Proceedings of ICGPSH 2024 Workshop: Industry 5 and Society 5 – A Study from The Global Politics and Socio-Humanity Perspective
DOI: 10.54254/2753-7048/71/2025.LC18067

Study on the Regulatory Model of Cross-border Flows of Personal Data: China's Perspective

Qiqi Wang[1,a,*]

[1]*School of Politics and Law, Chongqing College of Humanities, Science & Technology, Caojie Street, Chongqing, China*
a. wangq@ldy.edu.rs
**corresponding author*

Abstract: Personal data has become a crucial component of today's digital economy and trade. In recent years, nations have been proactively investigating the problem of cross-border data flows from a global viewpoint. China has gradually introduced relevant laws and regulations, including the Network Security Law of the PRC and the Personal Information Security Law of the PRC to protect personal information, among which are avenues for resolution that deal with the safeguarding of private information. Despite the internal circumstances in China, it is important to further explore the top-level design system and practical research in this area. This paper uses the literature research method and comparative research method as its main research methods, in accordance with the current views of relevant scholars both domestically and abroad, presents the US and Europe's effective implementation of legislative regulations to control data flow in China, and researches the specific practical issues of the Chinese legal framework governing the transfer of personal data across borders, to help guide how to regulate transnational personal data issues in China.

Keywords: Personal Data, Cross-Border Flows, Regulatory Model, Chinese Perspective.

1. Introduction

On July 21, 2022 China's National Internet Information Office (NIIO) decided on administrative penalties related to cybersecurity review against DDT Global Corporation (from now on referred to as DDT) in accordance with the law, fined DDT Global Corporation 8.026 billion yuan (RMB, same as below), and a fine of RMB 1 million yuan (RMB) each on Cheng Wei, Chairman and CEO, and Liu Qing, President, of DDT Global Corporation [1]. DDT is penalized for cross-border processing of national and personal information arbitrarily, as per the decision. This has had a significant negative impact on national security and the privacy of personal information of citizens. Regarding advancing new artificial intelligence technologies, the development of network data is more prosperous, and the problems posed by data flows across borders are infinite, at the same time, people are gradually paying attention to this field, the academic community has begun to address the issue of personal data flowing across borders. From a personal perspective, the issue impacts the security of personal privacy data, such as personal identifying, home address, and a series of information leaks that can be easily utilized by others to cause damage to the objectives of the person in question. In addition, the movement of personal data across borders, leading to the leakage of personal information, may to some extent hamper the emergence of the digital economy, thereby affecting the

DOI: 10.54254/2753-7048/71/2025.LC18067

economic ties between individual countries and becoming a stumbling block to the process of globalization of the world economy. In this way, how to emphasize the issue of cross-border protection of personal data in legal regulation has become a very important topic.

2. Concepts Related to Personal Data

Different voices have emerged on the understanding of the definition in different countries.The focus of this section is on comprehending the definitions associated with the transfer of transnational personal data, as well as analyzing the need for the development of this field in modern society.

2.1. Historical Evolution of the Definition of Personal Details

The earliest definition of personal data originated in the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data ("1980 Guidelines") issued by the Organization for Economic Co-operation and Development (OECD) in 1980, which set out a definition of personal data as as "any information relating to an identifiable or identified subject of personal data" [2]. The primary focus is on identifying personal data that pertains to the subject, The General Data Protection Regulation (GDPR) is based on the European Union and has Article 4(1), defines "personal data" as "all information relating to an identified or identifiable natural person, including location data, name, online identifier, identification number or any data relating to the physical, genetic, bodily, psychological, cultural, social or economic identity of that natural person [3]." The GDPR defines the term "personal data" with detailed explanations and examples. China's broader definition is the Information Security Technology Personal Information Security Specification (which is also known as the "Security Specification"), which came into effect in 2020 [4]. The specific meaning of "data export", i.e., the process of "transferring personal information collected and generated in the course of operations in the People's Republic of China", is explained in the Information Security Technical Data Outbound Security Assessment Guidelines (Draft for Public Comments) (hereinafter referred to as the "Assessment Guidelines"), data outbound is divided into three categories in a more detailed manner, including: (1) Providing personal information to a subject that is in China's territory but does not fall under China's jurisdiction or is not registered in China's territory. (2) Personal data is still on Chinese territory, but has access to an institution, an organisation, or an person outside of China. (3) The network operator transmits out of China internal data of the group or personal information collected or generated during the operation in China [5]. China's definition of it is more logical than those in both international and GDPR definitions, and the requirements for outbound data from abroad tend to be more in the direction of localization, rather than the U.S. "anti-localization" legal regulation model.

Driven by the background of global economic development, all countries attach great importance to its legal regulation and make adjustments in accordance with their own national conditions, and in a variety of regulation modes, China's legal regulation has become a major problem in protecting the flow of privacy in China.

2.2. The Need to Protect the Exchange of Personal Data between Countries

Data has become an indispensable part of human life, from 2016 to 2018, the number of cases of telecommunications fraud in China was 44.5 million, 50.4 million, and 597,000, and the amount of fraud was more than 16 billion yuan, more than 18.6 billion yuan, more than 23.5 billion yuan, the fact that telecommunications fraud is generally conducted across borders has led citizens to focus on the issue of securing the safety of personal data across borders [6]. The quality of personal information protection can be further enhanced by improving the rules model for cross-border data protection for individuals, reduce the risk of data leakage faced by nationals when surfing the Internet, and major

DOI: 10.54254/2753-7048/71/2025.LC18067

Internet firms such as Amazon, Google, Meta, and others., have all need a large amount of user information data circulation. This is an indication that the current problem is the reduction of the likelihood of illegal data acquisition in the circulation procedure.To enhance China's international discourse and improve its international competitiveness, it is important to gradually improve and strengthen China's model development in this field.

3. Analysis of the Actual Situation and Problems in the Development of Regulatory Models for International Flows of Personal Data in China

China's legal regulation of cross-border data flow was not initiated until later, and at the same time there are problems of unclear definition of legal regulation and lack of implementation in practice, the evolution of China's regulatory model in this field has been examined in this section to analyze its current status and problems.

3.1. Current Status of Development of Regulatory Models for Cross-Border Flows of Personal Data in China

The Personal Information Protection Law 2021 and the Cybersecurity Law 2017 are two of China's legal regulations that deal with cross-border data flow of individuals, and the relevant supporting rules under the Cybersecurity Law mainly include the Measures for Security Assessment of Personal Information and Important Data Outbound and the Measures for the Assessment of Personal Information, etc., while the two laws share the common supporting rules of the Measures for the Security Assessment of Data Outbound, and The Personal Information Protection Law does not have its own supporting rules for the time being. Article 38 of the Personal Information Protection Law stipulates that a processor of personal information needs to have one of four conditions when providing personal information to foreign countries to enable the cross-border flow of personal data, namely: (1) Completing the security assessment conducted by the national net information department in accordance with the law. (2) Receiving certification from a professional organization for personal information protection in accordance with the National Net Information Department regulations. (3) Being certified by a professional organization for the protection of personal information by the provisions of the National Net Information department. (4) Entering into a contract with the overseas recipient by the standard contract formulated by the state net information department, agreeing on the rights and obligations of both parties. (5) The State Net Information Department stipulates other conditions. The standard contract shall be based on the following conditions: The safety assessment mechanism, the certification mechanism for privacy of personal information, and the standard contract rules [7]. Meanwhile, Article 40 of the Personal Information Protection Law provides a more detailed description and explanation of the security assessment mechanism. Supporting rules are relevant supplements to specific laws for better utility in practice, such as the scope of application of the rule model, which distinguishes between offshore and onshore data flows [7]. And defines different data [7]. The Cybersecurity Law and its supporting rules are security assessment mechanisms that tend to be localized rules, mainly targeting enterprises that hold a large amount of user information and go abroad to list, and when such enterprises circulate their data outside of the country, they need to carry out a strict security assessment before they can do so, to prevent some enterprises from attempting to illegally disclose personal data or even national security data through unlawful means, which may cause damage to the interests of individuals and the State. This prevents some enterprises from attempting to illegally leak personal data or even national security data through illegal means, thereby causing damage to individuals and national interests. China has also made corresponding regulations on some special areas, for example, the Export Control Act and its supporting rules stipulate that export control requirements apply to data

DOI: 10.54254/2753-7048/71/2025.LC18067

on military products, nuclear, missiles, chemicals, technology, and related services [8]. At the same time, in 2021, China successively applied for accession to the Comprehensive and Progressive Trans-Pacific Partnership Agreement (hereinafter referred to as CPTPP) and the Digital Economy Partnership Agreement (hereinafter referred to as DEPA), the process of convergence between cross-border flow of personal data boards and international platforms will be progressively promoted.

3.2. Analysis of Issues in the Regulatory Model of the Flow of Personal Data Across Borders in China

3.2.1. The Establishment of Special Supervisory Authorities

Both the Personal Information Protection Law and Network Security Law have overlapped specific content, and in the early stages of the two laws conflict with the legislative purpose, and in different classes of laws and regulations overlap, the same class of legal documents overlap, the supporting relationship between the upper and lower classes of the law has a cross-cutting relationship, which will lead to conflict in the application of the law in practice by the legal workers easily [9]. In terms of data processing, a large enterprise will be involved in different areas of data processing, when dealing with multiple data types, enterprises often look for time-saving and fast ways to reduce cost consumption or use the user's personal information data to obtain illegal benefits, so the top-level design of the regulatory model should be resolved to address the issue of data categorization and conflict of laws. At the same time, the regulatory system should be strengthened by setting up a specialized regulatory authority to supervise enterprises in carrying out proper cross-border processing of personal data, to reduce the illegal use of personal data.

3.2.2. Low International Participation

China's personal data cross-border legal model of development compared to Europe and the United States or other countries started late, in the overall top-level design and regulatory system has not yet formed a complete model, in the processing of data with other countries or enterprises in the negotiation is at a disadvantage, and now looking for effective protection of the personal information of our nationals is the most important issue, to enhance China's discourse and competitiveness on the way. The following are some of the key issues that we are looking for. At the same time, due to the different basic national conditions of each country, the regulatory model set up by them is also completely different, or even diametrically opposite, so in the field of international cooperation, China's regulatory model in line with international standards, we should also focus on cooperation with other countries, and to take an active part in the formulation of international rules for the cross-border flow of personal data, and at the same time can be bilateral agreements with other countries, and strive to develop the cross-border flow of personal data to suit the situation of China's national regulatory system. Flow regulatory system suitable for China's national conditions.

4. The Regulatory Patterns of Cross-Border Data Flows of Individuals in Europe and the United States

This section explores the merits of the legal regulation of cross-border flow of personal data in the European Union and the United States by researching and analyzing their legal regulation, with a view to providing lessons for the development of regulation in China.

4.1. EU Regulatory System for Cross-Border Flows of Personal Data

Based on its own historical and cultural traditions and the status quo of Internet development, the EU has implemented a legal regulatory system for cross-border data of individuals based on “adequacy

DOI: 10.54254/2753-7048/71/2025.LC18067

determination", and at the domestic law level, it has clarified multiple paths of cross-border flow in the EU, including: (1) Determination of the level of adequacy protection. (2) Standard contractual clauses. (3) Binding rules for companies. (4) Cases of derogation, derogation situations, improving the data classification and grading system, and promoting the free flow of data under the premise of maintaining data security. The security assessment mechanism involved in China's current Cybersecurity Law is similar to the European Union's requirements for restricting the flow of corporate data, but in practice, it is unable to effectively protect personal information at the source due to the diversity of data and other objective factors. In the international context, the EU actively carries out multilateral cooperation mechanisms for the cross-border flow of personal data, and Chapter V of the GDPR emphasizes the importance of international cooperation. In practice, the EU and APEC have set up a joint working group to explore the mutual recognition and docking issues of the APEC Cross-Border Privacy Rules System (hereinafter referred to as the "CBPR System") and the two types of rules of the BCR. In practice, the EU and APEC have set up a joint working group to explore the mutual recognition and interface between the APEC Cross-Border Privacy Rules ("CBPR") and BCR. In addition, the EU also actively participates in the Budapest Convention and other international law enforcement mutual assistance conventions to ensure the effective implementation of GDPR-related mechanisms in the international arena, and China needs to actively participate in multi-level international rule-making and sign bilateral agreements with other countries to enhance China's right to speak in the field of cross-border personal data [10].

4.2. Regulatory System for Cross-Border Flows of Personal Data in the United States

The United States, as a recipient of personal data from multiple countries, has implemented anti-localization legislation externally while strengthening domestic institutions. From the lightning-speed repeal of the Consumer Data Bill of Rights by the Trump administration in 2015 to the U.S. Senate making a proposal for a Privacy Bill of Rights in April 2019 [11]. The U.S. government has gradually increased its focus on domestic legislation and regulation. Combined with the regional local character of U.S. state legislation, in 2021, the U.S. Uniform Law Commission voted to adopt the Uniform Personal Data Protection Act, Accelerating the harmonization of personal data protection rules across states [12]. In its 2018 signing of the Clarification of Lawful Use of Data Abroad Act (hereinafter referred to as the "Cloud Act"), the real intention of the Act is for the U.S. government to use large U.S. Internet companies as a means to access personal data lawfully localized in other countries and at the same time, to establish the APEC privacy framework as the leading CBPR system, which is committed to promoting loose and free rules for the cross-border flow of personal data, and which relies more on the self-regulatory behavior of enterprises to safeguard the security of personal data. In addition, the U.S. has actively pursued a bilateral agreement strategy with non-APEC members [13]. China's Internet enterprises are also an important part of the international Internet enterprises, but China's enterprises have a basic characteristic, its enterprise self-discipline is not strong, so the legal system is restricted and requirements, at the same time, China can also be committed to the establishment of the relevant data system to enhance China's right to speak in this field.

5. Specific Measures to Regulate Transborder Personal Data Flows in China

In order to provide substantive advice on the development of this area in China, this section draws on the development of regulatory models in Europe and the US, taking into account China's national context.

DOI: 10.54254/2753-7048/71/2025.LC18067

5.1. Improvement of the supporting norms of the Personal Information Protection Law

Starting from the rule of law in domestic law, to improve the effectiveness and practicability of domestic legal regulation and reduce the lag of lawmaking in the international arena, the overlapping contents and contradictory parts of the Personal Information Protection Law and the Cybersecurity Law should be effectively integrated and deleted, and some of the rules of the Measures for the Assessment of the Security of Data Exit should be separated, to improve the top-level design of the law in this area, to subsequently classify and regulate the different data types and to enhance sustainability and legality of personal data processing and flow. Classify and manage different types of data to improve the sustainability and legality of the processing and flow of personal data. Improve the supporting rules of the Personal Information Protection Law and establish a system of rules on the cross-border flow of personal data between companies within multinational corporations and specific enterprises, drawing on the BCR rules and CBPR rules of the European Union to an appropriate extent [8]. Reform of the system from within enterprises to help them improve self-regulation, and data refinement and classification from within enterprises. Aligning domestic law with public international law will provide a solid foundation for future international cooperation.

5.2. Establishment of Specialized Regulatory Authorities

The United States has referred in the Privacy Shield Agreement to the establishment of a commissioner to effectively regulate and scrutinize the EU-US flows of crossborder personal data. The country is currently supervised by the Internet Information Office, public prosecutors law enforcement departments, and industry regulators to supervise enterprise data processing, however, because of China's many small and medium, the rapid development of e-commerce, the main body of the data processing is decentralized and the number is huge, this paper believes that our country should set up a special data regulator to effectively regulate the data processors. At the same time, it can stop the behavior of obtaining personal privacy data from abroad through illegal ways, and the supervisory departments can regulate and supervise the behavior of enterprises from the source, forming an effective organization system led by special supervisory departments, cooperated by industry supervisory departments and supervised by public prosecutors and law enforcement departments, and at the same time, it is in line with the international rules to improve the mode of China's regulation in this field.

5.3. Participate in Developing and Actively Contribute to the Development of International Rules on the Transborder Flow of Relevant Personal Data

The RCEP, whose chapter on e-commerce regulates the cross-border transfer of information by electronic means and to which China has signed up, has now formally entered into force, requiring all parties to respect the legal requirements of other countries and not to obstruct the transfer of data across borders for economic purposes [14]. This provision reduces to a certain extent the conflict of mode regulation in the process of cross-border processing of personal data in the course of practice, but China's cooperation and development with the international and this field is still insufficient, actively promote China's accession to the CPTPP and DEPA to expand the scope of transborder flows of personal data in our country, and at the same time, China can also be based on the "One Belt, One Road" political ties. Simultaneously, China can also use the "Belt and Road" political bond as the basis to establish a cooperation system led by our country based on the unique national conditions of the regulatory model and create regional treaties or bilateral agreements to provide a systematic basis and combine the strengths of developing countries. for China's future economic development and international economic and trade cooperation.

DOI: 10.54254/2753-7048/71/2025.LC18067

6. Conclusion

The transnational movement of individual data within China serves as a catalyst for economic growth, furthermore, it presents a significant risk to the safeguarding of Personally Identifiable Information (PII), the primary challenge in regulating the flow of personal data across China's borders is the absence of a robust domestic regulatory framework governing the international transfer of data pertaining to individuals and the limited level of international participation in these regulations. Therefore, to strengthen the cross-border protection of personal data, this paper conducts an in-depth analysis of the regulatory model of the cross-border flow of personal data from China's perspective. It would be prudent for China to proactively address the issue of internal conflict within its domestic regulatory model, improve the supporting rules of the Personal Information Protection Law, and set up a sound system of data classification system, to improve the efficiency and legitimacy of the cross-border flow of personal data; on the other hand, it should sign a bilateral coordinating. It has also actively participated in the development of international rules on cross-border flows of personal data by signing bilateral agreements with other countries on coordination mechanisms. Only by continuously improving the establishment of the domestic regulatory system and keeping pace with international development can the level of privacy of personal information be effectively enhanced.

References

[1] *CNN. (2024) The Cyberspace Administration of China imposed a fine of 8.026 billion yuan on Didi. Retrieved from https://www.chinanews.com.cn/cj/2022/07-21/9808616.shtml.*
[2] *The 1980 Guide, Article 1, Paragraph 2.*
[3] *Directive (EU) 2016/680, OJ 2016 L 119/89.*
[4] *Safety Code (GB/T 35273-2020) 9.8.*
[5] *Safety acceptance assessment guide 3.7.*
[6] *Chaoxin Wen. (2024) Characteristics and Countermeasures of Telecommunication Fraud Crime in the Background of Big Data. Legal Expo, 18, 7-10.*
[7] *Personal Information Protection Act, Article 3, Article 28, Article 38.*
[8] *Jiayun Shi. (2022) Research on Legal Regulation of Cross-border Flow of Personal Data. Central University of Finance and Economics.*
[9] *Yiza Xue. (2020) The Construction of Multi-Level Data Exit System and the Realization of the Freedom of Data Flow: Taking the Change of Substantive Censorship as the Starting Point. Journal of Northwest University for Nationalities (Philosophy and Social Science Edition), 6, 64-74.*
[10] *Tian Wang. (2023) EU experience and China's reference on legal regulation of cross-border flow of personal data. Hebei University.*
[11] *U.S. Privacy Bill of Rights, Section 3.*
[12] *Security Insider. (2024) U.S. Passes Uniform Personal Data Protection Act (UPDPA). Retrieved from https://www.secrss.com/articles/33092.*
[13] *The White House.(1997) The Framework for Global Electronic Commerce. Retrieved from https://clintonwhitehouse4.archives.gov/WH/Ne w/Commerce/ index.html.*
[14] *Regional Comprehensive Economic Partnership, Article 15.*