Proceedings of the 2023 International Conference on Management Research and Economic Development
DOI: 10.54254/2754-1169/21/20230236

An Ingenious Study on the CPTPP's Governance of Cross-Border Data Flows

Wenxin Shan[1,a,*]

[1]*School of Law, Capital University of Economy and Business, Beijing, China, 100070*
a. vincyshan@outlook.com
**corresponding author*

Abstract: Obviously, due to the continuous development of Internet technology, transnational data flows brought about by e-commerce and other Internet enterprises have become the target of various countries' attention and searches for new governance solutions. By studying numerous laws and regulations, international treaties and related literature, this paper examines the differences between the traditional European and American governance systems for cross-border data flows and the high-standard regional trade agreements represented by the CPTPP in a comparative manner. The comparative study concludes that international treaties such as the CPTPP focus more on and takes into account the realities of developing countries than Europe and the United States, while the European and American systems are more inclined to dominate the content of international inter-treaties based on their own ideas.

Keywords: CPTPP, cross-border data flows, the U.S., EU, RCEP

1. Introduction

Due to the continuous development of Internet technology, the flow of data across borders has become more and more important, but things are not so simple, because it involves user privacy and even national security. In response to these issues, various countries or alliances have developed their own standards, which inevitably leads to conflicts and contradictions. And with the suspension of the WTO, a unified standard is not available globally, so this paper examines different regimes of data flow regulation by comparison. The intention is to identify the regimes and regulatory measures that best meet the current development needs, especially for developing countries. Likewise, it provides references to support the domestic legislation of other high-standard regional agreements or countries.

2. Comparison of Systems

2.1. Specific Instruments for the Governance of Cross-Border Data Flows in the U.S. and Europe

2.1.1. The United States.

In terms of bilateral treaties, the Safe Harbor Agreement and the Privacy Shield Agreement, signed with the EU in 2000 and 2005, respectively, provide legal support for the flow of data between Europe and the U.S. Despite the obvious differences between the parties, the parties still agreed in the agreement that they must obtain authorization from the data owner and ensure the security of the data,

DOI: 10.54254/2754-1169/21/20230236

as well as the consequences of the violation such as violating the data privacy of others. However, both of these agreements were declared invalid by the European Court of Justice because the United States unilaterally did not strictly abide by these two agreements. On the international front, under the impetus of the U.S., the OECD established the OECD Guidelines in 1980, which emphasized avoiding state intervention and advocated to secure the personal data through market principles, especially industry self-regulation. Since then, the U.S. has pursued data liberalization as the core flow rule within the APEC mechanism. Among the NAFTA and the USMCA provide that contracting parties shall provide favorable conditions for the free flow of data and that each Party shall minimize legal and institutional restrictions on data flows. The Trans-Pacific Partnership Agreement, the U.S.-Japan Trade Agreement, and the U.S.-Japan Digital Trade Agreement contain provisions prohibiting data localization measures. In summary, the U.S. has emphasized the free flow of data across borders in all aspects, and the U.S., through its pivotal international position and economic volume, has promoted the concept of individuals in international trade formulation and, through its position in bilateral agreements, has strongly dominated the formulation of agreements with Japan, South Korea, Mexico, Canada, and other countries, and its prohibition of data localization is aimed at entering the markets of data localization countries. However, the U.S. has applied a "double standard" for governing cross-border data flows internally and externally: the U.S. government has set many restrictions and requirements for its domestic data to leave the country. For example, some domestic laws, such as the Data Security Act of 2020, the Foreign Investment Risk Review Modernization Act, the CLOUD Act, and Executive Order 13556 restrict and require foreign network operators to store communication data, transaction data, and user data in the US, and the communication infrastructure must also be installed in the US. At the same time, personal data is considered a component of national security, and transactions involving personal data are included in the scope of the foreign investment security review, and all prohibit the flow of data to foreign countries on the grounds of national security. Therefore, although the governance of cross-border data flow in the U.S. is very perfect and mature for itself, it does not have reference value for the formulation of international trade agreements and other free trade agreements.

2.1.2. EU.

GDPR's export of personal data is very strictly limited, for example, in Chapter 5 it is explicitly stated that personal data may be transferred to a third country or international organization if the Commission determines that a sufficient level of protection is ensured in the third country, territory or one or more specific sectors within that third country or international organization concerned. Therefore, personal data can only be allowed to flow out of the EU to flow only to countries or regions that the EU recognizes as providing "adequate protection" or adopting "appropriate safeguards." And the EU needs to determine that it is "sufficiently protected," thus forming the core of the EU data flow governance system. The conditions for the determination are, firstly, whether the domestic legislation is in line with international rules. Secondly, whether there is a domestic regulatory body to ensure the precise implementation of the data protection law. Thirdly, whether the international commitment is willing to assume international responsibility. After these conditions are met, the EU will continue to review and monitor the situation. And if the standard of adequate protection is not met, “data controllers and processors are required to provide appropriate security measures, mainly Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs), etc [1].” In addition, on June 21, 2021, the European Data Protection Board (EDPB) issued additional measures for data transfers. The first is about encryption. Encryption only serves as a supplementary measure to provide adequate protection during the flow of data across borders. The second is the issue of relief. This supplementary measure requires data import and export organizations to provide assistance in obtaining remedies for data subjects, or even compensation directly from these organizations. At the

DOI: 10.54254/2754-1169/21/20230236

same time, the bill stipulates that non-personal data should be free from foreign government surveillance in the same way as personal data, in order to hedge against the impact of the US CLOUD Act. The core claim of the bill is to build an adaptable rule framework for EU internal and cross-border data flow, simultaneously maintain the security of data cross-border transmission and strengthen EU data sovereignty. Therefore, “the specific rule-making of the bill also shows the characteristics of one and two standards [2].”

The Data Act starts with the principle that "every user, whether an individual or an organization, should have the right to access the data that he or she generates." On this basis, the Data Act allows users of connected products to access the data generated by them. On the other hand, the Act is specifically designed to protect SMEs from unfair contractual terms and exemptions proposed by a stronger Party, and to establish standardized contractual terms in favor of fairness. Not only that, but the government departments may also have access to data held by the private organizations in specific circumstances, such as public emergencies and legal authorizations. To this end, the Act also devotes a great deal of space to elaborate on the operational rules and detailed pathways used to remove practical barriers to the flow, use and sharing of data, building a fairer and more complete system of rights and responsibilities. For the cross-border flow of non-personal data, the Data Act provides a special chapter, and its restrictions are as strict as those of the GDPR for personal data. First, the applicable scope of the Act is determined by the subject, not limited to the EU. Secondly, “the Act has designed five mechanisms to regulate the transfer of non-personal data outside the EU [3].” Although the introduction of the Data Act effectively fills the gap in the EU data cross-border regime, it also sets more obstacles for the cross-border flow of non-personal data to third countries in order to effectively restrict non-EU countries' access to non-personal data in the EU through local legislation. As mentioned above, the data law has more detailed and strict rules on cross-border data flow than the GDPR. However, only 13 countries in the world have met the "adequate protection" standard required by the GDPR and are allowed to conduct data flows with the EU. Therefore, it is clear that such a high standard system is undoubtedly an obstacle to economic development, and does not have much constructive reference value for countries entering into agreements for the purpose of facilitating trade.

2.2. Provisions on Governance of Cross-Border Data Flows in High-Standard Regional Trade Agreements, Mainly CPTPP

2.2.1. CPTPP.

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), a free trade area composed of Asia-Pacific countries, also is an upgraded name for the agreement after the U.S withdrew from the Trans-Pacific Partnership (TPP). The topic of Chapter 14 is "E-Commerce." Although it adopts the name of electronic commerce, actually it contains rules on the governance of cross-border data flows. With respect to the development of domestic law on the free flow of data, Article 14.4 provides that Parties should minimize or avoid imposing any unnecessary burden of regulation on electronic transactions and facilitate input from stakeholders in the process of developing a legal framework for electronic transactions. In terms of exceptions to the free flow of data, Article 14.11 emphasizes that Parties shall permit the cross-border flow of data, including personal information, if such activity is for the insured's business activities. This is the core provision of the CPTPP data cross-border flow rules and a mandatory obligation set for the Parties. Although paragraph 1 allows Parties to set regulatory requirements and does not specify the extent of regulation, in conjunction with paragraph 2, the CPTPP actually requires the extent of such regulation, i.e., regulation to the extent that it does not impede the cross-border flow of data. The third paragraph of Article 14.11 provides that nothing in this Article shall prevent a Party from pursuing a legitimate

DOI: 10.54254/2754-1169/21/20230236

public policy objective by introducing or preserving a measure, not in conformity with Article 2, provided that the measure: (a) not be applied in a form that will amount to either deliberate or unreasonable discrimination or a de facto restriction on trade, and (b) not apply limitations to the transmission of such information beyond those necessitated by the achievement of the objective. In addition, paragraph 3 of Article 14.2 expressly excludes government procurement and government information from the scope of application of Chapter 14. The definition of "applicable person" in Article 14.1 also expressly excludes "financial institutions" from the scope of application of that Article. In short, a significant number of public policy exceptions to the cross-border data flow rules remain in the CPTPP. In terms of cross-border data transfers, Article 14.13 provides that members shall not require that businesses use or set up their electronic computing facilities locally as a condition for allowing them operate locally. In short, members are prohibited from imposing local storage requirements. However, the CPTPP clarifies that governments may require any official information, such as critical facilities planning, confidential-level policy proposals, or social security information, to be stored on local servers, which indicate, first of all, the recognition of the autonomy of Contracting States to adopt different legal approaches to the protection of personal information, “as well as the autonomy of regulation in this matter, including the power to establish data localization measures” [4], etc. In addition, it also has comprehensive provisions in the area of data protection. However, this does not mean that the CPTPP is very lenient in terms of data protection requirements, with respect to the protection of personal information, rather Article 14.8 requires “ Parties to provide protection information in the face of e-commerce users, including at least how natural persons can seek avenues of redress and the relevant compliance practices required by the business” [5]. Considering that Parties may take different legal tools to the protection of personal information, each Party shall make its best efforts to support and facilitate the establishment of mechanisms for compatibility between these different systems. These mechanisms include recognition of regulatory outcomes and are awarded either autonomously, through joint arrangements, or within a broader international framework.

2.2.2. RCEP.

RCEP was signed later than CPTPP, and its leading countries are the ten ASEAN countries, and invited other Asian countries to participate together, so most of them are developing countries. With the current rapid development of the Internet economy, transnational data flows brought about by e-commerce and other Internet enterprises have become the target of various countries' attention and search for new governance solutions. By studying numerous laws and regulations, international treaties and related literature, this paper examines the differences between the traditional European and American governance systems for cross-border data flows and the new high-standard regional trade agreements represented by CPTPP in a comparative manner. For example, Article 12.4 cooperation: Parties should cooperate, as appropriate, to (a) work together to assist SMEs in overcoming barriers to the use of e-commerce; (b) establish targeted areas of partnership between Parties to help them enforce or enhance their legal frameworks for e-commerce, such as research and training activities, competence building and the availability of technical aid; 12-4 (c) communicate information, experiences, and best practices to overcome challenges associated with the promotion and use of electronic commerce; (d) encourage the business industry to develop methods or practices that will enhance transparency and consumer confidence in order to stimulate the use of electronic commerce; and (e) engage actively in both regional and the multilateral fora to further the development of electronic commerce. Parties should strive to achieve formats of cooperation that are based on, rather than overlapping with the existing cooperation initiatives in international forums. With respect to the electronic cross-border transmission of information, Article 15 adopts a different formulation than the CPTPP, changing the exception clause from "limitations beyond those necessary

DOI: 10.54254/2754-1169/21/20230236

to achieve the objective" to "any measure necessary to protect its essential security interests. Such measures may not be rejected by other Parties."

3. Conclusion

To sum up, this paper has comparatively studied the rules of the two systems of the UK and the US for the governance of cross-border data flows and summarized the characteristics of each of the two club systems, i.e., one espouses the protection of personal privacy and the other values the economic development brought by data flows. In addition, this paper introduces high-standard RTAs for comparison based on the two systems in Europe and the United States. As a result, this paper investigates how emerging data flow regulation provisions differ from traditional ones. In summary, the CPTPP exception is intended to state that each member may require the localization of facilities or restrict the cross-border flow of data if there is a need to achieve a legitimate public interest that requires reasonableness, nondiscrimination, and does not disguise regulation of trade; or if there is a need to protect essential national security interests and does not create divisions among the other members. Compared with the USMCA, which has no exceptions and strictly prohibits data localization, the CPTPP has few provisions for cross-border data flow, but it takes into account the dual objectives of national security and industrial development, and maximizes the consideration of the realistic needs of different countries. This is constructive for the development of the digital economy in the whole region. Therefore, the signing of CPTPP represents that the global governance system for cross-border data flows is gradually moving away from the U.S.-Eurocentric system, and developing countries are beginning to spontaneously seek a new governance system that suits their own development models. However, the EU data law is currently only a published draft. As well as domestic legislation in the United States, this study does not do a detailed comparative analysis, but only cites classic laws. Therefore, the research in this area needs a lot of information for further support. In addition, for high-standard regional trade agreements only, there are only a dozen countries in the world that have joined, and their representation is very limited, so the CPTPP solution can only represent the positions and views of a few economies in the world, and cannot be applied to all countries.

References

[1] *European Union. (2018) General Data Protection Regulation, Chapter Ⅳ, Section 5, Article 41*

[2] *Six Tone. (2022) Global Digital Governance | EU Data Act "One and Two Standards" of Data Flow Governance, https://finance.sina.com.cn/jjxw/2022-03-25/doc-imcwiwss8121995.shtml#:~*

[3] *European Union. (2018) Data Act (draft), http://www.ecas.cas.cn/xxkw/kbcd/201115_129085/ml/xxhzlyzc/202203/t20220322_4570243.html#:~:text*

[4] *Huang Shixi. (2022). Data localization regulation and security exception defense in Cptpp. International Trade (11), 81-87.*

[5] *Ma Qian and Li Zhiyi. (2022). On the legal regulation of the cross-border flow of cptpp data. Journal of Jingdezhen University, 37(5), 64-70.*