American Journal of Applied Scientific Research
2020; 6(2): 30-38
http://www.sciencepublishinggroup.com/j/ajasr
doi: 10.11648/j.ajasr.20200602.11
ISSN: 2471-9722 (Print); ISSN: 2471-9730 (Online)

Research on EU Legal Regulation of Cross Border Flows of Personal Data and Its Enlightenment to China

Dong Jingbo*, Xiao Fei

Faculty of International Law, China University of Political Science and Law, Beijing, China

Email address:
jingbod@cupl.edu.cn (Dong Jingbo), cuplelaine@163.com (Xiao Fei)

*Corresponding author

To cite this article:
Dong Jingbo, Xiao Fei. Research on EU Legal Regulation of Cross Border Flows of Personal Data and Its Enlightenment to China. *American Journal of Applied Scientific Research*. Special Issue: *Science and Law (Review of Several Issues of Contemporary Science and Technology Law)*. Vol. 6, No. 2, 2020, pp. 30-38. doi: 10.11648/j.ajasr.20200602.11

Received: February 20, 2020; **Accepted**: March 9, 2020; **Published**: April 23, 2020

Abstract: With the development of economic globalization and information globalization, the cross border flow of personal data has brought some challenges to national security and the privacy of data subjects, so it is necessary to regulate it. This paper mainly studies the legal system of regulating the cross border flow of personal data in the European Union. The rules for cross border transmission of data in GDRP provide for the specific circumstances in which personal data are transmitted to third countries or international organizations within its territory, limiting, to a certain extent, the cross border flow of personal data while protecting personal data. It has a far-reaching influence on the construction of the relevant legal system in many countries and regions. In addition, the EU-U.S Privacy Shield Framework also provides a new way to regulate the cross border flow of personal data. Through the analysis of EU's legal rules on cross border flow of personal data, some suggestions are put forward for China to regulate in this field: firstly, the legislation on cross border flow of personal data should be perfected to enhance the operability of the law; Secondly, we can strengthen international cooperation and actively participate in the formulation of international rules for cross border flow of personal data.

Keywords: Regulating Cross-Border Data Flows, GDPR, EU-U.S Privacy Shield Framework

1. Introduction

In 1980, the Organization for Economic Cooperation and Development issued "the Guidelines on the Protection of Privacy and Cross border Flows of Personal Data". The concept of the "cross-border data flow" was first put forward and the guiding framework for cross-border data flow was established. In recent years, the world enters a "Data-driven" era, the flow of data has created great business value and economic benefits, so many countries want to promote cross-border flow of personal data, reduce unreasonable restrictions on international trade rising from data protection. However, the disorder of cross-border data flow and the uneven level of data protection among countries pose certain risks to personal data security and national security, and some countries impose different degrees of legal restrictions on the cross-border flow of personal data, and if the restrictions are too strict, they will lead to the localization of data and result in trade barriers. So how to construct a regulation to find a balance between the cross-border free flow of personal data and the protection of personal data rights is of great significance. Since the European Union started earlier in the regulation of cross-border personal data flow and has a relatively complete system, and the latest General Data Protection Regulation has also further developed it, the author takes the legal rules of the cross-border flow of personal data as the research object. Through in-depth analysis of the EU's legal system for the cross-border flow of personal data, it will provide an experience for the establishment and improvement of the legal system for the cross-border flow of personal data in China.

2. The Reason of the Legal Regulation of Cross-Border Flow of Personal Data

With the economic globalization and further development of information technology, the Internet, cloud computing, block chain, Internet of Things and artificial intelligence have

penetrated into all aspects of social life and economic life, and the world has entered the "digital economy era." The digital economy is increasingly dependent on cross-border data flows, which have driven the digital economy and created new sources of employment, innovation and economic growth.[1] Some consulting firms estimate that cross-border data flows have increased global GDP by about 10.1 per cent over the past decade.[2] But there is no doubt that while the cross-border data flow creates large value, it also brings more risks.

First, the cross-border flow of personal data poses a great challenge to the rights of the data subject, and if there occurs actions violating the legitimate rights and interests of data subjects such as excessive collection of the data, improper use and data leakage, data subjects often faces difficulties in obtaining evidence and high cost of rights protection. It will also be difficult to relieve and implement. Therefore, compared with the domestic personal information protection system, the cross-border flow of personal data requires the international-compatible national data protection system to safeguard the legitimate rights and interests of the data subject. Second, cross-border flow of personal data is also closely linked to national security and public safety. As cross-border data flows penetrate financial, industrial, transportation, medical and many other fields, data-entry countries can process and analyze the data flowing into their own countries through emerging technologies to judge the consumption habits of residents in the data-exporting countries, the financial development trends of the exporting countries, the economic development dynamics and so on. Therefore, in view of the possible infringement of personal data rights caused by personal cross-border data flow, the potential threat to national security, public interest and the development of domestic information industry, it is legitimate and necessary to take into account the factors such as personal data security protection, national security protection and law enforcement facilities, and prohibit or restrict the transmission of personal data to other countries to a certain extent by means of legislation and so on. [3]

Nowadays, more and more countries have taken into account or have taken measures to provide more restrictions on cross-border data flow for purposes of national security, protection of personal data. Some countries require that the cross-border data flows need to correspond to their equivalent information protection conditions. For example, in terms of information transfer in India, information controllers can only transfer personal sensitive data or information to third parties if the third-party information users have adopted the same information protection measures as information controllers. Under the telecommunications industry regulations, the consumer bills and user information must not be transferred or accessed across borders. Russia requires that the personal data of Russian citizens, which are transmitted via the Internet, can only be stored in Russia Ross domestic servers, and Japan's 2015 amendment to the "Personal Information Protection Law" also strictly stipulates the conditions for providing information to third parties abroad. However, if the data localization requirements are too strict, there will be localized trade barriers, which will cause important obstacles to the process of global trade liberalization. Thus it can be seen that it is of great significance to coordinate the cross-border flow of personal data with the protection of personal data rights, and to design a regulatory system that can not only promote the free flow of personal data across borders, but also ensure the effective protection of personal data during the flow.

3. Rules on the Cross-Border Flow of Personal Data in the "General Data Protection Regulation"

3.1. Legislative Practice Before the Promulgation of the "General Data Protection Regulation"

The European Union has the tradition of respecting the individual's data rights, and has long-term commitment to personal data protection. The research on the cross-border flow of personal data has started earlier and provides a lot of creative institutional designs to the world to promote cross-border free flow of personal data on the premise of adequate protection of personal data rights. As early as 1981, the "European Treaty Series-No. 108. Convention For the Protection of Individuals with Regard to Automatic Processing of Personal Data"(hereinafter referred to as "108 Convention"), adopted by the Council of Europe, regulates the cross-border data flow, but the 108 Convention only deals with the flow of data between European member states. It stipulates a general principle that member states must not restrict the cross-border flow of data in a way that prohibits or specifically authorizes it in the purpose of protecting personal data. It can be seen that, as the first European regional legal document concerning the cross-border flow of personal data, the 108 Convention attempts to overcome the obstacles of cross-border data flow through legislation and promote the cross-border sharing of personal data among member states. By the end of 1989, the 108 Convention had been ratified by only seven member states of the European Community, and member states that had ratified it had not established supporting domestic implementation regulations.

In view of the fact that after the signing of the Convention, good expected results have not been achieved, and cross-border data flows face threats such as unauthorized collection, access, use, disclosure and tampering, the regulation of cross-border personal data flows in the EU has become increasingly strict.[4] On 24 October 1995, The European Parliament and the Council adopted the Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data. For cross-border flows of personal data within EU members, the Directive 95/46/EC requires Member States to develop their respective national data protection systems and prohibit restrictions on the free flow of personal data between member states. For the transmission of personal data to third countries, there are three legal methods of data transfer: First,

the destination country ensures an adequate level of protection which was recognized by EU under Article 25, paragraph 1, of the Directive 95/46/EC. [5] Second, the data flow falls within the derogations listed in Article 26, paragraph 1. [6] Third, the measures referred to in Article 26, paragraph 2, provide adequate safeguards. Article 26 provides the legal basis for standard contractual clauses and binding corporate rules. To sum up, Article 25, paragraph 1 is the principle of the cross-border flow of personal information in the EU. Once the adequate level of protection of a third country is achieved, personal data can be transferred to this country. Article 26 is the exception to Article 25, including statutory exceptions and adequate safeguards. The reason for statutory exceptions is that there exist individual rights that take precedence over personal data. In order to protect these interests, a statutory exception has been created to break through the provisions of Article 25. Adequate safeguards are used to promote and meet the cross-border flow of EU personal data when the overall level of personal data protection in a third country is far from the requirements of the EU's adequate protection level. Combined with practice, adequate safeguards include standard contractual clauses, binding corporate rules and so on.

In the twenty years since the implementation of Directive 95/46/EC, information technology has developed rapidly. Big data, cloud computing, and smart terminals have impacted the protection of personal data. In order to respond to the development of emerging technologies and establish a unified EU data market to strengthen personal data protection and promote cross-border free flow of data, the European Parliament and the European Council passed the General Data Protection Regulation (GDPR) on April 4, 2016, and it was formally applies to all EU member states on May 25, 2018, replacing the Directive 95/46/EC. GDPR is based on Directive 95/46/EC, which retains the basic framework and most of the content of it.[7] The regulation of cross-border flow of personal data has been greatly optimized, and more legal data flow methods are further defined.

3.2. Provisions of GDPR on the Cross-Border Flow of Personal Data

3.2.1. Transmission of Data on the Basis of an Adequacy Decision

Article 45 of GDPR provides that a transfer of personal data to a third party or an international organization may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of protection. Such a transfer shall not require any specific authorization. [8] The provisions of this article continue the "adequate protection" in Directive 95/46/EC, but GDPR enumerates the identification factors of adequate protection in detail and adds the object types of adequate protection.

According to Article 46 of GDPR [9], the European Commission should consider the following three factors when evaluating the adequacy of protection: first, whether the legal system related to data protection in third countries is complete; and second, whether there are effective independent supervisory authorities in the third country; the third is whether third countries have made international commitments related to personal data and undertake relevant obligations. At the same time, GDPR has also expanded the scope of the object of adequacy decision. In addition to assessing the country, the European Commission can also evaluate and judge the level of protection in a specific region of the country, in the field of industry and in international organizations, in order to further evaluate the level of protection of a specific region of the country, the industry area and the level of protection of international organizations, expanding the areas covered by adequacy decision.[10] At present, with the exception of EU member States, only 11 countries or territories are included in the "white list" that allows cross-border transmission of data, namely, Andorra, Argentina, Canada, Faroe Islands, Guernsey, Israel, Isle of Man, Jersey, New Zealand, Switzerland and Uruguay. Thus it can be seen that the method of listing "white list" through adequacy decision lacks broad applicability, and other system designs are needed to achieve the purpose of promoting the cross-border flow of personal data.

3.2.2. Transmission of Data Subject to Appropriate Safeguards

Compared with Directive 95/46/EC, GDPR defines more legal methods of cross-border flow of data for companies to choose from. Article 46 provides that when the third countries or international organizations do not have adequacy decision and there are no legally binding and enforceable legal documents between public authorities, personal data may be transmitted to third countries or international organizations if the data controller or processor provides appropriate safeguards. According to Article 46, these appropriate protection safeguards include: (a) binding corporate rules; (b) using the standard data protection clause; (c) appropriate safeguards in accordance with the approved code of conduct and commitments made by data controllers or processors; (d) appropriate safeguards provided in accordance with the approved certification mechanism and commitments made by data controllers or processors.

The Binding Corporate Rules (BCR), is a mechanism introduced by the Article 29 Committee after the issuance of Directive 95/46/EC. GDPR specifies it in detail in Article 47 and formally defines it as a statutory and effective cross-border data flow mechanism. BCR is made for international enterprises to carry out cross-border transmission of personal data, and the ultimate goal is to ensure that enterprises can guarantee the security of personal data according to certain protection standards when exporting and importing personal data.[11] If an enterprise group can comply with a complete set of data protection policies approved by the competent regulatory authority, the group can be regarded as a "safe harbor" as a whole, and personal data can flow freely across the border within the group. According to Article 47 of GDPR, it places extremely high requirements for binding corporate rules. Enterprise groups must ensure the security of personal data be fully guaranteed at every time,

every branch, data transmission, storage and processing. Otherwise they will face the legal risk of prosecution or complaint in the EU at any time.[12] With regard to the enforcement and supervision of binding corporate rules, GDPR uses its data protection officer system to monitor compliance with corporate guidelines: data protection officer or the relevant person-in-charge shall report to the regulatory body of the Member States on the implementation of the binding corporate rules, the circumstances of the changes and the possible negative impact of third States on the effective implementation of the rules.

With regard to the standard data protection clause, the European Commission approved the "controller to controller" standard contractual clause, the "controller to processor" standard contractual clause, the alternative standard contractual clause, the three standard contractual clause are still valid. On this basis, GDPR has added that the member's data protection agency can designate other standard contractual clause approved by the European Commission, providing businesses with more choices of contractual clause.

3.2.3. Derogations for Specific Situations

Article 49 of GDPR provides for derogations for specific situations. It is a statutory exception in the absence of "adequacy decisions" and "appropriate safeguards." As long as these statutory special circumstances are met, cross-border transfer of data to third States or international organizations may be made.[13] In addition to the seven exceptions provided for in the article, GDPR also provides for a save clause that seeks to exhaust the "necessary" cross-border transmission of data in all commercial flows and international exchanges, as reflected in its efforts to facilitate cross-border transmission of data. However, the provision contains many uncertain statements in the process of expression, such as "convincing legitimate interests". There is a great deal of uncertainty because the conditions are difficult to quantify. [14] Moreover, in order to protect the rights of data subjects, the EU has attached restrictions on the application of these save clauses without conflict with the data subjects. In particular, the article reflects the EU's efforts to strike a balance between strengthening the protection of personal data rights and promoting the cross-border flow of data, but this wobbling institutional design between the two may make the article virtually inoperable and extremely prone to legal risks.

3.3. Conditions for the Cross-Border Flow of Personal Data in GDPR

The above provisions of GDPR provide the legal basis for the cross-border transfer of personal data, but this kind of condition setting is hierarchical, and the next level condition is applied only when the conditions at the upper level are not met. First, if a third country or other organization obtains an adequacy decision, it means that the entire legal system of that country has been fully assessed and that data can be transferred across borders to those countries or organizations; if there is no adequacy decision, but some "appropriate" islands can be established through standard contractual clause or binding corporate rules, that is, appropriate safeguards have been taken, the data can also be transmitted across borders. Finally, derogations may be applied.[15] Therefore, the data protection agency believes that there are three different levels of data transfer: the first level is to transfer data to countries with "adequate protection"; the second level is countries that use the "appropriate safeguards" approach; and the last level is the applicable exception. (As shown in Figure 1)

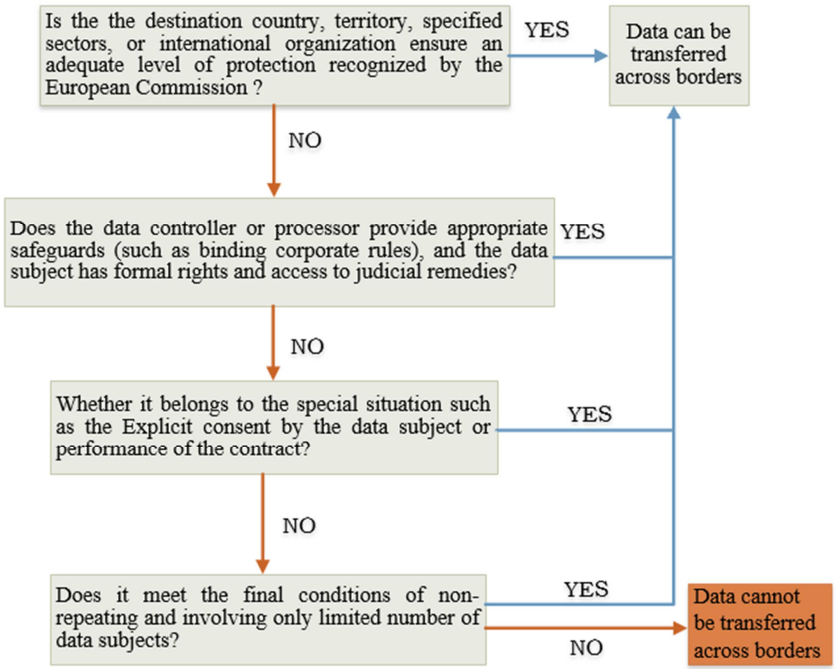

Figure 1. *Conditions for the cross-border flow of personal data.*

Throughout the institutional design of GDPR on the cross-border flow of personal data, it has established a new way of cross-border flow of data in the form of legislation. It uses standard contractual clauses and binding corporate rules to overcome the limitations of unified legal regulation, and at the same time, the scope of standard contractual clauses has also been expanded. So to a certain extent, it has promoted the cross-border data flow between the EU and third countries or international organizations, reflecting the design of a system that balances personal data protection and cross-border data flow. Although the European Commission has painstakingly designed rules to balance the relationship between cross-border data transmission and personal data protection, in practice due to the development of economy, technological progress and uncontrollable implementation may make it difficult to fully achieve the desired goals.

4. Research on the Cross-Border Data Flow Between the EU and the United States

With the frequent economic and trade exchanges between the United States and the European Union, personal data flow has gradually developed into the core and cornerstone of the close relationship between the United States and Europe in the field of business and law enforcement.[16] The two countries have strong commercial and social needs for the cross-border flow of personal data. However, because the United States adopts a loose attitude towards personal information protection based on the tradition of full trust in the market, and believes that rush legislation will restrict the development of e-commerce, the United States has not issued laws specifically for data protection and advocates the free development of e-commerce.[17] The EU therefore does not believe that the United States meets the standard of "adequate protection" of personal data and therefore does not include it in the "white list" of cross-border data flows. Restrictions on cross-border data flow have hindered business relating to the cross-border flow of personal data conducted by U.S. companies in the European Union. The United States and Europe have opened long negotiations to address the legal obstacles to the cross-border flow of data between the two places. In 2000, the U.S. Department of Commerce and the European Commission reached the U.S-EU Safe Harbor Framework. After the U.S-EU Safe Harbor Framework was ruled invalid by the European Court of Justice, the two parties reached the EU-U.S Privacy Shield Framework after urgent negotiations becoming a new scheme to regulate the cross-border flow of data between the two parties.

4.1. "U.S-EU Safe Harbor Framework" and Its Invalidation

The U.S-EU Safe Harbor Framework stipulates a series of principles and requirements for personal data protection. Enterprises can choose to join this agreement according to their commercial voluntary and the level of personal data protection. Enterprises that join the agreement must commit themselves to complying with the data protection principles under the agreement and fulfilling their obligations so that relevant data from the European Union can be obtained. Whether the data flow to the United States will face threat has always been a concern of the European Union, and the emergence of this agreement provides a single data protection mechanism for EU data flowing to the United States, Since the United States adopts a model of decentralized legislation, mainly based on industry self-regulation and market regulation. This legislative model gives concessions and compromises to the EU's unified legislation model of personal data protection. Resolving conflicts through coordination reflects the compromises and games between the EU and the United States, and provides a new direction acceptable to both sides to resolve the conflict for the increasingly integrated global economy.

But the U.S-EU Safe Harbor Framework itself has many shortcomings. First, it does not really provide a safe harbor for personal information of EU citizens. American enterprises join the safe harbor in accordance with the voluntary principle, so the agreement can only bind the voluntary American enterprises. The agreement stipulates the special exemption of national security and public interest, so when the legal obligations specified in American law conflict with the principle of safe harbor, the legal liability of enterprises for violating the agreement in order to fulfill their obligations will not be investigated. Second, the area of cross-border data flow under the agreement is limited to a certain extent. In the United States, certain industries that are not regulated by the U.S. Federal Trade Commission and other explicit government agencies are not allowed to join safe harbors, such as telecommunications, banking, insurance and so on, which makes a large number of American heavyweight enterprises have no access to the safe port, hindering the business in the European market. Thus it can be seen that the U.S-EU Safe Harbor Framework has defects in the protection of the data rights and the promotion of cross-border flow of personal data. At the same time, it lacks an effective balance mechanism.

In 2013 the Prism Gate event, the exposure of the US government and its private companies on the large-scale unauthorized processing of personal data shook the foundation of trust between the United States and the European Union. The two sides re-examined the validity of the U.S-EU Safe Harbor Framework. The Maximillian Schrems v. Data Protection Commissioner case [18] was a direct trigger for its eventual invalidation. The details of the case are as follows: Max Schrems, an Austrian, has been using the American social network Facebook since 2008. In June 2013, he filed a complaint with the Irish data protection agency, where Facebook is headquartered in Europe, alleging that Facebook transferred his own data from Facebook's Irish server to U.S. intelligence agencies based on data disclosed by Edward Snwden in 2013. He claimed that the United States did not meet the level of adequate protection under the European Union data Protection Act and required the Irish

data protection agency to ban the Irish Facebook from transferring his personal data from the European Union domain to the United States. But the Irish data protection agency believed that Schrems could not question the Safe Harbor decision made by the European Commission and rejected his appeal. The case was later referred to the European Court of Justice. The European Court of Justice has held that the data protection agencies of member States have the power to independently examine personal data protection and are not bound by the decision on safe harbor adopted by the European Commission. Moreover, the safe harbor mechanism applies only to self-certified United States enterprises that receive personal data from the European Union, but United States public institutions are not bound by it. When State-owned entities pursue interests and cause damage to personal data rights, not only does such damage fall within the scope of the mandate, but there is no effective protection mechanism for such damage. Thus, the European Court of Justice finally ruled that the U.S-EU Safe Harbor Framework was invalid.

4.2. New Development of the EU-U.S Privacy Shield Framework

After the U.S-EU Safe Harbor Framework expired, the two countries re-established the EU-U.S Privacy Shield Framework on July 12, 2016 after continuous dialogue and consultation. The "EU-U.S Privacy Shield Framework" is actually the system successor of the "U.S-EU Safe Harbor Framework". Both are designed to facilitate the free flow of personal data between the two areas while ensuring data security. [19] At the same time, the U.S-EU Safe Harbor Framework also has the following new developments in terms of rules:

In the aspect of regulation object, the agreement restricts the enterprises that join the list, the enterprises that withdraw from the list and the third party, at the same time, it also strengthens the obligations and responsibilities of American enterprises. If an enterprise that voluntarily joins the agreement withdraws from the privacy shield agreement but continues to store the personal data obtained under the agreement, it should also fulfill the corresponding obligations for the personal data. Moreover, in accordance with the "Transfer of Liability Principle", when transmitting personal data to third parties, listed enterprises should ensure that the data enjoy at least the same level of protection, unless there is clear exemption evidence, the enterprise needs to bear the consequences of violations of the rules by third-party agents. In terms of the content, the Privacy Shield Framework included not only cross-border transmission of data for commercial purposes, but also cross-border flow of personal data on national security grounds. Regarding the US government's data acquisition, the government promises that data acquisition by national institutions for national security, law enforcement, public interest and other purposes will be clearly restricted and regulated. This system responds to the request of the European Court of Justice to restrict the data flow of public institutions in Schremes case. In the area of monitoring enforcement and rights relief, the United States and the European Union have established an annual joint review mechanism, in which the European Commission and the United States Department of Commerce jointly exercise the power of review to ensure the effective implementation of the agreement. If the personal data of EU citizens are infringed, they can take remedies such as complaints to enterprises, complaints to their own data protection agencies, and free alternative dispute resolution mechanisms.

Due to the huge differences in the purposes, methods, and levels of personal data protection between the United States and the European Union, the Privacy Shield Framework is still essentially a product of compromises and concessions between the two parties. The United States has made a greater concession to the European Union's initiative than the U.S-EU Safe Harbor Framework in order to ensure the normal development of international trade between the two sides. The European Union considered the reality of close economic ties with the United States and the need to further promote cross-border data flow with the United States without including the United States in a white list of data protection to "adequate protection" levels. Bilateral negotiations and consultations ultimately led to this bilateral agreement on the cross-border flow of data. Therefore, this agreement actually better implements the EU's concept of protecting personal data rights, which not only strengthens the EU' s own data sovereignty and data governance rights, but also balances European and American data protection policies to a certain extent. It provides free flow of cross-border data between Europe and the United States, and provides institutional support and guarantee for the business activities and interactions between EU and US enterprises. In the international sense, the agreement also has a strong demonstration effect for the legislative perfection of cross-border data flow in other countries and regions, and provides a new direction for international regulation of cross-border flow of personal data.

5. Enlightenment of the Cross-Border Flow of Personal Data of the European Union to China

With the continuous expansion of the scale of digital trade, Chinese enterprises have also generated a large demand for data cross-border transmission of data. The cross-border flow of personal data is an irreversible trend, and good regulation of personal data flows is imperative. As a pioneer in the regulation of data cross-border flows, the EU's regulatory system has great reference and inspiration for China. The author intends to analyze the current regulatory situation of cross-border personal data flow in China, according to the special national conditions of China and the attitude of the cross-border flow of the personal data, put forward some suggestions for the establishment of a cross-border personal data flow mechanism in China with the practice of the EU.

5.1. Objectives of Rulemaking

EU countries have always attached importance to and protected personal data rights. They not only include personal data rights as the basic human rights of citizens in the Constitution, establishing their constitutional status, but also strengthen the protection of personal data rights through legislation. With the gradual flow of personal data through cyberspace and other media around the world, the data rights of data subjects are seriously threatened, at the same time, the data sovereignty of the European Union is also facing severe challenges. Therefore, under the new background of the digital economy era, in order to meet the challenge of the United States and other countries with large amounts of data, the European Union has constructed regulation on cross border flows of personal data with EU characteristics, where the protection of personal data plays an important role. The object of the regulation is also to balance the need of cross-border flow of personal data. From the regulations of the European Union, we can also see that the EU strives to realize the digital single market within the EU through the unified rules, promotes the internationalization of its own rules, and tries to play an exemplary role in the regulation of cross-border flow of personal data by expanding the extraterritorial effect of the law, leading the construction of global digital rules.

Compared with the European Union, China's personal data protection system has long been imperfect and has been criticized by the international community. However, with the implementation of the Cybersecurity Law, China's personal data protection system is expected to be improved in the near future. The state's stance and propensity for the protection of personal data is clearer, so that when designing cross-border data flow rules, it will also pay attention to personal data security while taking into consideration national security and law enforcement convenience. At present, China's attitude towards the cross-border flow of personal data is to stipulate data localization requirements. Unlike the EU's focus on "attack", which attempts to expand the extraterritorial effectiveness of laws, China’s main focus is on "defense". Important personal data or personal data that may affect national security, public interest, and personal data security should be stored, processed and read in China.

Therefore, from the perspective of rule-making goals, based on the different national conditions of China and the European Union, China pays more attention to national security and public interests when regulating the cross-border flow of personal data, and the protection of personal data is at a stage where it needs to be perfected. The regulation method is the requirement of data localization. However, in the light of the experience of the European Union, China can make certain changes to the purpose and attitude of legislation when it formulates the cross-border flow of personal data in the future. On the basis of improving the level of personal data protection through legislation, measures to restrict the cross-border flow of personal data should be more diversified. At the same time, it should be noted that these restrictions should not be too strict, so as not to hinder the commercial value of cross-border flows of personal data to international trade. The formulation of the rules is not only to improve the protection of personal data in China and to balance the commercial value brought by the data flow. It should also strive to promote the flow of data from other countries to China and improve China's influence and right to speak in the formulation of international data flow rules.

5.2. Specific Rules Design

5.2.1. Domestic Level

China started late in the field of data cross-border flow rules, but in recent years, with the rapid development of China's Internet industry and the increase of data cross-border transmission demand, the government has begun to pay attention to the cross-border flow of data. Although there is still no systematic special legislation, the relevant contents are scattered among all kinds of laws and regulations, departments regulations. However, a series of useful attempts have been made to balance personal data protection and personal data commercial utilization.

The Cybersecurity Law, promulgated in 2017, deals with the cross-border flow of data at the legal level, Article 37 of which states: "personal information and important data collected and generated by operators of critical information infrastructure in the territory of the People's Republic of China shall be stored within borders. If it is really necessary to provide it abroad for business needs, it shall conduct a security assessment in accordance with the measures formulated by the state cyberspace department in conjunction with the relevant departments under the State Council; if otherwise provided for by laws and administrative regulations, such provisions shall be followed." This article establishes the general principle that personal data and important data generated in the operation of critical information infrastructure are stored in the territory, it shows our country's cautious attitude towards important personal information and data. In order to further implement and perfect the provisions of Article 37 of the Cybersecurity Law, the Cyberspace Administration of China issued the Cybersecurity Review Measures (draft for comments) and the Measures for the Security Assessment for Cross-border Transfer of Personal Information (draft for comments) and solicited opinions publicly in 2019. The latter abandons the way in which personal information and important data are processed together, and breaks through the Cybersecurity Law. The requirements for the data exit assessment subject were broadened by operators of critical information infrastructure to all network operations. The personal data collected by the network operations should pass the security assessment by the provincial cyberspace administration. If the exit will have an impact on national security, public interest or personal information security, it shall not be transmitted cross border. However, the above measures are still at the stage after the conclusion of the consultation, which has little practical significance. At the same time, China has also put forward different degrees of data localization requirements for personal information in special industries through departmental regulations and other forms. For example, in the

financial industry, the People's Bank of China has issued a Notice Regarding the Effective Protection of Personal Financial Information by Banking Institutions, requiring that personal financial information acquired inside China shall be stored, processed and analyzed inside China. It can be seen that, in recent years, the regulation of cross-border data flow management has been made through relevant laws and regulations, department regulations and so on. Although special unified legislation has not yet been formed, relevant legislation and law enforcement activities have become more and more frequent.

Comparing the existing legal rules of cross-border flow of personal data between the EU and China, we can find that the cross-border flow of personal data in the EU is carried out under complete and systematic legal rules, with good institutional protection. Although a series of legislative attempts have been made in the cross-border flow of personal data in our country, some measures are still unwritten, many of the written ones are only regulatory documents. And there is still a lack of systematic written and mandatory data cross-border flow rules system. Therefore, it is still necessary to promote the formulation of the special law, modify and perfect the relevant supporting rules so that it can connect with the special law and cooperate with each other to build a systematic rule system. In terms of specific regulations, compared with the European Union, China's intervention in data cross-border flow activities is deeper and more direct, and it has adopted a one-size-fits-all approach to regulate the cross-border flow of personal data by requiring some data to be retained in China. The EU designed complete legal rules where the personal data can flow freely between member states. And cross-border flow of personal data with the third countries is legitimate only if different conditions are met at different levels. The reform direction of EU data cross-border policy also shows that if it is not possible to provide a diversified and effective cross-border channel, the policy direction cannot be communicated to the market. Diversified legal cross-border channels can guide enterprises to achieve their own data cross-border needs through predictable stability mechanisms, while simultaneously achieving user privacy and data security goals set by regulators. Therefore, China needs to consider in depth how to adopt a scientific and effective mechanism to design a specific and complete cross-border flow rule of personal data to provide as rich legitimate channels as possible for reasonable and orderly data flow in order to effectively balance data flow and security benefits.

Specifically, China can draw on the following system experience of the EU and set up a diversified legal flow mechanism in line with the needs of our country in combination with the actual situation of our country:

On the basis of improving the level of data protection, classify the data flowing across borders, and adopt different management methods for different types of data. For extremely important data, such as state secrets, a similar negative list model can be adopted, which clearly lists that data transmission can only be stored and processed in domestic data centers and prohibits cross-border transmission; strict control should be adopted for data transmission that may affect national security and social and public interests. These data needs to be submitted to the industry authorities for assessment and then make a decision on whether to allow the exit. Non-sensitive, non-large amounts of data cross-border transmission are based on self-assessment.

Drawing on the EU's "binding corporate rules", establish a corresponding system to regulate the cross-border transmission of personal data by multinational enterprises, and establish minimum standards for personal data protection in the region. However, this system needs to be established on the premise of improving the level of personal data protection in our country. At present, the level of personal data protection in many countries with close economic cooperation and exchanges with our country is higher than that in our country. If the minimum standard protection of personal data protection is not perfect, then the system itself has only disadvantages and no benefits to our country.

In accordance with the main standards of security assessment, establish a model guideline for data cross-border flow agreement, similar to the EU standard contractual model, and guide companies to control data exit risks through contract legal mechanisms during data exit.

Industry associations and other self-regulatory organizations are encouraged to participate in safety assessments. As a supplement to the market mechanism, it plays a role in security assessment, thereby establishing a dynamic data management order that can be implemented on the ground.

5.2.2. International Level

In addition to perfecting the unified data flow rules in the region, the European Union has also signed a bilateral agreement with the United States on the cross-border flow of personal data through negotiations, which to a certain extent has balanced the different demands of the two on the cross-border flow of personal data. At the same time, many countries have cooperated on the regulation of cross-border data flow at the international level, such as the bilateral agreement between the European Union and the United States, the practice of APEC on cross-border data flow, and the arrangement of cross-border flow of personal data in new free trade agreements such as TPP, USMCA. Thus it can be seen that the negotiation and cooperation of bilateral and multilateral data cross-border agreements at the international level is an effective and feasible scheme to improve the legal rules of cross-border flow of personal data. However, China does not have a bilateral agreement similar to the Privacy Shield Framework between Europe and the United States, and has not participated in the relevant international cooperation. Therefore, it is suggested that China can more involve the related issues of personal data in international consultations or political negotiations with EU and other countries or regions, and explore the cross-border flow of personal data between the two places on the basis of seeking the consensus of both sides on personal data protection, so as to provide each other with diversified channels for cross-border flow of personal

data. It is also suggested that China can use regional negotiations such as RCEP, FTAAP to seek to establish a cross-border in line with China's interests. The context data flow rule. With the improvement of China's status in international affairs, China can even use the Boao Forum for Asia, the “Belt and Road” strategy and so on to open regional personal data cross-border flow rules of cooperation agreements or rules negotiation and negotiation. The problem of data flow can be solved by a regional data flow protocol.

6. Summary

In the era of the rapid development of information technology, the cross-border flow of data not only creates great commercial value and economic benefits, but also brings many risks, which brings great challenges to the legal regulation of cross-border flow of personal data. As the most advanced and perfect region for the regulation of cross-border personal data flows around the world, the European Union has explored the balance between personal data protection and data cross-border flows. Its latest legal text, the General data Protection regulations, specifies the rules that allow personal data to be transmitted to third countries or international organizations. In addition to legislating to regulate the cross-border flow of personal data, due to the close economic ties between the European Union and the United States, the EU negotiated and negotiated with the United States for the purpose of facilitating cross-border data flow. The two sides reached the Safe Harbor Framework and the Privacy Shield Framework reached again after the expiration of the former, stipulating rules for the cross-border flow of data between the two areas. The EU's relevant rules on the cross-border flow of personal data provide reference for the establishment of China's relevant system. It is recommended that China improve its legislation on the cross-border flow of personal data, improve the operability of the law, and at the same time strengthen international cooperation and take full advantage of regional negotiations. The construction of personal data cross-border rules should seek to balance personal data protection and the promotion of cross-border personal data flows.

References

[1] UNCTAD. The value and role of data in electronic commerce and the digital economy and its implications for inclusive trade and development, third session, Geneva, 2019. P11.

[2] James Manyika, Jacques Bughin, Jonathan Woetzel. The New Era of Global Flows, McKinsey Global Institute, 2016.

[3] Anupam Chander. Data Nationalism. Emory Law Journal, 2015, 64: 677-740.

[4] Xu Duoqi. The International Pattern of Cross-border Movement Regulation of Personal Data and China's Response to it, Legal Forum, Vol 3, 2008, pp. 130-137.

[5] Article 25 of Directive 95/46/EC.

[6] Article 26 of Directive 95/46/EC.

[7] Van Alsenoy, Brendan. Liability under EU Data Protection Law: From Directive 95/46 to theGeneral Data Protection Regulation, Journal of Intellectual Property, Information Technology and Electronic Commerce Law, Vol 3, 2016, p. 271.

[8] Arctcle 45 of General Data Protection Regulation.

[9] Arctcle 46 of General Data Protection Regulation.

[10] Wang Rui. Main Content and Impact Analysis of EU General Data Protection Regulation, Financial Accounting, Vol 8, 2018, pp. 17-26.

[11] Gong Yongqin, Wang Jian. A study on the rules of cross-border movement of APEC and EU personal data, Asia-pacific Economic Review, Vol 5, 2015, pp. 9-13.

[12] Wang Rong. The Big Data Age: Data Protection and Flow Rules, Beijing: Posts and Telecom Press, 2018.

[13] Arctcle 49 of General Data Protection Regulation.

[14] JD Law Institute. Comments and Practice Directions of the General Data Protection Ordinance, Beijing: Law Pree, 2018.

[15] Christopher Kuner. European Data Protection Act, Beijing: Law Press, 2008.

[16] Liu Biqi. A Review of U.S.-European Private Shield Agreement, Chinese Review of International Law, Vol 6, 2016, pp. 35-47.

[17] Hu Wei. The Value Orientation of Cross-border Data Flow Legislation and's Choice, Journal of Social Sciences, Vol 4, 2018, pp. 95-102.

[18] Maximillian Schrems v. Data Protection Commissioner, Case C-362/14. Judgment of the Court (Grand Chamber) of 6 October, 2015.

[19] Schrems, Max. The Privacy Shield is a Soft Update of the Safe Harbor, European Data Protection Law Review, Vol 2, 2016, pp. 148-150.