ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

Improvement Path for Cross-Border Governance Rules of Personal Data from an International Perspective

Jiayue Yan[1,a,*]

[1]*Law School, Beijing Technology and Business University, Beijing, China*
[a]*2281632103@qq.com*
[*]*Corresponding author*

Abstract: *In the current era of data, it is important to focus on the issue of cross-border governance of personal data, particularly in the weak link of data transmission. After understanding the current legislative situation in China, we examine the historical evolution of rules governing cross-border governance of personal data and explore effective legislative models. We also review typical international legislative examples and draw on their legislative experiences. Finally, taking into account the current situation in China, which relies on a system of personal data governance with dispersed legal provisions and vague specific regulations, we propose actively participating in large-scale bilateral trade agreements and exploring solutions using such agreements to improve specific domestic regulations. Starting from the legislative source, we provide suggestions to improve rules for cross-border governance of personal data and contribute to the development of China's digital economy.*

Keywords: *cross-border personal data, international rules, free trade agreements*

1. Introduction

In 2022, China's digital economy reached a scale of 50.2 trillion yuan, with a year-on-year nominal growth of 10.3%, which has significantly outpaced the nominal GDP growth rate for 11 consecutive years, and the proportion of the digital economy to GDP reached 41.5%. At the same time, the European Union's Digital Decade policy plan aims to achieve digital transformation, enhance digital sovereignty, and build a resilient and competitive Europe by 2030. To support the implementation of this plan, the EU is expected to directly invest around 165 billion euros. On October 18, 2023, during the third Belt and Road Initiative International Cooperation Forum, China and 34 countries jointly released the "Initiative on International Economic and Trade Cooperation in Digital Economy and Green Development," focusing on the digital and green sectors and adhering to the principles of voluntarism, flexibility, pragmatism, and open development, aiming to jointly build a new era of green digital economic and trade "Silk Road. " In the flourishing development of the digital economy, frequent data transmission activities bring about efficient and convenient people's lives, but they also hide risks in terms of data security.

In the process of cross-border governance of personal data, the transmission link is the weakest, and in recent years, there have been frequent abuses of cross-border transmission of personal data. From the "Prism Gate" incident exposed in 2013 to Huada Gene's unauthorized transmission of some human genetic resource information abroad without national security review and permission in 2015, and to the present large-scale transnational telecommunications fraud groups using personal data for fraudulent activities. Data shows that since the beginning of the 21st century, there have been as many as 2,348 cases of abuse of personal data in China. The abuse of cross-border transmission of personal data not only threatens the personal safety and property of individuals, but also poses a threat to national security. At the same time, various countries have introduced specific rules for the governance of cross-border transmission of personal data, such as the United States, the European Union, and others. Drawing on relevant international governance experiences, the formulation of effective rules for the governance of cross-border transmission of personal data can efficiently address the problem of abuse in cross-border transmission of personal data.

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

2. Current Status of Cross-border Governance Rules for Personal Data in China

Compared to other countries and regions, China's legislation on cross-border governance of personal data started relatively late. The "Guidelines for Information Security Technology - Personal Information Protection in Public and Commercial Services Information Systems," implemented in 2013, first addressed the issue of cross-border data transfer. Subsequent laws and regulations focused more on the protection of personal information, indirectly touching upon the issue of cross-border transmission of personal data. It was not until the introduction of the "Cybersecurity Law" that China began to pay attention to the issue of cross-border transmission of personal data and established clear and specific legal rules.

Currently, the cross-border governance of personal data in China is part of the overall framework for personal data governance. However, it has a small and fragmented proportion within this framework, and some legal provisions are rather vague. For example, in the "Personal Information Protection Law," the third chapter specifically addresses cross-border transfer of personal data, but it only consists of six legal provisions, accounting for only about 8.1% of the entire law. The "Data Security Law" only includes one provision mentioning cross-border data security, and it is quite ambiguous. In the "Cybersecurity Law," security review requirements are only specified for the provision of personal information and important data collected and generated by operators of critical information infrastructure within the country to overseas entities. With the development of technology, the scale and speed of cross-border transmission of personal data are increasing. In response, China needs an efficient and clear set of governance rules to quickly address this issue. This is crucial for effectively mitigating the security risks associated with cross-border transmission of personal data and harnessing its potential for facilitating cross-border trade and communication.

2.1 Relying on the framework for personal data governance

The cross-border governance of personal data in China is carried out within the framework of personal data governance, and there is significant overlap between the frameworks for personal data governance and overall data governance. According to incomplete statistics, China currently has nearly 70 laws and regulations related to the protection of personal data, as well as 10 judicial interpretations and nearly 200 departmental regulations. [1] Currently, China's framework for the governance of personal data mainly consists of the "National Security Law", "Personal Information Protection Law", "Data Security Law,", "Cybersecurity Law", "Regulations on Cybersecurity Review", and "Measures for Security Assessment of Exporting Personal Data." Within this framework, the cross-border transmission of personal data is primarily governed by the Cyberspace Administration of China (CAC) and relevant departments under the State Council, in accordance with the "Measures for Security Assessment of Exporting Personal Data." However, these governance efforts must not violate the provisions of the "National Security Law," "Personal Information Protection Law," "Data Security Law," and "Cybersecurity Law" regarding the infringement of citizens' privacy rights, personal and property safety, and national security.

2.2 Fragmented nature of cross-border governance rules for personal data

Internationally, many countries have established dedicated legal frameworks to govern the issue of cross-border data transfers. Practical experience has shown that having a specialized legal framework is effective in addressing related issues. In contrast, the rules governing the cross-border governance of personal data in China are scattered. Currently, there is no specific law that regulates the cross-border transmission of personal data. The "National Security Law" serves as the foundational law for governing cross-border data transfers, but the specific provisions regarding cross-border governance of personal data are dispersed within the framework for personal data governance. According to Article 36, Article 38, and Article 41 of the "Personal Information Protection Law" and Article 31 of the "Data Security Law," as well as Article 37 of the "Cybersecurity Law," personal data must undergo security assessments conducted by the CAC and relevant departments under the State Council before being allowed to be transferred across borders. Therefore, the security assessment system is the primary means of addressing the issue of cross-border transmission of personal data in China. The standards for the security assessment system are defined in the 2022 version of the "Regulations on Cybersecurity Review" and the "Measures for Security Assessment of Exporting Personal Data."

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

2.3 Ambiguity in specific provisions

Although there is no specific legal framework dedicated to the governance of cross-border data transfers, China has established basic governance rules. However, due to practical requirements and incomplete research, some specific provisions still need further clarification. For example, the specific provisions and relevant standards for the security assessment system require further clarification.

In addition to the top-level design of the legal framework, China's security assessment system for governing cross-border personal data transfers needs further improvement. Article 7 of the 2022 version of the "Regulations on Cybersecurity Review" stipulates that network platform operators with access to personal information of more than one million users must undergo a cybersecurity review when seeking overseas listings. This provision supplements the 2020 version of the "Regulations on Cybersecurity Review," which was introduced in response to the listing of Didi Chuxing and its specific circumstances. Subsequently, the Cybersecurity Review Office initiated security assessments for a series of network platform operators that hold a large amount of personal data, such as "Yunmanman," "Huochetou," "BOSS Zhipin," and "Micron Technology."

Regarding the relevant rules for cross-border governance of personal data, further clarification is needed for criteria concerning identifiability and the standards for important data. Article 4 of China's "Personal Information Protection Law" defines personal information as various pieces of information recorded electronically or by other means that are related to identified or identifiable natural persons, excluding information that has been anonymized. The criteria for identification or identifiability are presented in contrast to de-identification and anonymization. Article 73, paragraphs 3 and 4 of the same law provide definitions for de-identification and anonymization, but these definitions are only principle-based and relatively vague, requiring further clarification. Article 4 of the "Measures for Security Assessment of Exporting Personal Data" states that data processors must declare data exports to the competent provincial-level CAC before providing data to overseas entities under certain circumstances. In summary, a security assessment is required when transmitting a certain quantity of personal data or when transmitting important data to overseas entities. Article 19 of these measures also defines the concept of important data, but the description is relatively broad and not conducive to companies and individuals complying with the obligation to declare security assessments, nor is it beneficial to regulatory oversight by security assessment agencies.

3. Historical Evolution of Cross-Border Governance Rules for Personal Data

To explore effective legislative models, let's take a look at the historical evolution of cross-border governance rules for personal data. Based on the periods when governance rules played a major role, the development of governance rules for personal data can be roughly divided into three stages: initial emergence in domestic laws, subsequent introduction of regional laws, and the current trend of countries leaning towards free trade agreements to address practical issues.

3.1 Emergence in Domestic Laws

The emergence of personal data protection laws can be traced back to the 1970s, during the rise of the third generation of computers when computer software was widely used in various data aggregation fields such as aerospace, weather forecasting, and military applications. In this process, a large amount of personal data was collected, processed, and utilized, raising concerns about the security of personal data. Sweden, the United States, Germany, and France were among the first countries to enact national-level personal data protection laws, serving as models for subsequent legislation in the field of personal data protection.

In 1973, Sweden enacted the world's first national-level "Data Act." The law introduced specific regulatory requirements for data controllers and data users, setting different norms for the public and private sectors, and providing corresponding civil and criminal remedies. Compared to the "Data Act," the United States passed the "Privacy Act" in 1974, which primarily regulated government actions, emphasizing the basic rights of U.S. citizens to access and modify personal information and protecting personal information as part of individual privacy. The concepts and content of Germany's "Federal Data Protection Act" (BDSG) in 1977 and France's "Law on Data Processing, Data Files, and Individual Liberties" (La loi n°78-17 du 6 janvier 1978 relative a l'information, aux fichers et aux libertés) in 1978 were similar, with the notable feature of categorizing personal data for management purposes, distinguishing between the public and private sectors, and internal and external commercial use.

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

Initially, the purpose of enacting personal data protection laws was mainly to regulate the misuse of personal data brought about by automated technologies. Since citizens' electronic records were mainly held by governments and individuals at that time, the legislation primarily focused on specific requirements for governments and individuals, neglecting the significant impact of businesses. [2] With the development and advancement of internet technology, businesses gradually became the main developers and controllers of computer technology, as well as holders of a large amount of personal data. In the 21st century, the regulatory scope of personal data protection laws shifted from government and individual actions to focusing on business practices.

3.2 Rise of Regional Law

The European Union (EU) is a pioneer in modern legislation on personal data protection and has established successful regional laws. At the inception of legislation on personal data protection, the legal basis was the protection of privacy rights. In 1950, the European Commission formulated the European Convention on Human Rights, which for the first time included provisions on the right to privacy. Through a broad interpretation under European human rights law, this provision also came to protect personal data. This marked the European Commission's first attempt at legislation in the field of data. Over the next forty years, the European Commission intermittently issued various resolutions on data protection, as well as the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, also known as Convention 108, enacted in 1981. However, these efforts did not yield concrete results. [3] During the legislative exploration phase, the European Commission's legislation was indirectly applied through the domestic legislation of member states rather than being directly applicable to each member state. In this process, the EU was unable to enforce unified legislative standards, resulting in significant discrepancies in personal data protection legislation enacted by individual member states. This greatly hindered the development of a single market within the EU. Consequently, after five years of negotiations, the EU adopted the Data Protection Directive in 1995. The directive aimed to harmonize the level of personal data protection legislation among member states, overcome barriers to the flow of personal data within the EU's single market, promote free trade, and protect fundamental rights within the EU community. This marked the first achievement of unified personal data protection rules within the EU and set it on a path from fragmentation to integration.

In a judgment on the case of Google Spain v. AEPD and Mario Costeja González in 2014, the European Court of Justice stated, "The free movement of information is of vital importance, but it cannot outweigh the need to safeguard dignity, privacy, and data protection within the European legal order." This statement reflects the EU's belief that the right to personal data protection is a fundamental right of its citizens, a value concept that it consistently upholds. Subsequently, the EU enacted the General Data Protection Regulation (GDPR), which differs from previous data protection rules. The GDPR establishes stricter standards for the protection of personal information, as well as unified procedural and implementation standards. The GDPR is considered a crucial component of the EU's "Digital Single Market" strategy. As the integrated rules for personal data protection within the EU, it has made outstanding contributions to promoting the free internal market of the EU and represents the highest level of data protection rules in the EU at present.

3.3 The Free Trade Agreement is Flourishing

Diverse domestic legislative standards among countries, combined with generally high standards of regional legislation, and the current international situation, which makes it difficult for countries to reach unified international rules, have all led to high compliance costs for businesses entering the market. Therefore, in the current practice, countries tend to conclude multilateral or bilateral free trade agreements to address the issue of cross-border transfer of personal data. Typical free trade agreements include the Regional Comprehensive Economic Partnership (RCEP), the United States-Mexico Agreement (USMCA), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), and the Digital Economy Partnership Agreement (DEPA). A Free Trade Agreement (FTA) refers to a trade agreement signed by two or more countries (including separate customs territories) to achieve trade liberalization between them. It promotes trade flow by reducing tariffs and opening up market access. FTAs are established based on Article 24 of the General Agreement on Tariffs and Trade (GATT) and Article V of the General Agreement on Trade in Services (GATS). They directly or indirectly incorporate the content of the World Trade Organization (WTO) agreements on free trade. Some scholars consider FTAs as supplements to the WTO's free trade framework and as "subsequent law" to WTO agreements. Therefore, in judicial practice, FTAs can refer to WTO cases for interpretation. [4]

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

4. Typical Legislation on Cross-Border Governance of Personal Data

To gain a deeper understanding of the international cross-border governance rules for personal data, it is valuable to examine influential examples and analyze their characteristics through comparative law, drawing on legislative experiences. For example, the Cloud Act in the United States, the GDPR in the European Union, the CBPR in APEC, as well as the RCEP, USMCA, CPTPP, DEPA, and other free trade agreements.

4.1 Extraterritorial Applicability: GDPR and the Cloud Act

The Clarifying Lawful Overseas Use of Data Act (Cloud Act) in the United States and the GDPR enacted by the European Union both possess strong extraterritorial effects. Both are based on the principle of personalism and extend their applicability beyond the geographic scope of individual countries or regions. This not only affects the establishment of compliance systems within multinational corporations but also influences the legislation of other countries and regions. The former belongs to domestic law, while the latter belongs to regional law. However, it is worth noting that the approaches taken by these two regulations to extend their applicability beyond their territories differ.

4.1.1 GDPR in the European Union

The GDPR employs the subjects within the European Union as the basis for its extraterritorial reach. As a region with early development in global personal data protection laws, Europe's historical development in this area holds significant value for the establishment of relevant laws in other countries or regions. The GDPR is an integrated set of rules for data protection within the European Union. Unlike previous regulations, the GDPR establishes stricter standards for the protection of personal information, as well as uniform procedures and implementation standards. As a regional governance rule, the GDPR significantly expands its territorial scope within the European Union. The GDPR applies mandatorily to the processing of personal data within the European Union when an establishment exists within the EU, to the processing activities of personal data pertaining to individuals within the EU, and to the processing activities of personal data governed by EU law chosen under international law. In the process of governing cross-border transfer of personal data, the GDPR can be directly applied as a legal basis. Throughout the entire process, from the collection of personal data by data subjects within the EU to its cross-border transfer and subsequent processing outside the EU, the GDPR can exert direct governance effectiveness, rapidly and effectively safeguarding the security of personal data.

After the introduction of the GDPR, there was a trend of legislation globally using the GDPR as a model in the field of data protection. Australian scholar Greenleaf conducted two empirical surveys in 2012 and 2017, which revealed that before the GDPR came into effect, among 101 countries or regions surveyed with data privacy laws in 2011, only the 28 EU countries or regions adopted legislation based on the "Data Protection Directive." However, in the 2017 survey of 120 countries or regions, more than 54 countries or regions referred to the GDPR, which had not yet come into effect in the EU, in their legislation. [5] [6]Why does the GDPR have such widespread influence? American scholar Bradford proposed the theory of "market-driven synergistic effects" to explain this phenomenon from an economic perspective, and named this phenomenon after the location of EU legislative institutions—Brussels—as the "Brussels Effect." [7]

Indeed, the progressiveness of the GDPR is evident. It transforms the legal framework for protecting citizens' fundamental rights into a law that promotes and safeguards the development of the EU's digital economy. However, some scholars question its institutional flaws. [8] The GDPR's high level of protection standards is overly rigid, emphasizing only the rights of individuals. This leads to high costs for other countries and regions accessing the EU market and to some extent hinders the flow of personal data. This deviates from its original intention of promoting the protection and development of the EU's digital economy. Furthermore, among the pathways for cross-border transfers established by the GDPR, only 15 countries meet the adequacy requirement, while other countries still rely on alternative restricted methods such as Binding Corporate Rules (BCRs) and Standard Contractual Clauses (SCCs). Despite providing a convenient pathway for free transfers, the high threshold for adequacy recognition has practically halted this approach, failing to achieve the expected goal of secure and swift personal data transfers.

4.1.2 The Cloud Act in the United States

The Cloud Act extends its jurisdiction beyond borders by using US multinational corporations as a leverage point. It addresses the legislative gaps in the Stored Communications Act regarding the unclear

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

jurisdiction over accessing data stored in other countries by multinational companies. The Cloud Act consists of two main aspects: first, it grants the US government the authority to access data stored by US companies overseas, and second, it allows "qualifying foreign governments" meeting certain conditions to request access to data under the control of US companies. The Cloud Act not only establishes lawful extraterritorial legislative jurisdiction for the US government but also unilaterally defines lawful extraterritorial enforcement jurisdiction for the US government.[9] However, establishing lawful extraterritorial enforcement jurisdiction requires compliance with the personhood principle of international conventions and specific powers granted by international treaties, as well as the valid consent of foreign governments.[10] It is evident that the Cloud Act's enactment is a unilateral US legislation that fails to meet the requirements for establishing lawful extraterritorial enforcement jurisdiction. The extraterritorial enforcement based on the Cloud Act severely undermines other countries' data sovereignty. With a significant number of multinational companies headquartered in the US and conducting global operations, the Cloud Act grants the US government the legal power to extend its jurisdiction beyond its borders through multinational companies. This enables the US government to collect global data and enforce its own data management model, thereby diminishing other countries' data jurisdiction.[11]

Unlike the GDPR, which advocates globalization, the Cloud Act's introduction accelerates the pace of data localization legislation in various countries. While the Cloud Act allows for mutual data access between other countries and the US, the conditions and procedures for data access differ between the two sides. The difficulty for other countries to access data from the US is significantly higher than the US accessing data from other countries. Directly accessing data stored within another country's borders not only violates that country's data sovereignty but also poses significant threats to national security and other major issues. The Cloud Act, unilaterally enacted by the US, provides legal justification for such actions without specific powers granted by international treaties and the valid consent of foreign governments. This is clearly illegitimate. To counter the extensive extraterritorial jurisdiction of the US, countries have hastened the process of data localization, enacting laws to block extraterritorial jurisdiction and insisting on storing important data within their own borders. This is done to defend their data sovereignty, with the protection of national security being the most crucial aspect. Currently, the EU, Australia, Germany, Russia, and China have established data localization legislation or policies, while countries such as Brazil, India, and Malaysia acknowledge and implement data localization laws.[12]

4.2 Soft Law Codification: APEC's Cross-Border Privacy Framework and CBPR

In today's world, the trend of deglobalization makes it difficult for hard law to reach consensus among nations. Instead, the growth in the number of soft laws over the past decades has been proportional to the increase in specific thematic demands. Soft law has gradually become a trend of the times, and the codification of soft law has entered the public eye. [9] Among them, a typical example is the Asia-Pacific Economic Cooperation (APEC) Privacy Framework issued by the Asia-Pacific Economic Cooperation in 2004 and the Cross-Border Privacy Rules (CBPR) established in 2012 based on the Privacy Framework. These laws set the minimum level of data protection in the Asia-Pacific region, stipulate nine principles for the protection of personal information, and encourage APEC members to develop domestic data protection laws based on their own circumstances. However, due to the significant differences in development levels among APEC members and the non-binding nature of the Privacy Framework, there is a large disparity in the level of personal data protection laws enacted by member countries, which hinders the cross-border transfer of personal data. In order to effectively implement personal data protection rules, APEC subsequently introduced the CBPR to codify soft law into hard law.

The CBPR system is a voluntary certification and regulatory system for enterprises to protect data. CBPR is the core rule of the CBPR system, which sets unified data protection standards based on the Privacy Framework. It elaborates the nine principles into 50 specific requirements for enterprises, specifies the application process for joining the system, and provides remedial measures when enterprises violate the CBPR. [10] CBPR is not a regional law but more like a contract reached between enterprises and APEC. It only certifies and regulates enterprises that voluntarily join the system. Enterprises that are certified under the CBPR system are allowed to freely collect, process, transfer, and use data in the Asia-Pacific region. However, for an enterprise to join the CBPR system, it needs to meet three conditions: first, the economy in which the enterprise is located has joined the CBPR system and has committed to following the requirements of the CBPR and assisting in the regulation and sanctioning of enterprises; second, at least one accountability agent in the economy where the enterprise is located has joined the CBPR system and has the capacity to assist the CBPR in certifying and regulating enterprises based on the nine principles and 50 specific requirements, including the enterprise's internal privacy policies, etc.;

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

third, the enterprise has made self-adjustments to meet the 50 specific requirements specified by the CBPR. Once an enterprise meets the standards, the accountability agent grants it the CBPR-recognized Privacy Trustmark and regulates its activities. If an enterprise that has voluntarily joined the CBPR violates its provisions, the accountability agent has the right to impose punishments such as notification, criticism, or revocation of certification. If the enterprise fails to rectify after being punished by the accountability agent, the privacy enforcement authority in the economy where the enterprise is located should assist the accountability agent in imposing more severe sanctions on the enterprise to compel rectification. The "dual-track" management mechanism of self-assessment and adjustment by enterprises and regulatory supervision by accountability agents can effectively ensure the implementation of the CBPR and enhance international trust in the CBPR system.

The purpose of the CBPR system is to facilitate the cross-border transfer of personal data to the greatest extent possible, introducing industry self-discipline norms, and accountability agents that provide certification are highly professional, increasing the likelihood that the system will operate as intended. However, the CBPR stipulates that participating countries cannot require data recipients to provide protection levels higher than the minimum level specified by the CBPR when controlling the export of personal information. [11] This to some extent undermines the regulatory standard autonomy of countries. Moreover, both countries, enterprises, and accountability agents need to apply for certification, which adds complexity and increases the transmission costs for enterprises.

4.3 Flexibility and Autonomous Choice: Free Trade Agreements

In recent years, frequent frictions between countries have made it difficult to reach multilateral agreements. Therefore, flexible and convenient bilateral free trade agreements have gradually become the primary choice for resolving conflicts in the governance of personal data between countries. Countries can autonomously determine the content of the provisions based on their own development status, negotiate, and sign agreements to ensure effective implementation.

4.3.1 Types of Free Trade Agreements

Based on the number of contracting parties and their geographical regions, free trade agreements can be divided into three types: large-scale free trade agreements, regional free trade agreements, and bilateral free trade agreements. Large-scale free trade agreements are typical multilateral agreements that are usually based on the principles of universality and non-discrimination, aiming to coordinate the relationships between contracting parties as widely as possible and achieve harmonious development of free trade. Currently, the three major free trade zones in the world are the European Union (EU), the Association of Southeast Asian Nations (ASEAN), and North America, all of which have obvious regional characteristics. The EU is a free trade area under a political and economic monetary union, while ASEAN and North America are established through large-scale regional free trade agreements. Among them, the largest free trade agreement is the Regional Comprehensive Economic Partnership (RCEP), which was jointly signed by ASEAN member countries and countries such as Australia, China, Japan, South Korea, and New Zealand. The e-commerce chapter of the RCEP sets specific provisions for cross-border transfer of personal data. Data shows that the RCEP accounts for approximately 30% of the global population, GDP, and merchandise trade. The agreement entered into full implementation on June 2, 2023, marking a new stage of comprehensive implementation for the world's most populous, largest-scale, and most development-potential free trade area. The leaders of the United States, Mexico, and Canada re-signed the North American Free Trade Agreement (NAFTA) on November 30, 2018, in Argentina, and renamed it the United States-Mexico-Canada Agreement (USMCA). Although the USMCA retains the basic framework of NAFTA, it sets strict restrictions in the field of cross-border transfer of personal data and serves as a model for subsequent bilateral free trade agreements signed by the United States with other countries.

Based on frequent trade exchanges, countries have also signed many small-scale regional free trade agreements. Regional free trade agreements are usually based on regional and exclusive principles, aiming to coordinate relationships between contracting countries, promote regional economic development, and safeguard overall regional interests. Compared to large-scale free trade agreements, regional free trade agreements involve fewer contracting countries and have a smaller regional scope, resulting in relatively weaker influence. At the same time, the contracting countries have greater autonomy and can actively participate in the formulation of the content of the free trade agreement to better safeguard their own trade interests. Examples include the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) signed by 11 countries including Japan, Canada, Australia, Chile, New Zealand, Singapore, Brunei, Malaysia, Vietnam, Mexico, and Peru, based on

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

considerations of digital trade. Another example is the Digital Economy Partnership Agreement (DEPA) signed online by Singapore, Chile, and New Zealand. Both agreements are representative regional free trade agreements that advocate the free flow of personal data across borders.

Bilateral free trade agreements are agreements signed by two related stakeholders based on principles of self-interest and flexibility to determine the rights and obligations of both parties. Due to different national conditions and levels of development, there are often significant differences between FTAs signed through free negotiations between countries, which better cater to the personalized needs of each country's economic development. Countries that have stable trade exchanges with each other generally sign bilateral free trade agreements, leading to a large number of bilateral free trade agreements between countries and gradually forming a global network of bilateral free trade agreements. For example, the United States has signed FTAs with 12 countries, including Australia, Bahrain, and Oman. The European Union, as a regional political organization, has signed FTAs with 10 countries, including South Korea and South Africa. China has signed FTAs with 8 countries, including Peru and Costa Rica.

4.3.2 Governance of Personal Data in Free Trade Agreements

With increasing global concern over personal data protection, the latest free trade agreements have included specific provisions regarding this issue. In comparison to its predecessor NAFTA, the US-Mexico-Canada Agreement (USMCA) introduced a chapter on digital trade, which includes specialized clauses regulating the protection of personal information and the cross-border transfer of data through electronic means. Similarly, the Regional Comprehensive Economic Partnership (RCEP) and the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) established e-commerce chapters, and the Digital Economy Partnership Agreement (DEPA) all provide specific provisions for the protection of personal data.

(1) Provisions for the Protection of Personal Information

Based on a comparative study of the above-mentioned free trade agreements, it is found that provisions for the protection of personal information share at least four common aspects. First, the contracting parties are required to establish effective legal frameworks for personal data protection, taking into account relevant international treaty guidelines and principles. Second, the contracting parties should adopt non-discriminatory practices to protect personal information from infringements within their jurisdictions. Third, the contracting parties should disclose the personal information protection measures they provide. Fourth, the contracting parties should establish cooperative mechanisms for personal data protection. However, each free trade agreement's provisions on personal information protection differ slightly based on their respective backgrounds. The rules in RCEP mostly use the term "encourage," which implies suggestions for the contracting parties on how to act, rather than requirements. In contrast, USMCA, CPTPP, and DEPA use the term "shall," which imposes obligations on the contracting parties, indicating that, in general, the parties must comply without special circumstances. USMCA and DEPA provide specific provisions on the legal framework and principles of personal data protection, with their key principles being almost identical. DEPA also further suggests encouraging companies to adopt data protection trustmarks and promoting communication between the contracting parties on the use of data protection trustmarks.

(2) Cross-Border Transfer of Data through Electronic Means

By comparing the specialized provisions on the cross-border transfer of data through electronic means in the aforementioned free trade agreements, it is found that, similar to the provisions for personal data protection, these provisions share common content. First, the contracting parties need to recognize that different regulatory requirements exist regarding the cross-border transfer of data through electronic means. Second, the contracting parties shall not impede the conduct of cross-border data transfers through electronic means by individuals or legal entities within their jurisdictions engaged in business activities. Third, without constituting arbitrary or unjustifiable discrimination or disguised trade restrictions, a contracting party may adopt measures to restrict the transfer of personal data based on the protection of its legitimate public policy objectives and basic security interests. Additionally, RCEP specifies that other contracting parties shall not raise objections to such measures. This provision grants the contracting parties the autonomy to determine the scope of legitimate public policy objectives and basic security interests, resulting in flexible standards among the contracting parties. USMCA, CPTPP, and DEPA do not have this provision. Furthermore, USMCA and DEPA stipulate that measures taken by contracting parties to protect their legitimate public policy objectives and basic security interests shall not exceed what is necessary, which significantly limits the authority of the contracting parties to use such measures. The WTO Appellate Body's ruling in the "EC-Asbestos Case" indicates that the standards underlying measures taken to protect legitimate public policy objectives and basic security interests should be

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

determined by the contracting parties themselves, provided that these standards are based on the principle of good faith and are subject to objective review by expert panels.[12] RCEP restricts the right of other contracting parties to raise objections to such measures, which undoubtedly poses risks of abuse for the contracting parties.

(3) Exception Clauses

In addition to specialized provisions for the protection of personal data, the general exceptions and security exceptions clauses in FTAs also affect the cross-border transfer of personal data. FTAs are agreements established within the framework of the WTO, and they generally make direct reference to the general exceptions and security exceptions of WTO agreements or further specify them. WTO case rulings also provide guidance for the practical application of FTAs. "The multilateral path is not only a matter of international law and good governance, but also an objective requirement of data without geographical boundaries." [13] [CPTPP and USMCA stipulate the application of the general exceptions clause under the General Agreement on Trade in Services (GATS), and in the footnotes, it is clarified that this clause does not affect the classification of electronic products as goods or services. On the other hand, RCEP and DEPA stipulate the simultaneous application of the general exceptions of both the General Agreement on Tariffs and Trade (GATT) (1994) and GATS, but with necessary modifications.

5. The improvement path for Cross-Border Governance Rules on Personal Data in China

Various countries, driven by considerations such as the development of the data industry, traditions of privacy protection, national stances, and perspectives on national security, have successively enacted restrictive regulations on cross-border transmission of personal data, raising the threshold for such transfers. However, the challenge faced by China is to find a balance between development, security, national stances, and traditions, considering the multifaceted impact of cross-border data transmission on economic, social, and technological progress stemming from the benefits of free trade.

5.1 Actively participating in major free trade agreements

As the era driven by data development continues to advance, the scope of cross-border personal data is expected to broaden. China, having started relatively late in governing cross-border personal data, needs not only to refine its domestic legal system but also actively engage in the formulation of major free trade agreements to promote the “Chinese approach” globally. This approach facilitates friendly exchanges between China and the international community based on experiences in cross-border personal data governance, ensuring better alignment with relevant international legislative frameworks and avoiding conflicts and inconsistencies. Currently, there is no unified international regulation governing cross-border personal data governance worldwide, creating a diverse landscape and an opportunity for agile advancements. China is actively seeking to join major free trade agreements, such as officially applying to join the CPTPP in September 2021 and actively progressing through the accession process. Since proposing to join the CPTPP, debates have arisen regarding China’s intentions, its ability to adhere to the high-standard data rules, and the benefits of its accession. Responding to these concerns, Ambassador Wang Xiaolong stated that joining the CPTPP is a serious decision made for China’s development strategy, asserting China’s capability to join. To prepare for accession, China established an expert group to study and evaluate over 2,300 rules of the CPTPP, aligning its legal and policy framework. In June 2023, China introduced 33 pilot measures, conducting stress tests in select free trade zones and the Hainan Free Trade Port in preparation for widespread implementation. Additionally, a report from the Peterson Institute for International Economics predicts that China’s accession to the CPTPP could double the annual benefits it brings to the global economy [14].

Furthermore, China should seize the opportunity presented by the “Belt and Road” initiative to establish a China-led “circle of friends” for cross-border governance of personal data. Over the past decade, the “Belt and Road” initiative has evolved into a widely embraced international public product and cooperation platform. Amid the impact of the COVID-19 pandemic, the rapid development of the digital economy has positioned China at the center of establishing the “Digital Silk Road,” aiding countries along the “Belt and Road” in digital policy alignment, technological innovation, and application. By July 2022, China had established “Digital Silk Road” cooperation mechanisms with 16 countries and bilateral cooperation mechanisms with 23 countries for “Silk Road e-commerce,” while constructing 34 cross-border land cables and multiple international sea cables. However, due to disparities in data capabilities among nations and concerns related to privacy protection, national security, and industrial development, strategic risks in the form of a game are increasingly prominent under “Belt and Road”

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

cooperation, posing significant challenges to cross-border data flow. In response, China should actively engage with countries along the "Belt and Road," reaching bilateral or multilateral agreements on cross-border data circulation. Efforts should be made to eliminate digital barriers, establish an international cooperation organization conducive to the development of cross-border regulations for personal data under the "Belt and Road," and formulate universally applicable rules and regulatory frameworks for personal data governance across the countries involved. On July 16, 2023, the United Kingdom formally announced its accession to the CPTPP, completing a process that took 2 years and 5 months from its application on February 1, 2021. In comparison, China's application has been pending for 2 years and 4 months without new negotiations or significant progress in the accession process with the CPTPP.

5.2 Establishing a network of bilateral free trade agreements

As international governance rules for cross-border personal data transmission are still evolving, countries are increasingly turning to free trade agreements as a solution to address conflicts in this realm. Among these, bilateral free trade agreements, with their self-serving and flexible characteristics, have become the preferred choice for many nations. Bilateral free trade agreements not only meet the diverse needs of countries by tailoring rules based on specific circumstances but also enable the signing parties to determine their respective interests through free negotiation, fostering a mutually beneficial cooperation. While reducing the barriers to cross-border personal data for the signing parties, bilateral trade agreements, relatively speaking, indirectly raise the threshold for other countries or regions outside the agreement. In an effort to mitigate this relative high threshold, other countries or regions may actively engage in separate negotiations to sign bilateral free trade agreements with the original parties. The increasing prevalence of bilateral free trade agreements gradually forms a chain reaction, creating a network of intersecting Free Trade Agreements (FTA) [15]. To avoid being indirectly excluded from this FTA network, China should proactively engage with other countries and regions to establish bilateral free trade agreements, creating a network centered around China. This network aims to promote cross-border transmission of personal data.

Currently, China has signed Free Trade Agreements (FTA) with only eight countries, including Peru, Costa Rica, Chile, Singapore, Pakistan, Australia, Georgia, and New Zealand, and these countries are geographically dispersed. Over the past decade, the "Belt and Road" initiative has faced repeated challenges and obstacles due to criticism of traditional geopolitical Cold War thinking, as well as conflicts such as the Russia-Ukraine war and the Israel-Palestine conflict, posing significant hindrances to the westward expansion of the "Belt and Road" construction. Globalization represents the interdependence among nations, and forming an FTA network through free trade agreements with countries along the "Belt and Road" is crucial to open up trade routes and alleviate the impact of geopolitical conflicts. Under the influence of the Russia-Ukraine war, the northern route of the "Belt and Road" Eurasian corridor is severely obstructed, while obstacles persist in connecting the central and southern routes, making it challenging for the three main routes to be fully operational in the short term. Given the difficulty of resolving the Russia-Ukraine conflict in the near future, China should prepare for the long-term disruption of the northern route. In response, China should accelerate the construction of transportation infrastructure along the central and southern routes, actively sign free trade agreements with countries along these routes, and provide policy support for smooth trade, thus alleviating the trade pressure caused by the obstruction of the northern route. Signing a free trade agreement with Russia is a top priority, considering Russia's economic shift towards the east and its emphasis on the development of the Far East region. The cooperation between China and Russia in the energy sector has deepened over the years, with milestones such as the opening of the China-Russia crude oil pipeline in 2011, the launch of the China-Russia Eastern Gas Pipeline in 2019, and the smooth customs clearance of the first batch of equipment for the Xudabao nuclear power plant in 2021. During the summit on February 4, 2022, customs authorities of both countries signed an arrangement on mutual recognition of Authorized Economic Operators (AEO), providing convenient customs conditions for enterprises recognized by both countries, promoting the expansion of trade openness between the two nations.

5.3 Clarifying the data classification and grading protection system

China's governance of cross-border personal data transmission primarily stems from a holistic national security perspective, favoring the establishment of static rules and advocating for localized data storage [16]. The data classification and grading protection system established in the "Data Security Law" aims to facilitate data flow while ensuring data security. It assigns different protection levels and methods to various types and levels of data, preventing unreasonable data leaks and overly strict restrictions on

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

data movement. The “Data Security Law” provides only a vague definition for the concept of important data. In practice, the country encourages various industries to determine classifications based on the actual use of data, allowing for different levels of protection. This is a “bottom-up” approach to data classification and grading. While this approach is highly practical and has led to the rapid adoption of industry-specific data classification standards, it can create challenges in aligning protection systems for cross-border data flow due to the multitude and complexity of standards. For domestic data classification and grading protection, the “bottom-up” approach is effective, but for cross-border data, there is a need for a nationally unified and clear data classification and grading protection framework “top-down” to seamlessly integrate with international data protection rules and ease the pressure of cross-border data security reviews.

Given China’s current status in personal data governance, the country can draw insights from the GDPR’s approach to classifying and protecting personal data. Establishing a system where different categories and levels of data are transmitted through specific cross-border channels can facilitate alignment with international personal data protection systems and enable efficient cross-border data transmission. Simultaneously, China should further clarify classification standards to prevent mismatches between cross-border data types and corresponding protective measures, such as identifiable criteria for personal data and application standards for security review systems. Additionally, China can learn from the experiences of the EU and APEC by establishing an independent and specialized institution for cross-border personal data protection. This institution could focus on regulatory oversight of cross-border personal data governance, enhancing regulatory efficiency and quality. Furthermore, China’s cross-border personal data protection institution can seek collaboration with similar institutions in other countries, creating a seamlessly connected regulatory system from China to other nations. This collaboration aims to lower the threshold for the free cross-border transmission of personal data while ensuring data security.

6. Conclusion

Driven by both epidemics and technology, countries around the world are accelerating their digital transformation, with frequent cross-border personal data transmission activities. The abuse of cross-border transmission of personal data is a recurring problem, and national governance actions are imminent, but how to find a balance between development and security is a huge challenge China is currently facing. In the field of cross-border governance of personal data, China's relevant legislation started late and only basic legal rules have been established. China's personal data cross-border governance rules are mainly encapsulated in the personal data governance system, which is small and scattered, and some legal provisions are vague. Looking at the historical evolution of international personal data cross-border governance rules, reviewing the three more common legislative models of domestic law, regional law and free trade agreements, and taking a look at the typical relevant legislative examples of countries or regions, we will make a comparative analysis of the three types of legislative examples with the same characteristics, namely, the extraterritorial extension of the scope of application, the hardening of soft law, and the flexibility of autonomous choice. Starting from the legislative source, it puts forward suggestions for improving China's cross-border personal data governance system, so as to lay a solid legal foundation for cross-border personal data governance and help China's international development.

Acknowledgements

To complete the thesis, I got much help from my professors. My deepest gratitude goes first and foremost to my supervisor Dr. Yu, who gave me the golden opportunity to do this wonderful on the topic. Then I would like to express my sincere gratitude to Dr. Du and 2023 Beijing Technology and Business University Postgraduate Subject Competition Project (Project No.: 19008023027). My professors are always patient and show continued support to me. Finally, I am grateful to my parents for their love, caring and sacrifices for educating and support me.

References

[1] Ma, Q., & Li, X. (2021). Constructing Regulatory Rules for Cross-Border Data Flow in China. Rule of Law Studies, 1, 91–101.
[2] Gao, F., & Wang, Y. (2019). On the Origin of Personal Data Protection System: Historical Analysis

ISSN 2706-6827 Vol. 6, Issue 1: 85-96, DOI: 10.25236/IJFS.2024.060116

and Enlightenment from Offshore Legislation. Henan Social Sciences, 27(11), 38–49.
[3] Hert, P. D., & Gutwirth, S. (2009). Data Protection in the Case Law of Strasbourg and Luxemburg: Constitutionalisation in Action. Springer, 3.
[4] Yang, G. (2021). On the Relationship between RCEP and WTO Rules. International Business Research, 42(5), 3–10.
[5] Greenleaf, G. (2014). Sheherezade and the 101 data privacy laws: Origins, significance and global trajectories. JL Inf. & Sci., 23, 4.
[6] Greenleaf, G. (2017). Global data privacy laws 2017: 120 national data privacy laws, including Indonesia and Turkey. Including Indonesia and Turkey, 145, 10-13
[7] Gao, F. (2022). The Institutional Defects of GDPR and Its Warning to the Implementation of China's Personal Information Protection Law. Rule of Law Studies, 3.
[8] Wang, X., & Shi, W. (2022). Globalization of Data Legislation Jurisdiction and China's Response. Intellectual Property Rights, 4, 54–75.
[9] Xie, Z. (2020). Data Privacy Protection in the Data-Driven Era: From Individual Control to Data Controller's Fiduciary Obligations. Legal and Business Research, 2, 54–75.
[10] Feng, Y., & Wei, H. (2020). The Theory and Critique of the "Brussels Effect" of GDPR: An Analysis of Its Extraterritorial Legislative Influence. Journal of Yantai University (Philosophy and Social Science Edition), 2, 1–11.
[11] Chander, A., & Le, U. P. (2014). Breaking the web: data localization vs. the global internet. Emory Law Journal, Forthcoming, UC Davis Legal Studies Research Paper, 378.
[12] Ferris, E., & Bergmann, J. (2017). Soft law, migration and climate change governance. Journal of Human Rights and the Environment, 8(1), 6-29.
[13] Shi, J. (2020). Latest Progress and Prospects of APEC Digital Economic Cooperation. International Economic Cooperation, 1, 37–44.
[14] Liu, H., & Cheng, H. (2020). Global Governance of Cross-Border Data Flows: Progress, Trends, and China's Path. International Outlook, 6, 65–88.
[15] Boklan, D., & Bahri, A. (2020). The first WTO's ruling on national security exception: balancing interests or opening Pandora's box? World Trade Review, 19(1), 123-136.
[16] Lin, F., & Du, Y. (2020). Development and Transformation: Reflection on the Construction Path of Digital Trade Rules from a Multilateral Perspective. Journal of Jianghai, 5, 161–162.