit refers to the collection in our country and produces electronic form of personal information and important data provided to overseas organizations, individual one-time activities or continuity activities.[3]

Since 1990s,rules of cross-border data flow roughly experienced three stages, from the initial EU dominate personal privacy protection to the value orientation of data flow freedom led by the United States in the early 20th century,until now,RCEP focus on protecting the security of cross-border data in Asia, the development of the three stages reflects the different value concept.[1]

2. The European-American supervisory path of cross-border data flow

2.1 The regulation path of the EU

Due to the influence of historical, geographical and political reasons, the EU attaches great importance to the protection of personal privacy, and protects personal information to the dimension of

[1]Refer to organization for Economic Cooperation and Development (OECD) privacy Framework.
[2]Refer to section 44 of the GDPR.
[3]Refer to Article 3.7 of the Information Security Technology Data Outbound Security Assessment Guide (Draft)

ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

basic human rights through the form of legislation. From 1973 to 1984,13 global countries had enacted data protection laws, eight of which were European countries.

The EU regards "personal privacy protection" as its fundamental position on cross-border data transmission. The EU initially limited data flows to the EU, but as the digital economy growing, the EU has realized that cross-border data flow should seize digital resources and boost the economy. Based on this, the EU has issued a series of conventions, directives and regulations, but it still retains the "human rights first" color. The Convention on the Personal Protection of the Automatic Processing of Personal Data, signed by the European Council in 1981 (the Convention), states that states' parties cannot restrict the cross-border data flow on the grounds of protecting privacy. In fact, the Convention only regulates the regional data flow within the EU, and does not take into account the relevant factors such as the data flow outside the region. However, as the first regional legal document to stipulate the cross-border data flow in history, it has a certain demonstration and leading role. In 1995, the European Parliament and the European Council adopted Directive 95 / 46 / EC on the Personal Protection of Personal Data Processing and the Free Circulation of Data involved (hereinafter referred to as the Data Protection Directive), requiring member states to translate it into domestic law for application, which is highly legally binding; For the first time, the concept of "third country" was introduced, with strict regulations on data transmission outside the region, introducing "standard contract terms" and "binding company rules". Chapter 4, Article 25, stipulates that "personal data can be transferred to a third country only when the third country ensures the appropriate level of protection". In 2016, the EU adopted the GDPR and officially took effect on 25 May 2018, replacing the Data Protection Directive. [2]GDPR stipulates that its terms can be applied directly to and within the EU members without transformation, avoiding the differentiated results caused by understanding differences among the country members; in addition, GDPR proposes stricter standards for data protection, expands the extraterritorial effectiveness of the terms, tries to expand the jurisdiction to subjects outside the EU, improve the "adequacy protection level" and establish a whitelist system for cross-border data transmission, and defines the criteria and applicable conditions. The EU's "adequacy recognition" is mainly based on the domestic data legislation and the degree of protection of the third country. If the level of protection in the country is comparable to that of the EU, the data can flow freely to the third country, and no protective measures are required. As of April 2021, there were 12 countries and regions had met the "adequacy recognition" and entered the EU's "white list".[4] If the highest level of equal protection requirements are not met, cross-border data will be transmitted through appropriate safeguards and exception scenarios, such as Binding Corporate Rules,(BCR) and Standard Contractual Clause (SCC). The BCR is mainly for multinational companies with places of business within the EU. If no third country reaches the above level of protection, the GDPR also provides legal exceptions, such as data subject consent, exercise, or the legal right to defend.[3]

2.2 American regulatory path

As a capitalist power, the United States has developed the information technology industry and obvious advantages in data resources, which has brought great benefits to its economic development. Therefore, the United States has a relatively large demand for data flow. It emphasizes the high and free cross-border data flow, but it restricts the export of sensitive data and strictly controls it. [5]Since the United States attaches great importance to the huge economic benefits brought by data flow, and believes that hard law will hinder the cross-border data transmission and business behavior, its regulation and protection of personal information are scattered in various industries, and it does not form a unified and orderly legal regulation system at the legal level. In order to accelerate the development of the digital economy and promote the free cross-border data flow in the world, the United States continuously expands and deepens its free value concept in the market field during the FTAs negotiations, and advocates the inclusion of the freedom of data flow as a principle clause to restrict the data transmission barriers. [4]The Trans-Pacific Partnership (TPP) is an important international multilateral economic and trade negotiation organization. The TPP takes the special "e-commerce" train as a chapter, which greatly reflects the US data interests of —— to fully realize the free flow of data. Although some provisions are vague and set without clear application rules, it is the first time for the United States to push its own concept of data flow outside the domain, which plays an important role in building its voice in data governance around the world.Later, the United States

[4]Andorra, Argentina, Canada (business organization), the Faroe Islands, Guernsey, Israel, Mana, Japan, Jersey, New Zealand, Switzerland and Uruguay.
[5]The White Paper on the Rules and Mechanism Construction for the Cross-border Flow of Global and Chinese Data, released by the China Electronic Information Industry Development Research Institute and CID Blockchain Research Institute, August 2021.

ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

withdrew from the TPP, based on it,the rest of the countries reached the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). CPTPP inherits TPP 95% of the content, and formally modifies only the rules of cross-border data flow, which essentially reflects that countries with strong data power are exporting their legal systems and ignoring the interests of weak countries. In addition, the United States has taken multiple measures to limit the transmission of sensitive personal data. For example, the Foreign Investment Risk Review Modernization Act passed in February 2020 regards sensitive data as an important part of national security and conducts investment security reviews for cross-border transmission and transactions of sensitive personal data; In June 2021, President Joe Biden signed the Executive Order on Protecting American Sensitive Data against Foreign rivals, which states that foreign rivals can access and capture large amounts of information from applications, to prevent international security, and to conduct security assessments for applications related to foreign rivals.[5]

From the regulation path of cross-border data flow in Europe and America, it is not difficult to see that due to the huge differences between economy, politics and culture, there are differences in setting and protection of cross-border data flow clauses in different legal countries. At present, the relatively perfect regulatory pattern still remains at the regional level, and a sound international legal pattern has not been formed.

3. Cross-border data flow rules of RCEP

On November 15th, 2020, The Regional Comprehensive Economic Partnership (RCEP), which covers 15 member states, Including the developed and developing countries, Covering a population of 2.264 billion, With 29% of the global economy and 38.3% of global international direct investment, It is currently the free trade agreement with the largest population, the largest scale of commercial trade and huge development potential in the world; at the same time, It will also become the fourth major regional free trade zone in the world after EU, CPTPP and the US-Mexico-Canada Free Trade Zone (USMCA). The signing and rapid approval of the RCEP truly reflects the firm commitment to a fair and open multilateral trading system. It will effectively curb the development trend of "unilateral trade protectionism" and "anti-globalization", and will be conducive to the improvement of regional free trade and the multilateral system.[6]

RCEP did not take cross-border data flow as the content of its negotiations, but with the development of digital globalization, more and more free trade agreements put cross-border flow of data clauses in the FTA to promote the sound development of the digital economy. The RCEP's rules on the cross-border data flow are mainly distributed in Chapter 8 "Trade in Services" and Chapter 12 "E-commerce". Due to the large number of member countries and the development level and scale of digital economy, RCEP in an open attitude, from the perspective of benefit maximization, fully respect and inclusive of the laws and policies, allow cross-border free flow and limit data localization provisions,for example the "free data flow" as the basic principle, "data security flow" as the exception principle, considering the free flow and full protection of data.[7] The balance between Europe and the United States. It does not blindly limit the data flow and protect personal privacy, nor does it just pursue the economic benefits brought by the flow of data, but to focus on safe cross-border data flow.

3.1 Establish the principle of free cross-border data flow

Article 14 of RCEP, Chapter 12, specifies the location of computing facilities, where paragraphs 1 and 2 recognize that each party may have its own measures for the use or location of the computing facilities, including requirements seeking to guarantee communications security and confidentiality; but the parties shall not use the computing facilities within its territory as a condition of engaging in business within its territory. [6]Article 15 paragraphs 1 and paragraph 2 of "Cross-border Transmission of Electronic Information" provide that parties recognize that each party may have its own supervision over the electronic transmission of information; but one party may not prevent the covered electronic transmission of information across borders for commercial conduct. Both terms show that the party shall not restrict the location of computer facilities and cross-border transmission of data, and another party to commercial activities in its territory shall not take "computer facilities localization" measures, namely prohibit the implementation of data localization, therefore, the data flow here can be understood as "limited to the cross-border flow of commercial data".[8]At the same time, the States

[6]The RCEP terms are quoted from the Regional Comprehensive Economic Partnership Agreement (RCEP), published in the China Free Trade Zone Service Network.

ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

parties shall not impose unnecessary barriers to the cross-border data flow, and should follow the principle of free flow, which, in fact, is the core obligation set by the RCEP. Paragraphs 1 and 2 of Chapter 8, Trade in Services, Financial Services, Article 9, Information Transfer and Information Processing, provide that each Party may set its management requirements for information transfer and information processing;but shall not prevent information transfer or processing required for the daily operations of financial service providers in its territory, including data transfer electronically or otherwise. Annex II, article 4 of "Access and Use", provides that each party shall guarantee that another party's service provider may use public telecommunications networks and services to transmit information across borders within their territory, including internal corporate communications of such service providers, and access to the information contained in databases within any party territory, or information stored in machine-readable form.[9]

From the above terms, we can see that the RCEP does not set restrictions on the cross-border flow of important financial telecommunication data, allowing free cross-border flow, which further reflects the openness of the RCEP members at the negotiations.

3.2 Establish an exception principle for cross-border security interests of data

The exception principle of cross-border data flow established by RCEP is essentially a conditional restriction on the localized storage of data.The data transmission restriction requirement, which imposes certain conditions on the cross-border data flow in certain circumstances. The implementation of data localization storage is mainly derived from the traditional territorial protectionism. The RCEP member states have different laws and policies in the implementation of data localization, and the degree of data localization storage is also different,which can be divided into the following three categories: first, there are no data localization requirements; second, the copy of data can be stored in China and processed abroad. This category is mainly for telecommunication data and business financial data, usually to ensure regulatory requirements; third, the data can only be accessed, stored and processed in China, which is strictly prohibited. For example, Australia's 2012 The Personally Controlled Electronic Health Record (PCEHR in 2012) requires some personal electronic health information be stored, processed by local data centers, which is the most stringent data localization measures.[10]

Article 12 of RCEP "E-commerce" Article 14 "Location of computing Facilities" and Article 15 "Cross-border Transmission of Information through Electronics" both stipulate that the party is to achieve legal public policy.The Objectives and the national basic security interests may take the necessary measures for the cross-border transmission of data, provided that the measures do not act in a manner that constitutes arbitrary or unreasonable discrimination or disguised trade restrictions. Other Parties may not dispute such measures. [11]Therefore, the implementation of the exceptional principle must comply with the following four conditions: first, the public policy or national security implemented in the country is suffered or will be lost; second, not constituting arbitrary or unreasonable discrimination; third, not affecting the normal trade order; and fourth, not exceeding the maximum limit of the measures taken. Only if the above four conditions are met can the parties act to protect public policy objectives and basic national security interests to ensure the safe of cross-border data flow.

The RCEP fully respects the differences of development and regulatory in different countries, while allowing the free flow of data, and makes exceptions to the safe flow, which are never found in previous e-commerce agreements.

3.3 Progress of the RCEP cooperation programme

The RCEP's cross-border data flow rule is an inclusive program of multi-country cooperation and co-governance, which essentially embodies the concept of a data community of shared future and has obvious progress. It is briefly described as follows:

On the one hand, the RCEP states parties in negotiations considering the economic development differences and the difficulty of implementation rules and set the flexibility of differential treatment clause, shows that the RCEP states parties are aware that there is a "data gap" in the international community, for the developing countries to adapt to cross-border data transmission rules set a buffer period, as far as possible to balance the dividends between developed and developing countries. [12]For example, the RCEP states in some sections like Cambodia, Brunei Darussalam, Myanmar, the Laos and Viet Nam shall not be required to apply the relevant provisions of this paragraph for three or

ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

five years from the entry into force date of the agreement, and individual countries may extend it for three or five years if it's necessary.

On the other hand, the setting of differential treatment terms highlights the safe cross-border data flow advocated by the RCEP. The RCEP members include developed countries such as Japan, South Korea and New Zealand, undeveloped countries such as Cambodia and Laos, and developing countries with strong economic strength such as China.Cross-border data flow rules in developed countries, relatively relaxed,rules in developing countries are stricter, some countries are both RCEP and CPPTPP members, [7]and bring the principle of highly free rules into the RCEP negotiations. What is more progressive than the US model is that the RCEP sets basic national security interests as an exception to cross-border data transmission, and implements the policy of full data protection and free flow of data, which is regarded by the US will seriously hinder the free flow of data and violates its claim for an open digital trade environment. [13]In addition, most of the contracting parties of RCEP participate in the formulation of cross-border data flow rules, which, to some extent, will cause pressure on developed economies that have the right to speak in regulation, give birth to new competitive patterns and game processes, and objectively promote the evolution of the global regulatory system for cross-border data flow.

To sum up, RCEP data sovereignty and data security, respect the development of different countries, support safe and efficient data free flow rules, and different categories of countries when participating in data governance have certain voice, this fully embodies the RCEP regional data governance.

4. The influence of RCEP on the regulatory pattern of global cross-border data flow

RCEP is a regional free trade agreement which has responded positively to cross-border data flow rules after the WTO and CPTPP. RCEP's cooperative co-governance program has eased the pressure of fragmentation of cross-border data flow rules and insufficient institutional supply to some extent. RCEP members cover developed and underdeveloped countries. Based on data sovereignty, all countries formulate rules for cross-border data flow from the perspective of mutual respect to promote orderly cross-border flow of data through cooperation and share the dividends brought by data development. The cross-border data flow rules of RCEP are obviously progressive, different from Europe and the United States, so it has an important breakthrough impact on the existing global regulatory pattern of cross-border data flow.

4.1 A breakthrough in the European and American pattern

The United States and the EU rely on their respective dominance in digital trade and personal privacy protection to develop and lead the current orders and norms for cross-border data flow. The United States pursues the free flow of data and downplays the data sovereignty; the EU strengthens the data sovereignty, develops a single digital market, emphasizes the free flow of data within the EU, strictly restricts the data flow outside the region, and selects the digital trade partners by restricting the flow conditions. Although the rules of Europe and America have different priorities, they are all developing in the direction of free flow of data, but RCEP is different.

First, the RCEP is an FTA based on Asia and developed by Asian countries. The United States and the EU are not involved in the negotiations and are not a member of the RCEP, indicating that underdeveloped countries are aware of the importance of cross-border data flow. China and the Association of Southeast Asian Nations (ASEAN) have massive digital resources. In order to safeguard their own data interests, they began to actively participate in and lead the regional FTA negotiations. [14]RCEP integrates regional forces to export the beneficial experience of the contracting parties in the form of treaties, especially China, pushing the internal inclusive rules outside the region. In addition, it also shows that Europe can still develop better cross-border data flow rules, even better than Europe and the United States, and contribute to the Asian solution for the formation of unified rules for global cross-border data flow, leading the development trend of digital governance.

Secondly, the specific flow rules of RCEP are also different from those of Europe and the United States, and its cross-border flow of safe data is more in the interests of most countries in the world. In the post-epidemic era, countries with massive digital resources are rising as producers and consumers of cross-border data services. A large number of emerging economies begin to join the formulation of

[7]The RCEP and CTPPT overlap in seven countries: Japan, Australia, Singapore, Malaysia, New Zealand, Vietnam, and Brunei.

ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

cross-border data flow rules, formulate and implement rules systems in line with their own interests, and have an impact on the regulatory pattern in Europe and the United States.

Finally, after the European and American "safe port" agreement invalid "privacy shield" agreement effective five years later, on July 16,2020, the European court declared the European and American "privacy shield" agreement invalid, transatlantic data cross-border transmission chain fracture, shows that Europe and America data cross-border flow rules have certain disadvantages, cross-border flow of data still need security, and more rational thinking how to find data protection and data free flow balance. [15]Therefore, the formation of RCEP cross-border data flow rules will strongly impact the corresponding rules of Europe and America, and even combat the unilateral digital trade strategy system, beneficial Asian countries lead their own cross-border data flow regulation scheme. In the global data governance level, only by ensuring the equal participation of different types of countries and having the institutional voice, can we build a new digital trade order and promote a more fair, more open and more inclusive international digital legal pattern.

4.2 Impact on the WTO data flow rules

As the core trading system of the world, the WTO provides a guarantee for the development of international trade. However, with the decline of multilateralism and the rise of regional protectionism, and the obstruction of the United States to improve the WTO mechanism, the functional mechanism of the WTO has been damaged, and it is difficult to form unified rules for global hot issues. In view of this, China, Japan, the EU and other countries have repeatedly put forward improvement plans to the WTO many times, which also shows that the WTO is still an effective multilateral mechanism for unifying rules and handling disputes. On January 25,2019, along with the conclusion and signing of the Joint Statement on E-commerce, the WTO members launched the bilateral negotiations on e-commerce clauses, aiming to promote the development of the digital economy and establish new international trade rules. Since the WTO negotiations began, the world's major developed economies have dominated the negotiations, and different types of countries have disagreed on cross-border data flows. The WTO negotiations on cross-border data flow are based on the existing rules and their defects, due to the dominant position of Europe and the United States and the voice in system building. The United States strongly advocates the liberalization of digital trade, reducing the barriers to digital trade, advocating the rules and legal policies of free flow of data across borders and prohibiting data localization, arguing that only free data flow can promote the development of global digital economy and trade, and other developed economies hold basically the same view as the United States; The difference is that other developed economies such as the EU, Canada and Japan have added the regulation of cross-border data flow based on the concept of the US. The policies of advanced economies such as Europe and the United States will partly harm the interests of underdeveloped economies and further intensify the existing digital divide around the world. [16]Developing countries are also aware of the importance of cross-border data flow, but they do not blindly emphasize the importance of free data flow. Instead, from the perspective of security, they advocate that free cross-border data flow should be limited by certain exceptions, such as the protection of national interests and public policy objectives. Clearly, the RCEP's inclusive cross-border data flow rules advocate a safe and free flow of cross-border data, taking into account the level of digital development in different types of countries. With the signing and effectiveness of the RCEP, the implementation of the cross-border data flow rules in the region will certainly have a impact on the WTO e-commerce negotiations. The RCEP cross-border data flow rules not only establish rules in the interests of member states in Asia, but also will promote the further improvement and integration of rules at the international community in this field. As one of the four major trade agreements in the world, the RCEP pushes the WTO back to multilateral negotiations with a critical number of open cross-border negotiations by formulating regional cross-border data flow rules. Thus to the WTO data cross-border flow rules negotiations, accelerate the formation of a unified regulation pattern, its cooperation and governance scheme provides reference for the WTO e-commerce negotiations, opened a new idea, pay more attention to the position of developing economies, promote the formation of data governance pattern under the framework of WTO.

5. Adjustment cross-border data flow rules of China under the RCEP

In the era of digital economy, China's data scale is growing rapidly, and it is becoming increasingly important for economic development, people's lives, nation and social governance. China has also paid more attention to the legal regulation of cross-border data flow. Since the adoption of the Cyber

ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

Security Law in 2016, China has further strengthened the domestic regulation and legislation on cross-border data flow. After joining the RCEP, China should first consider the connection between the relevant regulatory measures and the RCEP cross-border data flow rules.

Firstly, further emphasis is placed on the principle of free data flow. Although China's current legislation allows the cross-border data flow,but the provisions are relatively vague, easy to cause unnecessary disputes, and is not conducive to the implementation of China's treaty obligations. Therefore, it is necessary for China to further emphasize the principle of free data flow in the Network Security Law, the Data Security Law and the Personal Information Protection Law, and better coordinate with the RCEP cross-border data flow rules. RCEP gives parties wide discretion, China on the basis of confirming the principle of cross-border free flow, in personal information and important data protection regulatory measures with the provisions of the RCEP, but still need to further improve the relevant supporting system, first try it in free trade area,Forming a replicable and feasible experience,, to meet the needs of digital trade development and data security protection.

Secondly, unified the definition of relevant concepts. It is mainly the definition of cross-border data exception terms in the laws and regulations of cross-border data flow in free trade agreements. The terms of the Cyber Security Law and the Data Security Law use "national security" and "public order" in the public interest, while the cross-border flow of FTA data exceptions such as the RCEP use the term "basic security interest". Given the fact that the basic security interests exception clause contains the self-ruling phrase "its opinion", if the panel kindly reviews China's measures to invoke the cross-border flow of the basic security interests exception regulation data, it is likely to examine the definition of the basic security interests in China's domestic law. [17]In this regard, it is suggested to unify the expression of interests in China's cross-border data flow legislation and the exception provisions of FTA, so as to help provide domestic legal guidance for the interpretation of possible disputes.

Thirdly, we will improve data classification and classification rules, and clarify the safety assessment standards for cross-border data flows. Clarify the security assessment standards for cross-border data flow, exit assessment measures should also be explicitly listed in laws and regulations or department regulations, such as the map management regulations, the automobile data safety management provisions " the relevant provisions, to avoid other contracting parties about national security, social order threat actually exists. In addition, China has established a data security evaluation system, but the evaluation standards have not yet been issued. Therefore, our country should accelerate the personal information exit security evaluation method, the data exit security assessment method and other supporting measures, determine the evaluation subject, clear evaluation standards and procedures,at the same time,to clarify and perfect the personal information cross-border transmission standard of the specific content of the contract terms and the specific way of personal information protection certification, in order to improve the operability of the rules.

Fourth, expand the "list of inconsistent measures" and expand the regulatory space for cross-border data flow in China.Discussing from the legislative level that the cross-border data flow regulatory measures can comply with the RCEP exception clause, China can also guarantee the policy space through the Commitment Form of Service and Investment Retention and Inconformity Measures in the negotiation process of joining CPTPP and DEPA.Article 3 of Chapter 12 of the RCEP also clearly stipulates that Article 15 "Cross-border electronic information transmission electronically" does not apply to the retention and inconsistency measures stipulated in the "Trade in Services" or "Investment" section. CPTPP 14, Article 2 also provides similar measures. In terms of "inconsistent measures", there is no lack of retention provisions that may be associated with data localization. For example, South Korea's irresponsible measures commitment table under the RCEP stipulates that it has the right to take any relevant regulatory measures for a state-owned electronic information system that contains proprietary government information or information collected by the government according to its regulatory functions and powers. [8]The system will necessarily involve the cross-border flow of national security or public order information. Therefore, in our country's future CPTPP and DEPA treaty negotiations, can adopt this model, in making inconsistent measures promised, For areas and industries with possible important cross-border data or information, it is clear that the "electronic cross-border information transmission" clause does not apply, thus providing clear legitimacy for the regulation of cross-border data flow in this field in China.

[8]RCEP, ANNEX III,Schedule of Reservation and Non-Conforming Measures for Services and Investment,Korea.

ISSN 2706-6827 Vol. 4, Issue 9: 113-120, DOI: 10.25236/IJFS.2022.040918

References

[1] Mitchell, A., & Mishra, N. (2021). WTO Law and Cross-Border Data Flows: An Unfinished Agenda. In M. Burri (Ed.), Big Data and Global Trade Law (pp. 83-112). Cambridge: Cambridge University Press. doi:10.1017/9781108919234.006

[2] Xu Duoqi. International pattern of cross-border flow of personal data regulation and China's response [J]. Law Forum, 2018, 33 (03): 130-137.

[3] Sun Nanxiang. CPTPP digital trade rules: institutional game, standard differences and China's response [J / OL]. Academic Forum: 1-10 [2022-07-18]. DOI:10.16524/j.45-1002.20220701.001.

[4] Dan Jerker B. Svantesson, The regulation of cross-border data flows, International Data Privacy Law, Volume 1, Issue 3, August 2011, Pages 180–198, https://doi.org/10.1093/idpl/ipr012

[5] Wu Weiguang. Criticism of Personal Data Information Private Rights Protection under Big Data Technology [J]. Politics and Law, 2016(07):116-132. DOI:10.15984/j.cnki.1005-9512.2016.07.011.

[6] Xu Chengyujin. WTO E-commerce Rules negotiation and China's response plan [J]. International Economic Review, 2020 (03): 29-57 + 4.

[7] Susan Aaronson. Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security [J]. World Trade Review. 2015 (4).

[8] Mattoo Aaditya, Meltzer Joshua P. International Data Flows and Privacy: The Conflict and Its Resolution [J]. Journal of International Economic Law. 2018 (4).

[9] Yakovleva S., Irion K. The Best of Both Worlds? Free Trade in Services and EU Law on Privacy and Data Protection [J]. European Data Protection Law Review. 2016 (2)

[10] Zhang Yu. The application dilemma of international Investment Protection Rules under the rise of data localization measures [J]. Wuhan Review of International Law, 2021, 5(04): 139-157. DOI: 10. 13871/j.cnki.whuilr. 2021.04.012.

[11] Li Dongdong. Evolution, differences and enlightenment of the path of digital trade liberalization in the Asia-Pacific region [J]. Asia-Pacific Economy, 2021 (04): 23-32. DOI:10.16407/j.cnki. 1000-6052.2021.04.003.

[12] Willemyns Ines. Agreement Forthcoming? A Comparison of EU, US, and Chinese RTAs in Times of Plurilateral E-Commerce Negotiations [J]. Journal of International Economic Law. 2020 (1)

[13] Wu Chien-Huei. ASEAN at the Crossroads: Trap and Track between CPTPP and RCEP [J]. Journal of International Economic La. 2020 (1)

[14] Jie Huang. Comparison of E-commerce Regulations in Chinese and American FTAs: Converging Approaches, Diverging Contents, and Polycentric Directions? [J]. Netherlands International Law Review. 2017 (2)

[15] Li Mosi. CPTPP + Digital Trade Rules, Influences and Countermeasures [J]. International Economic and Trade Exploration, 2020, 36(12):20-32. DOI:10.13687/j.cnki.gjjmts. 2020.12.002.

[16] Ma Qijia, Li Xiaonan. Research on Cross-border Data Flow Regulatory Rules under the Background of International Digital Trade [J]. International Trade, 2021(03): 74-81. DOI:10. 14114/j.cnki.itrade. 2021.03.010.

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