The Establishment of the Legal System of Data Outbound Transfer from the Perspective of Comparative Law

Liang Chu[1, a], Fangrui Ding[1, b], Yanbo Sun[2, c]

[1] School of Law, Hangzhou City University, Hangzhou, China

[2] School of Faculty, Hangzhou City University, Hangzhou, China

[a] CL389155725@163.com, [b] 521760661@qq.com, [c] 2218686477@qq.com

Abstract. Data are considered as one of the basic production factors, the cross-border flow of which has brought new development opportunities for the digital economy, but the unordered data outbound transfer has brought new challenges to national, public and enterprise interests, and the rights and interests of data subject. The legislation of different countries and regions has basically formed three paradigms: absolute prohibition, complete openness and conditional cross-border transmission. China should draw on the mature international mechanisms for the control of cross-border data flows, and combine its national interests and data protection realities to establish a legal supervision mechanism with hierarchical and categorical data management and control as the core, so as to realize the secure and free cross-border flow of data.

Keywords: Comparative Law; Data Outbound Transfer; Data Security; System Construction.

1. Introduction

Data is the fifth major production factor followed after land, labor, capital and technology, and is the new oil in today's world. The surge, circulation and reuse of data have promoted production, innovation, efficiency and growth, and become a new source of huge economic and social value. The value release of data production factors depends on circulation and sharing. In the era of digital economy, products and services tend to be globalized, and cross-border transportation and storage of massive data has become an inevitable demand scenario. For example, in international trade, the address and order information of domestic buyers inevitably flow to overseas enterprises, and if overseas enterprises cannot protect the personal information of information subjects by perfect means, personal privacy rights will inevitably be violated. Not only the interests of data subjects, but also the interests of enterprises, the public and the countries may be violated in the disorderly flow of data, so it is urgent to legislate and regulate cross-border data transmission.

2. Legal challenges to cross-border flows of data

The formulation of cross-border data flow policies is the product of the dynamic balance among national interests, industrial interests and risk control. There must be contradiction between the utilization and protection of data, and the value release of production factors of data depends on the frequency of circulation, but the circulation of data will inevitably lead to an increase in the difficulty of risk control. Adopting loose regulations on cross-border flow of data is conducive to the development of the digital industry, but it will increase the difficulty of risk control. Meanwhile, it may harm the national interests of developing countries while help achieve international data hegemony through data flow for developed countries. Adopting strict regulations on cross-border flow of data is not conducive to the development of digital industries, but it will reduce the difficulty of risk control, avoid data control for developing countries, but make it difficult for leading enterprises to develop in developed countries. In conclusion, whether the regulations are loose or strict, it will cause challenges in the protection of personal privacy, corporate interests, and national security if damaging the dynamic balance among three factors.

2.1 Challenges in personal privacy protection

As mentioned above, in the cross-border flow of data, the cross-border flow of personal information is inevitable, and even the outbound transfer of personal data is the prerequisite for obtaining high-quality services, but if the overseas data recipient cannot effectively protect personal privacy or abuses personal information, the security of personal information becomes difficult to guarantee. At present, more and more industries and enterprises are focusing on the collection and utilization of personal information, but if they are unregulated and too hidden, it will lead to algorithm discrimination and undermine the equal rights of individuals. Excessive algorithm involvement will change personalized recommendation to personalized control, causing individuals to lose the right to freely absorb diverse information, making groups with different views antagonistic to each other and undermining social stability, so that individual and collective wisdom are erased; Moreover, criminals use various means to illegally steal personal information and resell it for profit, directly infringing on the personal information right, resulting in leakage and abuse of personal information.

At present, there is no international consensus on the cross-border flow of personal data, and a unified international law guarantee system has not been constructed. The protection of personal privacy still stays in the FTA between individual countries and regions, and the "Cross-border Privacy Protection Rules"(CBPR) advocated by intergovernmental international organizations such as APEC has not become a common standard generally adopted by the international community, so the cross-border protection of personal privacy has become a challenge for cross-border data flow.

2.2 Challenges in corporate interests' protection

From a practical point of view, the typical usage scenario of data elements is enterprise data, that is, secondary data obtained by enterprises processing user data through various big data technologies, such as user personal information and other data obtained by network service providers through privacy policies and other means. The secondary data obtained by enterprises is an important business resource for enterprises and an important way to gain advantages in market competition. The collection, formation and industry research and judgment based on secondary data are intellectual achievements of enterprises. Although big data technology itself is protected by traditional intellectual property rights, there is no consensus on how to protect the big data collection containing the fruits of labor of data controllers. At present, judicial practice mainly carries out protection through trade secret protection rules, competition rules and criminal law rules. However, they all avoid the issue of confirming corporate data rights. The lack of rules for confirming data rights makes it difficult to clarify the responsible subjects of data in cross-border flows, increasing the risks and bringing challenges to the protection of legitimate business interests of enterprises.

2.3 Challenges in national security protection

The cross-border flow of data may also cause national security challenges. The current digital industry of various countries is still in a serious imbalance because data flow from developing countries to developed countries so that developed countries can rely on big data, artificial intelligence and other technologies to analyze the human behavior patterns hidden in the data of developing countries, including food preferences, living habits, health conditions, etc., to accurately picture the social situation of the developing countries, and gather targeted intelligence, threaten national security, and further promote the formation of data hegemony, finally becoming another major weapon of unilateralism. At the same time, data leakage can also affect politics, such as Facebook's influence on political elections in the United States through personalized recommendations. The US "prism" proves that the United States has violated and threatened the security of other countries by invading other countries' network systems, illegally obtaining other countries' data and transferring them across borders.

All in all, the cross-border flow of data will cause security risks in many aspects such as personal privacy, commercial interests, and national security, which will bring challenges to countries' cross-

border data supervision, so how to balance data utilization and data protection has become a major difficulty in the current legislation.

3. Legislative models and analysis on international cross-border data transfer

3.1 Conditional cross-border data transfer represented by the EU

EU legislation focuses on protecting individual rights, and data flow regulatory policies are mainly reflected in the personal data protection regulation. The sphere of application of the EU GDPR includes data controllers and processors who operate and carry out data activities and intent to do them within the European market. The EU's establishment of the personal data outbound transfer management system is based on the "adequacy protection decision" as the core to realize the basic values of personal data protection.

The adequacy protection decision is the primary principle of GDPR, that is, EU data can only be freely transferred to the "adequacy decision" area, where its data protection is considered by the EU to reach the level of "adequate protection", while the data flowing to other countries and regions needs to go through adequate safeguards except for specific occasions including user consent, the need to execute contracts, etc. In practice, only 11 countries and regions are considered to have adequate protection: Andorra, Argentina, Canada, Switzerland, Faroe Islands, Guernsey, Isle of Man, Jersey, Israel, New Zealand and the Eastern Republic of Uruguay.

The assessment criteria for the "adequacy protection decision" are as follows: first, the legal situation of the third country, including the protection of personal data, the regulations for cross-border flow of data, the law enforcement and judicial situation of personal data protection, etc.; second, whether there is a special agency responsible for data protection law enforcement; the third is the multilateral and bilateral treaties about protection of personal data.

This assessment is too abstract and subjective, and even involves political considerations, implementing strict legal regulations, but this approach is likely to have negative impacts on the Internet economy and international trade, and even become one of the important factors that make it difficult for the EU to have leading Internet companies.

3.2 Completely open cross-border data transfer represented by the United States

The United States has built a logical, complete and multi-level sovereign data guarantee system, allowing the free flow of foreign data but restricting the outbound transfer of domestic data. Mainly through export control, foreign investment security review, controlled non-confidential information management and other means, the United States ensures that important domestic data is not outbound transferred. In addition, the CBPR and Clarify Lawful Overseas Use of Data Act (CLOUD Act) are combined for reference to establish the "Global Data Controller Standard" to achieve extended jurisdiction over global data.

In terms of data outbound transfer, the United States strictly restricts the export of data in key technologies and specific fields, such as the Export Administration Regulations (EAR), which require the export license from the Security Agency if the regulated technology and data need to be transferred to servers located outside the United States.

At the same time, the "long-arm jurisdiction" breaks the "server standard" to allow access to data from telecommunications services or computer services that are not in the United States, expanding the right of U.S. law enforcement agencies to get overseas data, and other countries must pass the review of qualified foreign governments in the United States to access data in the United States.

Although based on data openness, governments and businesses can carry out public management and business activities through flowing data to achieve higher efficiency and profitability and promote economic growth. However, completely open cross-border data transfers may lead to disputes over data sovereignty, while personal information leakage can cause distress to personal lives and trigger a crisis of trust in public administration.

3.3 Absolute prohibition of cross-border data transfer represented by Russia

As mentioned above, some developing countries, because of their national interests, prevent data from being used by other countries, and have taken measures to restrict the flow of data, extending national sovereignty to data, and putting the iron curtain of data between national borders, that is, a country is entitled to the highest exclusive right to its own data, that is, the supreme power of the country to independently occupy, process and manage its own data and exclude the intervention of other countries and other organizations.

This approach is led by Russia. Article 12, paragraph 2, of The Personal Data Protection Bill adopted by Russia in 2006 stipulates that Russian authorities can prohibit or further restrict the data transfer on the grounds of national security, national defense, and protection of the legitimate rights and interests of the public, reflecting Russia's emphasis on the national security of data flows. Law on Data Localization passed at the end of 2014 requires all data controllers who collect personal data of Russian citizens to set up their servers in Russia so that the principle of data localization is established. Although the law does not directly restrict cross-border data professionals, it reflects more directly considerations on national sovereignty and national security similar to the EU's adequacy decision.

3.4 Integration and cooperation of cross-border data transfers: bilateral agreements

As mentioned above, countries have different attitudes towards the cross-border flow of data, but given the increasing value of data and the need for international exchanges, countries often communicate and coordinate through bilateral or multilateral agreements. Typical examples include the US-led USMCA Digital Trade Chapter, the EU-U.S. Privacy Shield Agreement and Safe Harbor Agreement between the United States and the European Union, and the APEC Privacy Framework developed by APEC.

Taking Europe and the United States as examples, the United States has determined that the collection and processing of personal data is lawful without causing harm to the data subject and except for the situations expressly prohibited by U.S. law, while the EU prohibits the processing of personal data in principle, unless there is a clear legal basis. It was this huge disagreement that led to the backlash in the United States when Europe enacted GDPR. However, huge commercial interests in the United States and the European Union have prompted them to explore more viable models for cross-border data transfers, and Safe Harbor Agreement and Privacy Shield Agreement are the product of the search for consensus between Europe and the United States. This model of bilateral or multilateral agreement points out the direction for the international coordination of cross-border data transmission in the future, and can undoubtedly provide inspiration for China's legislative rules.

4. Establishment of regulations on cross-border data flow in China

4.1 Factors to be considered in the establishment of regulations

4.1.1 Combined with traditional Chinese culture

China's personal information protection legislation is deeply influenced by the EU's General Data Protection Regulation (GDPR), and the requirements for personal information protection are quite high, but it is also in line with Chinese characteristics. All aspects of Chinese society are deeply influenced by traditional Confucian culture, and people are more inclined to use morality rather than law to judge social hot issues. Law is only the minimum standard of morality, and the public's standards for others are often higher than those of enterprises. This tendency is very different from Western values, so China often presents a value trade-off orientation of “collective vs individual” at the legislative level.

Under such a value orientation, China's individual rights are often transferred to social interests, which hinders the realization of personal information protection and also brings uncertainty to the privacy protection work of enterprises. Taking epidemic prevention and control as an example,

ordinary citizens have given maximum concessions in terms of personal information and personal privacy, and through the health codes, they can know all the itinerary of individuals and all the people they contact; Sensitive information such as family member information and health information are uploaded on school and enterprise check-ins, and personal privacy rights are transferred faced with the big picture to achieve collective epidemic prevention. At the level of corporate privacy protection, enterprises not only need to take legal compliance as the yardstick, but also need to meet the public's moral standards, which are more complicate due to people's information asymmetry and cognitive limitations, which is more uncertain than the law.

Although Western humanistic values are more consistent with the protection of personal information rights and personal privacy rights, under China's national conditions, cross-border data transmission needs to consider the balance between national interests, public interests, corporate interests and individual interests.

4.1.2 Combined with China's industrial development

As mentioned above, different countries have different levels of digital economy development, national interests and cultural traditions will lead to different attitudes towards cross-border data flow. Countries such as the United States, which has advantages in the development of the digital economy, are more inclined to advocate the free flow of data, while developing countries and less developed countries pay more attention to the development of digital infrastructure and promote the development of their digital industries through localized data storage.

From the perspective of China's industrial development, Alibaba, Tencent, Huawei and other leading Internet companies have formed leading advantages in cross-border e-commerce, cross-border payment, information services and other aspects. However, according to McKinsey estimates, although the scale of China's digital economy has reached the second largest in the world, the broadband data flow only ranks eighth in the country, only 20% of the United States, and the scale of China's data flow is too small. The cross-border flow of data has become the focus of the further development of China's digital economy, and China should accelerate the legal construction of cross-border data flow, promote cross-border data flow and provide institutional guarantees on the basis of ensuring national interests and personal data security.

4.2 Specific rules for cross-border data flows

4.2.1 Establish a hierarchical and categorical data supervision system

Although Article 37 of People's Republic of China Network Security Law requires the establishment of a cross-border data flow assessment system, there are currently many norms and standards for data classification and grading in China, and different authorities, industries or market entities have issued different norms and standards. Different industries have different data grading standards such as Financial Data Security-Guides of Data Security Classification for the financial industry and Guides of Industrial Data Classification for the industry. At the same time, different provinces and cities have different data grading standards such as Digital Reform-Guides of Public Data Classification in 2021 for Zhejiang and Guides of Public Data Classification for Shanghai in 2019. To a certain extent, various standards adapt to local conditions consider the influencing factors such as region, industry, and business nature, and meet their own management needs. However, it still causes the objective phenomenon of different data standards and hinders the cross-border flow of data.

As far as cross-border data flow is concerned, the author thinks that it should establish a unified national classification and grading standard, and should distinguish personal data, commercial data and special industry data in the standard. In terms of classification, data should be divided into five levels according to sensitivity, and cross-border restrictions of data should be determined according to the comprehensive consideration of classification and grading. For example, commercial data with level 0 sensitivity can be outbound transferred unconditionally, special industry data is not allowed to be transferred regardless of the level of sensitivity, and personal data with level 3 sensitivity can

be conditionally transferred with ensuring the security of personal data. This both keeps data secure and facilitates its flow.

4.2.2 Diversify legal flow channels

From China's current practice, the outbound transmission of specific industry data and personal data involving national interests and public interests is absolutely prohibited, and other personal data and commercial data are set up with relatively strict permit regulatory procedures before export, including “notification and consent”, security self-assessment, and industry authority assessment. Although this measure strengthens the security of China’s data, it also restricts the reasonable flow of data and reduces benefits. At the same time, the permission procedure treats different things alike, bringing ineffective practice and increasing the administrative burden.

China can learn from the Safe Harbor Agreement and Privacy Shield Agreement of the United States and Europe to sign bilateral or multilateral agreements with other countries to facilitate data flow; EU’s GDPR can also afford us lessons to set up a whitelist to reduce the frequency of review of data outbound flows, and at the same time determine adequate security measures. If data controllers and data processors promise to provide adequate data protection measures, data can flow across borders.

Of course, the channels for data flow will go beyond the above types as practice develops, and flexible and diverse measures should be taken to cope with the needs of cross-border data flow.

4.2.3 Improve the risk management system of relevant entities in the process of data outbound transfer

China should set up special agencies at the government level or strengthen coordination between agencies that take charge of cross-border data flow. Measures for Security Assessment for Outbound Personal and Important Data Transfer (Draft) promulgated by China National Internet and Information Office confer the power of information and supervision on the Cyberspace Administration of China, public security departments, security departments, People's Bank of China, the China Banking and Insurance Regulatory Commission, industrial and commercial institutions and other departments with administrative supervision and law enforcement powers. Moreover, the enforcement basis of these regulatory authorities is different, so there will be repeated punishment or no punishment, which reflects the insufficiency of information sharing and coordination between different departments. The most effective measure is to establish a professional regulatory authority, which can speed up and intensify the censorship of cross-border data flows. However, considering that China is still in the preliminary exploration stage in the field of cross-border data flow, the foundation for establishing professional regulatory authorities is still insufficient, so strengthening the collaboration between departments is more in line with China's current national conditions. The collaboration suggestions are as follows: First, the punishment information of various departments for enterprises needs to be exchanged in time to avoid repeated penalties and omissions of penalties for non-compliant enterprises. Secondly, each department divides its own scope and content of supervision, coordinates supervision, and avoids prevarication when encountering problems. Finally, they should collaborate to develop compliance standards and plans for cross-border data flows and then facilitate the realization of compliance plans.

Acknowledgements

Funded by the National College Student Innovation and Entrepreneurship Training Program (Project No.: 202213021044).

References

[1] Wang Liming, Research on Major and Difficult Issues in Personality Rights, Law Publishing House,711(2019); Shen Weixing, On the Right to Usufruct of Data, Social Sciences in China, No. 11, 2020, 113(2020).

[2] Wang Yegang, An Outline of the Relationship between Enterprise Data Rights and Personal Information Protection[J], Comparative Law Research,2022(04):33-44.

[3] Zhang Jinping, International Regulation of Cross-border Data Transfer and Response of Chinese Law: A Review of Cross-border Data Transfer Restriction in China's Cybersecurity Law[J], Politics and Law, 2016(12):136-154.

[4] Cao Bo, Legislative Models and Improvement Path of Cross-border Data Transfer: Based on Article 37 of the Cybersecurity Law[J]. Journal of Southwest University for Nationalities (Humanities and Social Sciences Edition),2018,39(09):94-100.

[5] Huang Xianqing. The Construction Path of China's Cross-Border Data Flow Regulation under the Background of Digital Trade[J], Southwest Finance,2021(08):74-84.

[6] Chen Si, Ma Qijia, China's Path to Regulatory Coordination of Cross-border Data Flow[J], China Circulation Economy,2022,36(09):116-126.

[7] Wang Liming, Research on Major and Difficult Issues in Personality Rights, Law Publishing House,711(2019); Shen Weixing, On the Right to Usufruct of Data, Social Sciences in China, No. 11, 2020, 113(2020).

[8] Hui Zhibin, Zhang Heng, Research on Cross-border Data Flow Management for Data Economy, Social Sciences, No. 8(2016).

[9] Zhu Caihua, Reconstruction of Market, National and International Economic and Trade Rule System, Foreign Affairs Review (Journal of Foreign Affairs University), No. 5, 2019.

[10] John Carlo Bertot, Policy Framework for Big Data and Open Data: Issues, Politics Policies and suggestions[J]. Zheng Lei, XU Huina, Bao Linda. E-Government, 2014(1) .