Proceedings of the 3rd International Conference on Literature, Language, and Culture Development
DOI: 10.54254/2753-7064/37/20240178

Legal Regulation of Transnational Data Flows: International Experience and Chinese Solutions

Xuezhu Zhao[1,a,*]

[1]*School of Civil and Commercial Law, Southwest University of Political Science and Law, Bao Sheng Avenue, Chongqing, China*
a. 202004033139@stu.sdp.edu.cn
**corresponding author*

Abstract: The arrival of the big data era has made most countries realize the importance of data resources for economic development. On the one hand, data flow promotes trade between countries, and on the other hand, the rapid expansion of the scale of multinational business giants has led to a proliferation of incidents of illegal collection and utilization of user privacy, putting national security at risk.In 2019, WTO members of the e-commerce negotiations put forward proposals for cross-border data flow based on their own positions, and major countries such as China, the United States, Russia and other major countries have all put forward different proposals.It can be seen that data flow regulation has become a key topic in the international arena nowadays, with sufficient necessity and practical significance. As a result, this paper adopts the comparative analysis method, normative analysis method and other research methods to analyze the issue and make suggestions on the direction of China's legislation.

Keywords: Data flow, Personal privacy, Public security, Cross-border supervision

1. Introduction

Today's society has stepped into the information age, the rapid development of the field of electronic science and technology, in the international market has a significant position. Information is an important resource, which is not only conducive to the development of enterprises, but also closely related to the trade security of the country. Under the trend of economic globalization, data, as a form of information, has received more and more attention from multinational institutions. However, it is precisely because of the urgent need for data resources in many countries that risks such as the leakage of personal information continue to occur, challenging citizens' right to privacy. The leakage of large amounts of information can pose a threat to national privacy and security, and therefore, as the subject of the data, the state should protect itself through legislation.

Currently, most countries have formulated corresponding domestic laws based on different cultural and political backgrounds, such as China's Data Security Law and Russia's Personal Data Law of the Russian Federation. In addition, some international organizations have achieved the undertaking of data regulation among different countries in a certain region by formulating organizational charters to constrain the data flow behavior of member countries (e.g., the EU's General Data Protection Regulation). From the entity level, the current regulatory mechanisms in this area include bilateral, multilateral and regional trade [1]. These rules are committed to removing unreasonable restrictions

DOI: 10.54254/2753-7064/37/20240178

on cross-border data flows through different ways, and at the same time, they maintain individual privacy and national security. Therefore, by summarizing the existing regimes among different countries and international organizations, the author analyzes the shortcomings in the field of data regulation in China and proposes improvement measures conducive to the protection of data security.

2. Principles for International Regulation of Transnational Data Flows

2.1. The Principle of Proportionality

The principle of proportionality usually refers to the use of means that cause the least harm in achieving a legitimate aim. In the concept of data flow, it emphasizes more on the balance and constraints between individual and public interests. The flow of cross-border data has facilitated the development of digital trade, in which many countries participate, legally exchanging information through electronic platforms and reaching a pattern of data sharing by mutual agreement. Once such sharing is constrained, digital trade based on data flows will not be possible. However, personal privacy and data exchange have always been contradictory concepts, and the privacy and security of citizens cannot be guaranteed without restricting excessive data flows. Therefore, when weighing the two, the State should adopt the principle of proportionality and take into account the interests of both sides.

In safeguarding data sovereignty, countries often cite "national data security concerns" and "privacy protection" as reasons for restricting flows, which involves the issue of political sovereignty [2]. Countries involved in cross-border data flows include not only developed countries but also developing countries, and the former are in a better position to safeguard their own data security because of their advantages in science and technology, business and other fields. Therefore, enhancing the privacy status of developing countries in data exchange is another manifestation of the principle of proportionality.

2.2. The Principle of Public Interest Protection

As an independent international subject, the State should prioritize the protection of its independent status on the basis of domestic public security before participating in international exchanges. Currently, domestic laws mostly adopt categorized regulation to provide additional protection for special kinds of data and restrict their flow to avoid threats to public interests. In essence, transnational data flow is a combination of market operation and administration, covering both the public and private spheres of power. As a result, some norms have established public policy saving clauses that seek to balance the rights and obligations of both the free flow of international data and domestic data regulation. That is to say, States parties need to bind the data in question for legitimate public policy purposes before they can engage in the flow of data.

2.3. The Principle of Personal Privacy Protection

Different types of data have different risk values, and one of the most important categories is personal privacy data. Europe was the first international region to protect the right to privacy through the enactment of national laws, but early data protection tended to be unilateral, i.e., the legislation centered on restraining the international flow of data involving personal privacy, rather than on protecting against infringement of those data already in circulation. These provisions were ex ante preventive and lacked avenues for ex post relief.

Compared with other subjects, the subjects of personal data are in a weak position, and most cases of data leakage occur when the subjects are not aware of it, so it is very difficult for the State to realize the protection mechanism effectively in the cross-border process. The economic value of personal

DOI: 10.54254/2753-7064/37/20240178

information determines that cross-border data flow mechanisms should minimize and eliminate legal obstacles to the free flow of personal information, thus avoiding the use of the pretext of defending rights by governments to hinder the progress of free trade [3]. In addition, information is a complex concept that encompasses the dual characteristics of property rights and personal rights, which reflects the main legal value of judicial supervision: the remedy and protection of personal data rights and interests.

2.4. The Principle of Trade Liberalization

The advancement of the internet has transformed the traditional model of financial development, and as the internet world has been updated, concepts such as blockchain, big data and artificial intelligence have been born, leading to a number of new ways of trading (e.g., online payments, e-banking). These new trading modes are all based on cross-border data flows. With the emergence of trade agreements, the promotion of trade globalization has gradually become the main direction of development, and as the main form of trade, the progress in the field of e-commerce is conducive to promoting the diversification and liberalization of trade. At the same time, in the face of cross-border data flow, countries lack uniform standards, and this unstable competitive relationship may lead to fluctuations in the international trade market. Therefore, the establishment of a comprehensive regulatory system for cross-border data flows is crucial to the future and destiny of every country.

3. Status of Legal Regulation of Transnational Data Flows

3.1. Legal Regulation of Transnational Data Flows within China

In recent years, data security has been a key topic in China's national governance and a major focus of legislation in the digital field. China's legislation on cross-border data flows can be roughly divided into three stages: the stage of decentralized legislation, the stage of standardized legislation and the stage of refined legislation [4]. Initially, provisions on cross-border data flows were mainly presented in the form of administrative regulations or departmental rules, which were less effective compared to laws, and the content was mostly limited to the financial and health fields. At this stage, legislators did not pay attention to the importance and risks of personal data and did not make systematic provisions for them, and the legal framework for cybersecurity had not yet been established.

Since the enactment of the Cybersecurity Law in 2016, China's cross-border data flow legislation has officially entered its second phase. Shortly afterward, China enacted the Personal Information Protection Law and the Data Security Law, establishing a comprehensive cybersecurity governance system and a regulatory system for data transmission overseas. Since then, China has basically formed a regulatory structure centered on these three laws.

Table 1: Summary table of three important Chinese laws

Laws or regulations	Date of adoption	Outline
Cybersecurity Law of the People's Republic of China	November 7, 2016	1.Network Operational Security 2.Network Information Security 3.Monitoring, early warning and emergency response

DOI: 10.54254/2753-7064/37/20240178

Table 1: (continued)

Data Security Law of the People's Republic of China	June 10, 2021	1.Data security system 2.Data security protection obligations 3.Government data security and openness
Personal Information Protection Law of the People's Republic of China	August 20, 2021	1.Rules for handling sensitive personal information 2.Rules for cross-border provision of personal information 3.Special provisions for the handling of personal information by State organs 4.Rights of individuals in relation to personal information processing activities 5.Obligations of personal information processors

Taking "important data" and "personal information" as their entry points, these three laws differ markedly in their regulatory objectives, scope of application, and means of regulation, forming a "parallel dual-track system" that safeguards the security of the control of the transmission of nationally important data overseas while taking into account the protection of personal privacy [5]. The Cybersecurity Law gave birth to the concept of data sovereignty, which is the right of the state to manage and control data and its related technologies and devices. As an extension of state sovereignty in the data domain, the law primarily adopts the principle of territorial jurisdiction and introduces the concept of "critical information infrastructure" [6]. For the first time, the Data Security Law introduced the "principle of free flow of data security" and proposed the establishment of a hierarchical data protection system, which facilitated data security reviews.

Entering the stage of detailed legislation, the main way in which China's legislation has been implemented is through the introduction of a series of supporting measures for the Cybersecurity Law, which promotes the effective functioning of national data regulation. For example, the Measures on Cross-border Cybersecurity Assessment provide detailed guidance on the assessment that should be conducted when providing important data. In terms of cross-border data flow, China adheres to the concept of "secure flow" and fully draws on extra-territorial experience based on the domestic situation. After years of practice, China's digital economy had developed rapidly, facilitating integration with other international economies.

3.2. Legal Regulation of Transnational Data Flows by Other States and Organizations

3.2.1. USA

The long-arm jurisdiction of the United States not only gives it a high degree of control over data within its borders, but also allows it to effectively access data outside its borders. Such a situation cannot be separated from the dominant position of the United States in the field of data flow. First, as a pioneer of the Internet, the United States possesses a technological advantage that guarantees its

DOI: 10.54254/2753-7064/37/20240178

absolute control over the data medium. Second, as a data power, the United States advocates the free cross-border flow of data on a global scale, but exercises strict territorial jurisdiction over data within the United States [7]. Collecting data in the name of openness not only gains the economic benefits brought by the data, but also enhances the U.S. right to speak on global data. Finally, the United States has not only introduced domestic laws for data management, but also signed relevant treaties with other countries and actively promoted the United States model in the international market.

When it comes to the topic of personal information protection, the United States has been implementing a market-driven, industry self-regulation-centered policy for the protection of personal data flows. Generally speaking, there are two types of industry self-regulation systems: third-party certification organizations and the development of recommended industry self-regulation guidelines. This system has largely made up for the inadequacy of personal data protection legislation. Compared with the national hard law, industry self-regulation is the commitment of market subjects, and personal data protection based on the consensus reached by the subjects can reasonably safeguard the rights and interests of individuals while avoiding the restriction of technological innovations based on the state of industrial development [4].

3.2.2. EU

With regard to transnational data flows, the European Union has adopted a "whitelisting system", which establishes a limited number of white-listed countries for the free flow of economic data across borders through a "sufficiency determination". In practice, the European Commission assesses the following factors: (i) the rule of law and its implementation in the third country or territory with regard to respect for human rights and fundamental freedoms; (ii) the existence and effective functioning of an independent supervisory authority in the third country or territory; and (iii) the third country's participation in, or ratification of, international commitments, conventions, or instruments relating to the protection of personal data. Direct transfers of personal data to countries that have been certified as having a data protection capacity that is considered by Europe to exceed the level of "adequate protection" will be permitted.

In recent years, the legislative focus of the EU has gradually shifted from the harmonization of the internal market to the strengthening of the regulation of businesses across online platforms [3]. The current EU data legislation adds relevant regulations in a number of areas. The weaker protection of individual privacy rights in the new legislation has somewhat enhanced its ability and legitimacy to regulate trade and work towards completing the institutional infrastructure and overall legal framework.

3.3. Legal Regulation of Transnational Data Flows by International Regional Agreements

3.3.1. Legal Regulation of Cross-Border Data Flows in RCEP

RCEP is the largest and most important free trade agreement negotiated in the Asia-Pacific region, which, when concluded, will cover nearly half of the world's population and nearly one third of its trade volume, making it the world's most populous, diversified and dynamic free trade area. First, the agreement fully respects the data rights of member States by giving all contracting parties the freedom to choose what constitutes "legitimate public policy" in its annotations. It provides parties with regulatory space, emphasizing the rights, security and common development interests of all parties. Secondly, the RCEP places special emphasis on the security of cross-border data flows; the RCEP faces an important difficulty, namely, the different economic strengths of the contracting parties, which cover both developed and developing countries, and carry a certain degree of mobility risk. As a result, the agreement adopts different attitudes towards data regulation for different countries. However, even for those countries with relatively lax regulations, RCEP still does not grant them

DOI: 10.54254/2753-7064/37/20240178

complete freedom of movement. In terms of content, the principle of "security exclusion" is explicitly stipulated under the "general conditions and exclusions" rule of RCEP, which aims to safeguard the data sovereignty of countries under the agreement and maintain public order.

Finally, RCEP has also made a certain contribution to blocking "long-arm jurisdiction". Some countries, led by the United States, have violated the data sovereignty of other countries in the name of "long-arm jurisdiction", which has aroused the vigilance of many countries. In order to deal with the problem of "long-arm jurisdiction", the RCEP establishes the prohibition of transfer of information systems of telecommunication and financial institutions in transnational circulation, which blocks the opportunity for the U.S. to intervene as a third party in the regulation of the financial markets of the contracting parties [8]. The RCEP emphasizes in its provisions that "no personal information received shall be disclosed to any agency, social entity or person to whom the contracting parties have not granted the right to submit personal information", thus effectively preventing the illegal acquisition of personal information due to long-arm jurisdiction.

3.3.2. Legal Regulation of Cross-Border Data Flows in CPTPP

The CPTPP evolved from the TPP, and the economies of the 11 signatories together account for 13.4% of global GDP. In terms of content, it is advanced in two ways. First, it strictly limits data localization and affirms the regulatory powers of the parties. The CPTPP establishes mandatory obligations for parties to transmit electronic data across borders using e-commerce methods, allowing parties to impose or maintain measures restricting data transfers on a purpose, manner, and limit basis. Secondly, it also recognizes "security exceptions" for parties based on national security. On the one hand, it prevents illegal acts from infringing on trade and makes the flow of data more secure; on the other hand, it recognizes the subjective status of the State and the importance of public security, and accords full respect to States parties.

At the level of personal information protection, the CPTPP allows for the establishment of institutions to promote compatibility between various regimes and provides for non-discrimination in the protection of personal information. Although, due to the withdrawal of the U.S., the agreement never came into effect, it reflects, to a certain extent, the expectations and requirements of different countries on data regulation and provides a model for future relevant legislation.

4. China’s Improvement Program under the Transnational Data Flow Problem

4.1. Hierarchical Management of Formation Data

China has long practiced a "top-down" regulatory system in which data security is controlled by administrative organs at various levels to maintain market security. With the progress of society, the total amount of data is increasing, and the huge database has brought a certain burden to the administration. In the face of different layers of data, administrators need to identify them one by one and then adopt different processing methods, which greatly reduces the work efficiency of the authorities. It can be seen that the "bottom-up" approach to information security management is no longer able to cope with the new information security risks arising from the explosive and rapid development of big data analytics and new business models. In order to solve this problem, China needs a hierarchical management of data. Based on factors such as domain, security factor, and rarity, administrative agencies can categorize data into different levels and prescribe regulatory review methods with varying degrees of stringency. For example, those privacy-related data need to go through at least three levels of approval and be licensed before they can enter international market circulation; for relatively unimportant data, the government can give the market the initiative to rely on industry guidelines and its own restorative power to achieve data regulation.

DOI: 10.54254/2753-7064/37/20240178

The coercive nature of public power and the spontaneity of the market are contradictory concepts, and the flow of data is both an economic and a social issue, so it needs to play to the strengths of both the public and private tiers at the same time. After the hierarchy, these two rights can be well balanced and contribute to data security in their respective fields. In this way, huge amounts of data can be judged by a standard when entering or leaving the Chinese market, promoting the controllability and security of its circulation.

4.2. Clarify the Boundaries of Data-processing Responsibilities

Currently, China generally takes a "reactive" approach to data regulation, i.e., after a data breach, the leaker is penalized, and data security is re-established. However, the illegal dissemination of data is a relatively low-cost crime with very serious consequences and should be taken seriously by administrators. If the state relies only on after-the-fact remedies, it can only serve as a warning against this type of behavior to a certain extent but cannot truly eliminate this risk. The impact of data leakage is tragic, so the State should emphasize the importance of data regulation, clarify the boundaries of responsibility, and raise the level of attention paid to it by administrators.

In terms of safeguarding national data sovereignty, States should adopt a system of dual responsibility, whereby both the data processor and the administrative subject should be responsible for the security of cross-border data flows. Data in modern society has developed into an important "intangible asset", therefore, when processing data, the subject should take the initiative to assume the corresponding obligations. Among them, some large Internet platforms play a particularly prominent role, and in order to safeguard national data sovereignty and personal privacy security, and to reduce possible data leakage in the process of cross-border data flow, they should strictly abide by the relevant national laws and regulations and apply for approval by the relevant departments in a timely manner for the cross-border flow of important data.

4.3. Improving the Extraterritorial Application of the Data Security Act

As a subject of international relations, China should not only adhere to its own subject position, but also abide by the basic rules of international law and the principle of equality of data sovereignty, adhere to multilateralism, and advocate the building of a community of a common future for mankind. Data is intangible, reproducible and non-territorial, and data exchanges may involve some foreign-related issues and touch the legal boundaries of other countries. China must take the basic principles of international law as the bottom line, regard the prohibitive rules of international law as warning lines, and practice extraterritorial jurisdiction over data on the basis of full respect for the data sovereignty of other countries, so as to limit data control to the framework of national rights.

Secondly, China should adhere to the "actual damage" standard. If the conduct of another State actually infringes on the data interests of the State, society or individuals, it should be subject to legal regulation. It is important to note that, as in other laws, there must be a direct causal link between the act and the result. Finally, China should indicate the legal liability for extraterritorial data infringement, including civil, criminal and administrative liability, and adopt measures such as fines and confiscation of illegal gains. Because the international flow of data is more risky, extraterritorial offenses should not be held to a lower standard than domestic ones, reducing citizens' concerns about their privacy. The domestic application of the Data Security Law has served data regulation well, and lawmakers should place it in an international perspective to urge orderly data flows.

5. Conclusion

Facing the problem of data regulation, many countries have reached a consensus on the four basic principles, dissected and understood them, and formulated national laws to safeguard national data

DOI: 10.54254/2753-7064/37/20240178

security. It can be learned through the summarization of this paper that China has made outstanding legislative achievements in this field in recent years, going through three stages and forming a regulatory system with three laws as the core. Compared with the systems of other countries and international regional treaties, China's system has its own cultural characteristics, but there are still deficiencies. Therefore, China should continue to explore and formulate new provisions in the areas of forming hierarchical data management, clarifying the boundaries of responsibility for data processing, and improving the extraterritorial application of the Data Security Law, as well as expanding its scope of application internationally, so as to contribute to global data regulation.

In the future, the world's databases will become even larger, which will require not only the maintenance of their own security, but also their full cooperation in limiting data sharing to the legal limits and promoting the rapid development of world trade.

References

[1] *Xia Han, Paradigm Shift of European Union (EU) in Cross-Border Data Flow Supervision - From the Perspective of Digital Services Legislation, 13 J. WTO & CHINA 69 (2023).pp:13.*

[2] *Junmeng Liu, Research on WTO Regulation of Cross-border Data Flow,2022.DOI:10.27354/d.cnki.gtcjy.2022.000856.pp:19.*

[3] *Jin Han, International Regulatory Research On Cross-border Data Flow[D]. 2023.DOI:10.27106/d.cnki.ghbju.2023.000515.pp:13.*

[4] *Weiwei Zheng, Comparative Study on the Legal Regulation of a Cross-Border Flow of Personal Data and Its Inspiration to China, 15 FRONTIERS L. CHINA 280 (2020).pp:290.*

[5] *Jinrui Liu, Towards a Global Regulatory Framework for Cross-Border Data Flows -Fundamental Concerns and the China's Approach, 17 FRONTIERS L. CHINA 412 (2022).pp:427.*

[6] *Si Chen, Research on Data Sovereignty Rules in Cross-Border Data Flow and Chinese Solution, 18 US-CHINA L. REV. 261 (2021).pp:266.*

[7] *Si Chen, Application of U.S. Long-Arm Jurisdiction in Cross-Border Data Flows and China's Response, 19 US-CHINA L. REV. 65 (2022).pp:67.*

[8] *Jia Wan, Research on legal regulation of cross-border data flow in China, 2022.DOI:10.27422/d.cnki.gxzfu.2022.000183.pp:21.*