ISSN 2706-6827 Vol. 5, Issue 16: 105-110, DOI: 10.25236/IJFS.2023.051616

The Necessity of Extraterritorial Application of the Personal Information Protection Law and Suggestions for Its Improvement

Guanxiang Wang

School of Graduate, People's Public Security University of China, Beijing, China

Abstract: *With the development of big data technology and the arrival of the digital age, it is difficult to regulate the cross-border flow of data under the jurisdiction of national territorial scope, and it is impossible to achieve the balance between data sovereignty and cross-border data law enforcement. Data flow is related to national security and economic development. The extraterritorial application of the Personal Information Protection Law should balance the interests of data flow and international security. While maintaining national data security, it is also necessary to reduce data barriers and promote the departure of legitimate data. At the same time, it is also necessary to proceed from reality, further clarify the important role of the principle of "territorial jurisdiction", strengthen international cooperation, and promote the formation of a global data jurisdiction power system, so as to achieve orderly global data governance.*

Keywords: *extraterritorial application; The place where the behavior occurs; Cooperation and game; Data exit*

With the development of The Times, the digital economy has become an important driver of international competition in a world undergoing profound changes unseen in a century. With the development of big data and Internet of Things technology, the legal nature of data is no longer limited to the bearer of individual interests. It is a new type of "asset" bearing social and national interests, which is formed under the actual social interaction and has economic and social value such as identification and analysis. Which makes it necessary for countries to safeguard their national interests to expand the extraterritorial effect of data protection legislation. In the Opinions of the CPC Central Committee and The State Council on Building a More Complete Market-oriented Allocation System and Mechanism of Factors issued on April 9, 2020, China clearly listed data, land, labor, capital and technology as the five major factors of production for the first time, and stressed the need to accelerate the cultivation of data factor markets, and required the development of data privacy protection systems and security review systems in terms of legal protection. With the advancement of legislative work, the Personal Information Protection Law will come into effect in November 2021, which will be a milestone for the protection of Chinese citizens' personal information.

1. The raising of issues

How to build a perfect personal information protection system to protect China's data sovereignty security, so as to grasp the initiative and discourse power in the formulation of international governance rules in cyberspace, create orderly data circulation channels, and safeguard national security and economic development? With the development of big data technology, data circulation becomes more frequent. As an important cornerstone of data circulation, it is of great significance to realize effective protection of personal information. At present, China has relatively complete regulations on the collection and use of domestic data. Although the current Personal Information Protection Law of China has relevant provisions on overseas data processing activities, there are still some practical difficulties in how to realize the extraterritorial application of the Personal Information Protection Law. Based on the current legislative status at home and abroad, this paper will focus on the effectiveness of personal information protection, and provide some references for the improvement of China's extraterritorial application of personal information protection system.

ISSN 2706-6827 Vol. 5, Issue 16: 105-110, DOI: 10.25236/IJFS.2023.051616

2. Definition of the concept

According to Article 1034 (2) of the Civil Code, "Personal information is information recorded electronically or by other means that can be used alone or in combination with other information to identify a specific natural person, including the natural person's name, date of birth, ID number, biometric information, E-mail, telephone number, health information, whereabouts information, etc." Its core lies in "being able to identify a specific natural person". Obtaining "extraterritorial jurisdiction" is the prerequisite for a country's law to realize extraterritorial application. Within the permissible scope of international law, a country can enfranchise the extraterritorial effect of a certain law by expanding its territorial application scope or object application scope in legislation, that is, the external manifestation of state exercising legislative jurisdiction. From this point of view, the extraterritorial protection system of personal information refers to a legal system in which a country implements jurisdiction over the acts of natural persons or organizations that process personal information outside the jurisdiction of a certain law, so as to extend its jurisdiction beyond its territory. It is determined that its processing behavior should comprehensively consider the nature and extent of its behavior and the importance of data protection, so as to consider whether the extra-territorial information data controllers and processors should be included in the jurisdiction of our country's laws. From the theoretical perspective, "data sovereignty" provides a more explanatory basis and theoretical basis for the extraterritorial effect system of the personal information Protection Law. The academic community generally believes that data sovereignty refers to a country's supreme power over the data generated by individuals, enterprises and related organizations within the jurisdiction of its political power. Specifically, data sovereignty has two connotations: "Internally, it is embodied that a country has the supreme power over the generation, processing, analysis and utilization of any data within the jurisdiction of its political power; Externally, it means that a country has the right to decide what procedures and ways to participate in international data activities, and has the right to take necessary measures to protect data rights and interests from other countries." [1]Based on data sovereignty, a State can obtain jurisdiction over the processing of information by natural persons or institutions in accordance with law. With the development of technology, the benefits carried by data are no longer limited to the individual level. Due to the social interaction it generates, personal data also involves the interests of other (not) specific people, and even the interests of national security. Therefore, based on the theory of data sovereignty and the need to safeguard national security, a country's jurisdiction to obtain overseas data has a legitimate basis.

3. The necessity of realizing extraterritorial protection of personal information

3.1. Protection of the legitimate interests of individuals

With the development of big data technology, data flow has become more convenient, and jurisdiction based on the scope of national territory has become difficult to regulate the cross-border flow of data, nor can it achieve a balance between data sovereignty and cross-border data law enforcement. From the perspective of personal information itself, the data carrying personal information is different from other general data. It focuses on identification, that is, it can correspond to an individual through this information. In the context of big data, there are digital personality, commercial utilization,[2] right to personal information and other rights and interests, among which personal interests include both personality interests and property interests. At the same time, because it also carries the interests of other people who are not specific, a collection of multiple interests is formed. At the same time,[3-4] due to the development of modern technology, personal information data not only carries the basic information of the data subject, but also the data controller can use it freely without being detected. At the same time, considering the cost of individual litigation, the cost of individual extraterritorial litigation is high. Strengthening the protection of the basic rights and interests of data subjects is the logical premise of the Personal Information Protection Law. Compared with the high cost of private rights relief, public rights relief is therefore more necessary. Considering the effectiveness of the right relief, only civil liability is not enough to complete the task of personal information protection. Based on the convenience and mass of current data transmission, individual tort litigation has great difficulties in determining causality and compensation. Especially for extraterritorial infringement, individual litigation costs more and is more difficult. Therefore,[5] it is necessary to have a dedicated authority at the level of public power to achieve relief.

ISSN 2706-6827 Vol. 5, Issue 16: 105-110, DOI: 10.25236/IJFS.2023.051616

3.2. Safeguarding national sovereignty and security

As cyber sovereignty is characterized by a strong de-territorialization, cross-border data in cyberspace makes the national governance of data go beyond its territorial scope, and the traditional concept of judicial jurisdiction can no longer handle cross-border[8]137-138 data in cyberspace. From the perspective of the legislation of countries around the world, the global flow of data will be greatly increased under the background of the development of big data technology. For the consideration of digital sovereignty, public security and economic interests, all countries try to adopt double standards. On the one hand, they try to expand the extraterritorial application of domestic legislation as much as possible to obtain data from other countries; On the other hand, they try their best to avoid the outflow of domestic data and establish "data barriers", which makes it difficult for a country's own legislation, judicial and administrative law enforcement to solve the extraterritorial personal data protection generated in the data flow in the context of global data flow. As mentioned above, personal information data under big data technology not only involves individual interests, but also involves personal data. It often involves social interests and even national security, and has gradually become a social resource. [5]Therefore, in order to cope with the future international challenges, it is necessary for China to seize the initiative in the future cyber space, maintain the security of our data and the protection of personal information, and build an extraterritorial application framework of our data protection.

4. Current situation and analysis of legislation on extraterritorial application of data protection

4.1. Current legislation status in China

According to Article 3 of China's Personal Information Protection Law, "This Law shall apply to activities outside the territory of the People's Republic of China that process the personal information of natural persons within the territory of the People's Republic of China, as long as they involve the purpose of providing products or services to natural persons within the territory of China and the analysis and evaluation of natural persons within the territory of China." It can be seen that its applicable effect extends to the activities of processing the personal information of domestic natural persons abroad, which clearly extends the scope of China's data jurisdiction to extraterritorial areas. From the perspective of jurisdiction, the extraterritorial jurisdiction in the Personal Information Protection Law does not break through the principle of actual connection in the selection of connection points, and is a reasonable expansion of jurisdiction based on China's data sovereignty. At the same time, according to Article 42, "Where overseas organizations or individuals engage in personal information processing activities that infringe upon the personal information rights and interests of citizens of the People's Republic of China, or endanger the national security and public interests of the People's Republic of China, the national cyberspace administration may add them to the list of restrictions or prohibitions on the provision of personal information and announce them. It can be seen that China's current extraterritorial information processing behavior mainly takes the "behavior" itself as a consideration factor for the legislative power of extraterritorial jurisdiction, breaking the restriction of territorial jurisdiction, and having certain progressive significance from the theoretical level; From the perspective of the Data Security Law, according to Article 1, the purpose of this Law is to "regulate data processing activities, ensure data security, promote data development and utilization, protect the legitimate rights and interests of individuals and organizations, and safeguard national sovereignty, security and development interests". Based on the development of big data technology, personal information is more electronically transmitted, therefore. As the object of data processing activities, personal information processors should carry out relevant activities within the legal framework of safeguarding national sovereignty and security interests. It can be seen from this that personal information security is a part of the overall national security, and information processors have the obligation to attach great importance to and protect personal information when collecting, processing and processing.

It can be seen that, based on the current legislation of China's legal system on the security of citizens' personal information and data, China has clarified the legal protection of personal information, including the rights of information subjects and the obligations that information processors should abide by, and clarified the boundaries of personal information; China's extraterritorial jurisdiction in the Personal Information Protection Law has broken through the traditional "territorial jurisdiction" principle based on "the result of the act", expanded the jurisdictional effect to the "place of the act", clarified the corresponding sanctions against the harmful behavior, stipulated the rules of data exit in China and the obligations of the information processor, and also defined the specialized organ for the relief of rights. However, the current protection of data security in China still adopts the mode of "empowerment +

ISSN 2706-6827 Vol. 5, Issue 16: 105-110, DOI: 10.25236/IJFS.2023.051616

limitation of rights", that is, using the data subject's "knowledge + consent" to determine the data controller and processor's processing behavior boundary, while ignoring the economic value and public interests of the data itself.

4.2. The EU General Data Protection Regulation and the US Cloud Act

The General Data Protection Regulation (GDPR) adopted by the European Union in 2018 is of great significance for global data protection. Article 3 of the GDPR sets out the geographical scope of application of the Regulation, which provides for the jurisdiction of data controllers and processors whose place of business is in the EU, regardless of whether the data processing takes place within or outside the EU. At the same time, the European Data Protection Board has adopted the criteria of "actual operation criteria" and "target market criteria" under the provisions of the Guidance on the Interpretation of the Geographical Scope of the GDPR. Regardless of whether the data subject has an entity in the EU, as long as it provides products or services to the domestic subject, or monitors its behavior, or as long as it processes and holds the data of the data subject residing in the EU, it is subject to its regulation. It can be seen that countries within the EU have the basis for extraterritorial jurisdiction, reflecting the idea of defining the scope of jurisdiction according to the effect of the behavior itself. [6]139-140That is, the "place where the act occurred" is taken as the connection point for initiating the extraterritorial jurisdiction. In the legislative process, GDPR advocates the expansion of geographical scope, and the reason why it chooses a unilateralist stance in the regulation of data processing behavior is mainly restricted by the limitations of the existing international law rules to provide personal data protection. From the perspective of technological development and the EU's own situation, it not only addresses the jurisdictional difficulties caused by cloud computing technology in other countries and regions, but also fully reflects the EU's determination to compete for the right to speak in global data competition through personal data rights. It is precisely due to the bilateral rules are characterized by rule fragmentation, concept differentiation and high negotiation costs, multilateral rules show the characteristics of soft law and lack of legal binding force, the EU has set too strict data protection standards in GDPR and other objective facts, the EU can only hope to expand the geographical scope of GDPR application. [7]68-70Also, as some scholars have put it, the EU has promoted the overseas expansion of its legal system, "a disguised extension of its territory in cyberspace". [8]Unlike the European Union, which regards the right to protection of personal information as a basic right for systematic protection of legislation, the United States does not legislate for uniform personal information protection, but separately regulates various fields such as business, finance and medical care, and realizes diversified regulation for different types of information. This kind of domestic law regulation of industry self-regulation in the United States reflects the maturity of the self-regulation rules of domestic enterprises in the relevant market, which is conducive to improving the efficiency of data utilization by enterprises and creating greater economic benefits. In order to solve the dilemma of international judicial assistance, the United States has introduced the Cloud Act, which aims to solve the problem of decentralized storage due to changes in data storage locations and data fragmentation. However, as some scholars argue, "The Cloud Act actually unilaterally gives the US government 'long-arm jurisdiction' over the vast majority of the world's Internet data, which poses a great challenge to countries that emphasize 'privacy protection' and even 'digital sovereignty' and is bound to trigger a backlash."

To sum up, based on personal information as an embodiment of the basic rights of citizens, the EU further expands the scope of extraterritorial effect of the law and establishes the principle of jurisdiction based on the territorial principle and supplemented by the principle of effect. Although it reflects the emphasis on the control right of data subjects, such strict "entry" conditions are not conducive to the development of foreign investment in the EU. And the adverse impact on its own economy. [9]5-7However, the United States mainly starts from its unilateral interests, and uses technology and market dominant American enterprises to control global data in order to maximize its national interests. Such data jurisdiction concept constructed on the basis of unilateralism will eventually weaken the benign interaction between the United States and other countries in data governance and business exchanges, which is not conducive to the formation of a global orderly data governance order. At the same time, considering the legislation of various countries, under the current situation that international practices and treaties have not yet been formed, the extraterritorial effect expansion through domestic legislation is a common approach for most countries to safeguard data sovereignty and participate in the international governance of cyberspace.

ISSN 2706-6827 Vol. 5, Issue 16: 105-110, DOI: 10.25236/IJFS.2023.051616

5. Suggestions for improvement

5.1. The game between economic development and national security

As mentioned above, in the context of modern technology, the information carried by data has gradually expanded from "individual interests" to non-specific social interests and national security interests. Therefore, from the perspective of interest balance, data, as one of the most important production factors at present, the state imposes excessive restrictions on the cross-border flow of data, which will affect the management rights of enterprises. This involves the basic attitude of various countries towards cross-border data flow, and a rational balance should be struck between state intervention and enterprises' independent operation. In the relevant legislation, it is of great significance to set up diversified exit conditions for data, especially the exit conditions through the signing of contracts between data processors and overseas data recipients. According to the relevant provisions of China's "Personal Information Protection Law", data exit needs to go through the security assessment of the national network information department, considering the scope of information exit assessment standards, still need to be further clarified. In this regard, the author believes that it is necessary to carry out a double-layer analysis of "quantity" and "quality" of information, with "quality" as the main and "quantity" as the supplement. [10]The reasons are as follows: First, from the legislative purpose, the effective protection of personal information is the logical premise of the Personal Information Protection Act, but personal information is often inseparable from national security, and national security is the prerequisite for the protection of personal information; Second, although some scholars advocate that the right[11] of individuals to control their information should be clarified, from the characteristics of data generation, it is non-exclusive, with both personal and public interests, and cannot become an absolute, exclusive and universal right object, otherwise it will hinder the development of digital society. [12]Therefore, data issues related to personal interests should not be overly emphasized, and the overall national security should be taken into account. However, in order to realize the analysis of data subjects, data controllers or processors will inevitably build on a large amount of data. Therefore, as long as the number of outbound data reaches a certain scale to realize the analysis degree of data subjects, it also involves the overall data security of a country, and security assessment needs to be carried out according to this standard. Therefore, in order to better realize the balance between the interests of data circulation and national security, data exit should be based on the overall security and interests of the country, with the quantity standard as the auxiliary consideration standard.

5.2. Give further play to the role of "territorial jurisdiction"

According to the relevant provisions of China's Personal Information Protection Law, China takes the "place of occurrence" as the standard for extraterritorial application of this law, that is, when overseas data controllers and processors collect and process information about Chinese data subjects, they must comply with Chinese laws. However, this is only stipulated from the theoretical level and returned to the reality. How to prove that there is a collection and processing of personal information of Chinese data subjects abroad, the cost of obtaining evidence is high. As some scholars have said, "In the environment of cloud computing, it is difficult to accurately determine the location of personal data storage and equipment processing specific personal information, and the location of data processing behavior is fuzzy, so the investigation of the 'place of behavior' should be weakened, and the investigation of the 'data processing behavior' itself should be strengthened." [5]76-77According to the experience of EU legislation, if the "place of operation" company forms an "inseparable link" with the "data controller and processor", the overseas data processing behavior will be "naturally" included in the territorial jurisdiction of GDPR. Therefore, the author believes that when determining the scope of extraterritorial application, starting from the actual cost, we should focus on "territorial jurisdiction" and combine the standard of "place of conduct" to achieve the maximum effect of legal regulation.

5.3. Strengthen international cooperation and promote the orderly exchange of data among countries

The effectiveness and effectiveness of a legal system should be considered. Extraterritorial legislative power often reflects the effectiveness of extraterritorial application, while extraterritorial enforcement power often reflects its effectiveness. How to implement extraterritorial law enforcement is the key to evaluating the extraterritorial effectiveness of a country's legal system. With the development of society and the increasingly close relationship between sovereign states, the essence of the current global personal information regulation dilemma lies in the fact that countries around the world mainly expand the extraterritorial effect through domestic laws, and lack of unified and effective international standards.

ISSN 2706-6827 Vol. 5, Issue 16: 105-110, DOI: 10.25236/IJFS.2023.051616

Especially in the context of the 2020 COVID-19 pandemic, effective channels of data exchange have been built to promote the sharing of epidemic and medical data among countries. Has become the consensus of all countries in the world. Therefore, in this context, data governance through multiple approaches is the way to achieve the development of the international community. According to Article 38 of China's Personal Information Protection Law, "China abides by the relevant provisions of the international treaties or agreements to which it is a party on data exit", which means that international soft law based on international treaties or agreements has room for implementation. Therefore, global uniform rules for cross-border data transfer have not yet been established. Countries should establish a multilateral framework for data flow through communication and consultation, and ensure the coordination and unification of data jurisdiction and data localization rules by respecting national sovereignty and basic rights of citizens, ensuring information security and Internet freedom, upholding the legality of state actions and enterprise self-discipline as the basic principles.

Conclusion: To create a strict personal information protection system is not to prohibit the use of personal information, but to create a safe information environment, through big data technology analysis, is conducive to the formulation of social policies and the improvement of public service level, and the ultimate benefit is the social individual. Although the construction of discourse systems in the field of cross-border data in Europe and the United States has lasted for many years, and occupies a leading position in the formulation of international rules, China still has a huge space to create and develop its own discourse system. On the basis of safeguarding national sovereignty, security and development interests, the Personal Information Protection Law imposes restrictions on overseas retrieval of personal information, laying the foundation for building a China-led international data cross-border flow system.

References

[1] Qi Aimin, Pan Jia. Establishment of data Rights, data Sovereignty and Basic Principles of Big Data protection [J]. Journal of Suzhou University (Philosophy and Social Sciences Edition), 2015, 36(01):64-70+191.

[2] Zhang Li 'an, Han Xuzhi. Private Law attribute of Personal Information Right in the era of Big Data [J]. Law Forum, 2016, 31(03):119-129.

[3] Gao Fuping, Yin Labei. Personal information rights and interests in data: Paradigm shift from protection to governance. Zhejiang Social Sciences,2022,(01):58-67+158.

[4] Shen Hongyu. Challenges and Countermeasures of the legal system of Personal Information Protection in the context of big Data flow -- based on the perspective of Comparative law [J]. Chinese Journal of Applied Law,2021,(02):1-13.

[5] Yu Shengjie, Lin Yanping. The regulatory logic, practical reflection and legislative Enlightenment of the extraterritorial effect of the General Data Protection Regulation [J]. Chongqing Social Sciences, 2020, (06):62-79.

[6] Cole D D .Outsourcing Terror: Extraordinary Rendition and The Necessity For Extraterritorial Protection of Human Rights[J].Prisoners in War, 2010, 101:372-381.DOI:10.1590/S0073-47212011000300011.

[7] Xueping Y , School L , University L .On the Extraterritorial Application of the Indian Competition Laws and Its Inspirations for Developing Countries[J].Legal Forum, 2015.

[8] Feng Junwei. Cross-border data governance should pay attention to the overall consideration [J]. China Information Security, 2021, (05):75-77.

[9] Ding Xiaodong. Dilemma and Outlet of Private Law Protection of Personal Information [J]. Legal Studies, 2018, 40(06):194-206.

[10] Zhang Linghan. Three Dimensions of Cross-border Personal Information Flow System. China Law Review, 2021, (05):37-47.

[11] Yang Lixin. Personal Information: Legal Interest or Civil Right—Interpretation of "Personal Information" stipulated in Article 111 of the General Provisions of the Civil Law [J]. Legal Forum, 2018, 33(01):34-45.

[12] Zhang Hui. Community of Shared Future for Mankind: Contemporary Development of social Basic Theories of International law. Social Sciences in China, 2018, (05):43-68+205.