Journal of Commercial Law Review
2024, VOL. 8, NO. 4, 61-72
DOI: 10.47297/wspjclrWSP2516-249709.20240804

Disputes Over Cross-border Data Flow and Its China's Legal Solutions

Jing Lin

Human Rights Research Institute of Southwest University of Political Science and Law, Yubei, Chongqing, 401120, China.

ABSTRACT
With the deepening development of data globalization, cross-border data flows have become increasingly frequent, leading to increasingly severe legal disputes. Against this backdrop, this article delves into the disputes arising from cross-border data flows. It deeply analyzes the manifestations of these disputes from the perspectives of data sovereignty and national security, economic development and data protection, as well as cross-border law enforcement cooperation. Based on this, it further explores the reasons behind these disputes, taking into account both international experience and China's national conditions. It strives to balance the relationship between data sovereignty, national security, and data economy development, providing ideas and references for the development of China's governance rules for cross-border data flows.

KEYWORDS
overall national security concept; cross-border data flow; legal disputes

1 Legal question about disputes over cross-border data flow

In recent years, due to the rapid development of technologies such as the Internet, cloud computing, and big data, cross-border data flows have become more common and frequent. Various issues associated with cross-border data flows have gradually attracted the attention of domestic scholars, mainly reflected as follows: First, research on cross-border data flows incorporating game theory. As the two major global economies, Europe and the United States have engaged in multiple rounds of games around cross-border data flows, and domestic scholars have conducted research on the focal points, processes, and means of the game between Europe and the United States. Yan Feng, Pan Feifei, et al. (2016) believe that the core of the game of interests between Europe and the United States lies in the commercial value of cross-border data flows, and the outcome of the game is determined by the value of data, the players involved, and the strength of both parties. Cao Wei (2018) believes that the focus of the competition between Europe and the United States is the international discourse power and rule-making power of cross-border data flows. Liu Wenjie (2022) also believes that the competition between Europe and the United States is for the dominance in determining standards for cross-border data flows. Second, research on the governance of cross-border data flows. Currently, the governance of cross-border data flows has attracted widespread attention and discussion among researchers in related fields, exploring the governance models, dilemmas, and paths of cross-border data flows in typical countries. Wang Yan (2022), Cha Hongwang, et al. (2019) analyzed the representative governance models of cross-border data flows in the United States, the European Union, and China. The study found that the United States advocates the free flow of data across borders; the European Union emphasizes the

protection of personal privacy and data, proposing a "loose inside and strict outside" governance model for cross-border data flows; compared to Europe and the United States, China's governance of cross-border data flows takes national security as the core goal, taking into account personal privacy and rights protection, and trying to reduce unnecessary restrictive measures to avoid hindering the development of digital trade. Chen Bing, Xu Wen (2021) analyzed the problems existing in China's cross-border data flow governance system, such as a single domestic governance mechanism, weak operability, insufficient grasp of international discourse power, difficulties in compliance work for multinational enterprises, and potential to be activated. Third, comparative research on the rules of cross-border data flows. Compared with Europe and the United States, China's construction of cross-border data flow governance rules started relatively late, and there are some shortcomings and deficiencies. Therefore, domestic scholars have sorted out the cross-border data governance rules and models of important sovereign countries and international organizations such as the European Union, the United States, and Japan, and compared them from different perspectives to provide countermeasures for China.

Deng Song, Huang Lan, Ma Butao (2021) systematically analyzed the value selection, strategic planning, legislative confirmation, institutional setting, and cooperation mechanism of cross-border data flows in China, Europe, and the United States, compared the differences and common experiences of cross-border data management between Europe and the United States, and provided effective suggestions for the construction of cross-border data management in China. Song Jingjing and Wu Jianhua (2022) analyzed the opportunities and risks faced by cross-border data governance based on the interpretation of its basic connotation, identified the main paradigms of current cross-border data governance, and proposed coping strategies for China's cross-border data governance. Sun Pengpeng (2023) provided relevant references and insights for further improving China's cross-border data flow regulatory measures by comparing and analyzing the legislative models, specific rules, and rights and obligations of cross-border data regulation in Europe and the United States.

Based on relevant research, it is evident that there is no unified international governance rule for cross-border data flows. Countries, considering factors such as historical traditions, cultural levels, and industrial differences, hold varying attitudes and coping strategies towards cross-border data flows, adopting distinct governance models. This diversity has led to the formation of barriers hindering cross-border data flows, necessitating policy coordination among nations. Currently, competition and cooperation in the governance rules for cross-border data flow disputes are intertwined. These issues are crucial for national development and security, urgently requiring in-depth research and discussion. In light of this, this article, based on the aforementioned research on cross-border data flows, conducts an in-depth analysis of disputes arising from cross-border data flows and their causes. Furthermore, through a comparative analysis of the governance experiences of cross-border data flows in Europe and the United States, it aims to contribute to the construction of China's governance rules for cross-border data flows. This, in turn, will better enable China to address risk challenges in great power rivalries, safeguard national security, and uphold data sovereignty.

2 Manifestations of disputes over cross-border data flow

With the deepening development of data globalization, the scale of cross-border data flows continues to rise, and the number of factual disputes and legal controversies exposed is also increasing. This has triggered concerns and worries among countries about data security, and has led to strengthened control and regulation of cross-border data flows.

2.1 Conflict between data sovereignty and national security

Cross-border data flow has gradually become an issue closely related to national sovereignty and national security. The boundary between state secrets and non-secrets has also become blurred, and traditional data security boundaries have been unable to meet the complex and ever-changing data security needs. On the one hand, important data such as geographic information of important targets, safety supervision information of civil nuclear facilities, and security information of financial institutions are closely related to national security and do not require aggregation and analysis. Once they leave the country, they may endanger national security. On the other hand, under the influence of technologies such as big data and artificial intelligence, massive amounts of data reveal hidden information. In the process of transition from quantitative to qualitative data changes, the surface-level personal privacy or commercial interests are associated with national security interests, which may pose a threat to national security. The review of Didi Chuxing by the Security and Cybersecurity Review Office of the National Internet Information Office is a typical example. As China's largest travel and transportation platform, Didi continuously collects personal travel, traffic, and street view data from all cities in China. Its listing on the New York Stock Exchange in the United States is likely to result in a large amount of personal data flowing to the United States. Through the analysis and processing of the acquired massive data, it can be used for military purposes, thereby endangering China's national security.

In the context of digitalization, internet platforms represented primarily by search engines, social media, and e-commerce websites have rapidly become the main entities for cross-border data flows. Commercial companies in the form of large internet platforms can collect, process, and commercialize personal information on a large scale for commercial purposes. Users may unintentionally disclose relevant data to foreign entities when using online services of overseas websites. Through the aggregation and correlation analysis of massive, real-time, and dynamic data, national intelligence may be leaked, threatening national security. The "Prism" incident in 2013 fully exposed the use of nine internet companies including Microsoft, Google, Apple, and Yahoo by the US security department to monitor or listen to users outside their service territory, and transfer overseas data to domestic areas, causing global panic and widespread concern among sovereign states. Since then, "data sovereignty" has been proposed and widely discussed. Countries claim national sovereignty over the possession, processing, management, and exclusion of interference from other countries and organizations in their data. For example, Russia, Vietnam, and Indonesia regard data sovereignty as an essential aspect of national security and prevention of foreign surveillance. However, the characteristics of cross-border data flows such as their super-regional, open, and global nature make data sovereignty interdependent, which traditional sovereignty does not possess. Countries need the cooperation of relevant countries to exercise or maintain their data sovereignty to a greater or lesser extent. When sovereign states exercise data sovereignty, they cannot forcefully apply their own data governance rules to related countries. The regulation of cross-border data by a single sovereign state may endanger the sovereignty of other countries. For example, the "Cloud Act" passed by the United States in 2018 established the standard for data controllers. As long as the data is under the control of American internet companies, it is assumed that the US government can directly retrieve data from around the world, seriously affecting the sovereignty of data storage countries over their data. This has made it difficult to bridge the gap between the United States and data storage countries. Although the "Cloud Act" stipulates that the obligation of data controllers to disclose overseas data is only applicable in major cases involving crimes that endanger US national security or serious criminal offenses, given the increasingly intense geopolitical struggle situation worldwide, there is a high possibility that the United States will generalize and abuse "national security" to obtain extraterritorial data for its political purposes.

For example, the US government has signed executive orders to forcefully suspend Chinese companies' operations in the United States or prohibit US entities or individuals from trading with Chinese companies on the grounds of threatening national security. As a short video social platform, TikTok's data does not fall under the definition of critical information infrastructure as outlined in the 2013 U.S. "Improving the Security and Resilience of Critical Infrastructure" Act. It does not involve U. S. national security or fundamental security interests. The U. S. imposing cross-border data flow regulation measures on TikTok under the pretext of national security is an abuse of national security provisions. Evidently, the limitations of the U. S. "Cloud Act" cannot eliminate the sense of data sovereignty crisis in the EU and other sovereign countries, inevitably leading to significant disagreements and contradictions among nations regarding this development trend.

2.2 Contradiction between economic development and data protection

In the context of digitalization and the globalization of trade, the scale of cross-border data flows has rapidly increased, and its impact on economic growth has surpassed that of traditional cross-border trade and investment. However, different countries have varying requirements for data regulation, leading to significant differences in their pursuit of economic development and data security protection. On the one hand, the free flow of cross-border data can promote the development of digital trade and further invigorate the global digital economy. On the other hand, countries aim to safeguard national security by controlling data flows to prevent potential security risks posed by data leakage. To promote the development of the global economy, the international community advocates promoting cross-border data flows under the premise of ensuring data security, national security, and respecting other countries' data sovereignty. Organizations or institutions such as the WTO, G20, and OECD have been promoting global or regional rules for cross-border data flows, committed to fostering the development of the global digital economy.

The United States also maintains a relatively liberal stance in the multilateral or bilateral agreements it leads on cross-border data flows, opposing the establishment of trade barriers by other countries through restrictive data cross-border laws and policies. As the world's largest economy, the United States boasts a developed digital economy and industries, which are inseparable from the cross-border transmission, development, and utilization of massive, real-time, and heterogeneous data resources spread across the globe. Unrestricted free flow of data aligns more closely with American interests, while promoting data localization would hinder the development of the US technology and information industries. However, for countries with weaker digital economy capabilities, advocating for free cross-border data flow could lead to their industrial and economic markets being occupied by foreign enterprises, thereby impeding the development of their digital industries. Moreover, unrestricted cross-border data flow could weaken a country's ability to control its own data, posing risks of personal privacy leakage and the erosion of national data sovereignty. Therefore, countries have introduced data localization measures to restrict the flow of cross-border data. Countries such as Russia, India, Malaysia, and Brazil have adopted data localization storage methods to strictly limit data flowing out of their territories, in order to curb national data security risks. It is evident that countries adopt different policies based on their emphasis on economic value and security value. Countries pursuing free cross-border data flow often emphasize freedom and efficiency in digital economy and trade between countries, while countries restricting free data flow focus more on the security and development of sovereign states. This means there is tension between the public policy reservation requirements proposed by developing countries and the open digital trade environment advocated by developed countries.

Whether regulatory measures for cross-border data flow can truly achieve the purpose of protecting individual rights and national security is questioned by countries with advanced digital

technology. They believe that data security is determined by the way data is stored and transmitted, and is not related to the location of data storage. The cross-regional nature of the Internet makes attacks on data indistinguishable Boundaries. If a country adopts overly strict regulations on cross-border data flows for the purpose of protecting data security and data sovereignty, it may increase the operational costs of data controllers and processors, thereby hindering global data flows, affecting cross-border trade, and even impeding domestic enterprises from entering the international market. Over the long term, this will have a negative impact on economic development. If the host country requires enterprises operating in the country to store data locally, enterprises will have to repeatedly build data storage facilities, increasing data storage and processing costs. They will also need to determine the applicable laws and data collection and processing methods based on the source of the data, increasing the compliance costs of cross-border data business. According to economists' estimates, the requirement for local data storage leads to a 30% to 50% increase in data storage costs for enterprises, resulting in welfare losses of up to $63 billion per year for China, and losses of up to $193 billion for the European Union.

2.3 Challenges in cross-border law enforcement and cooperation

Due to the transnational nature of data flow, issues related to law application and jurisdiction in different countries and regions pose challenges in addressing cross-border crimes or data breaches. Firstly, the application of law poses a difficulty. Cross-border crimes or data breaches may involve laws from different countries, making it challenging to determine the applicable law. Legal provisions for the same act may vary or even contradict each other across countries, adding complexity to the application of law. For instance, the laws of a certain country may only apply to data processing and storage within that country, while the laws of other countries may cover the entire globe. This leads to inconsistent application of laws across different countries and regions during cross-border data flow, resulting in legal conflicts and disputes. Secondly, there are disputes over legal jurisdiction. The scope and standards of legal jurisdiction over cross-border data vary among countries and regions. Different countries may believe they have the right to govern the processing and storage of related data based on their sovereignty, which can lead to cross-border data being subject to the jurisdiction of multiple countries and regions, resulting in legal conflicts and disputes. For example, if data is generated by citizens or legal entities of a member state of the European Union and is transmitted across borders to a processor in the United States, it involves the application of both the General Data Protection Regulation of the European Union and the U.S. Clarification Act on the Lawful Use of Overseas Data. According to the U.S. Clarification Act on the Lawful Use of Overseas Data, any U.S. electronic communication service provider or foreign service provider operating in the United States is obligated to provide data preservation and backup to the U.S. government, granting U.S. law enforcement agencies the authority to retrieve data stored on servers outside the United States from enterprises. Based on this, U.S. law enforcement agencies can obtain personal information of EU citizens through service providers under the Cloud Act. However, the EU has not recognized and agreed to the applicability of the U.S. Cloud Act in EU countries. Furthermore, according to the General Data Protection Regulation of the EU, regardless of whether a data controller or processor has an entity established within the EU, their personal data processing behavior towards data subjects is subject to the application of this law. Therefore, it can be seen that differences in legal provisions for cross-border data among different countries and regions lead to disputes over jurisdiction among various parties.

The uncertainty surrounding the legal application and jurisdiction of cross-border data not only increases the legal risks associated with cross-border data flows but also hinders international law enforcement cooperation. Countries have varying enforcement mechanisms and regulatory systems

for data protection, and the absence of a unified coordination and cooperation mechanism may lead to requests for law enforcement cooperation being rejected or delayed. The existing cross-border law enforcement rules are based on the physical world, and cross-border law enforcement activities between different jurisdictions are carried out through the signing of bilateral or multilateral treaties and mutual legal assistance agreements. However, the practical implementation has been ineffective. Through treaties or mutual legal assistance agreements, law enforcement agencies need to report to central authorities such as the Supreme Court or Ministry of Foreign Affairs for diplomatic negotiations, facing complex paperwork and lengthy waiting periods. If there are no treaties or mutual legal assistance agreements between two countries, each case must be negotiated individually, facing great uncertainty and being susceptible to political interference. This process is time-consuming and inefficient, which is not conducive to combating illegal and criminal activities.

3 Causes of disputes over cross-border data flow

3.1 Fragmentation of international rules

Currently, various countries and regions in the world have inconsistent governance rules regarding cross-border data flow, and there are even many contradictions and conflicts, making it difficult for the international community to form unified governance rules, leading to frequent disputes over cross-border data flow.

Firstly, at the national/regional level, the varying levels of digital economy development and legislative value objectives among countries lead to different interests in cross-border data flow governance rules, making it difficult to reach a consensus. Most developed economies, based on their advantages in the information industry and leading position in the digital economy, have a greater demand for the free flow of cross-border data, believing that strict restrictions on the flow of cross-border data will create trade barriers. For example, the United States, as the country with the most developed Internet technology globally, advocates for the free flow of cross-border data in the trade agreements it leads or participates in, in order to leverage its industrial and technological advantages in the field of digital economy and trade. Unlike the United States, the European Union places more emphasis on data security and privacy protection, actively promoting the free flow of data among its member states, but imposing strict controls on countries and regions outside the EU, requiring data receiving countries to meet similar protection levels as the EU before allowing cross-border data flow. Compared to developed economies, developing economies such as China, India, and Malaysia have relatively lagging data industry development and insufficient information technology levels, making cross-border data flow more risky. Therefore, their governance rules for cross-border data flow are more concerned with national security, implementing measures such as data localization storage to protect national data security, which leads to numerous data protection barriers that restrict cross-border data flow. The differences in governance rules for cross-border data flow reflect the choices of different countries regarding freedom and security values, and the contradiction between these two goals is difficult to balance in a short period of time.

Secondly, multilateral rules lack enforceability. The current multilateral governance rules for cross-border data flow disputes exhibit an imbalance between "hard" and "soft" rules. Whether it is the "Guidelines for Privacy Protection and Cross-Border Flows of Personal Data" issued by the Organization for Economic Cooperation and Development (OECD), or the Cross-Border Privacy Rules (CBPR) under the framework of the Asia-Pacific Economic Cooperation (APEC), although they have a certain degree of global influence and flexible and broad judgment standards and interpretation space, they are mostly initiative and principled rules, essentially belonging to the nature of "soft

law", lacking in enforceability and operability in terms of responsibility content and procedural arrangements. In addition, the existing WTO rules are also difficult to handle disputes over cross-border data flow. Due to the large number of WTO members and the significant differences in economic development levels among them, as well as different interests in data flow, it is difficult for all parties to achieve a balance of interests under this multilateral framework.

Finally, bilateral cooperation is fraught with contradictions and conflicts. For a long time, there have been differences in the protection concepts and institutional designs of cross-border data flow between Europe and the United States. In order to address the obstacles in data flow, the two sides have successively reached the Safe Harbor Agreement and the Privacy Shield Agreement. However, both agreements were subsequently declared invalid by the European Union Court of Justice. This reflects the fundamental contradiction between the EU's emphasis on protecting personal data rights and the United States' pursuit of economic interests. Although both sides have attempted to compromise and integrate, they have failed to reach a "balance point" and thus cannot achieve sustainable development. Due to the short-term differences that are difficult to eliminate between major digital powers, it is difficult for the international community to form a unified, multilateral governance rule for cross-border data flow disputes.

3.2 Conflicts over data sovereignty jurisdiction are severe

Cross-border data flow involves multiple actors, including data subjects, data controllers and processors, as well as data regulatory authorities. During the generation, collection, trading, transmission, storage, and other processes of a piece of data, it may undergo processing by multiple actors, which can easily lead to overlapping or even conflicting sovereignty interactions. From existing practices, it can be observed that data is composed of bytes and can be transferred, copied, and distributed across multiple jurisdictions without affecting access within the territory at any time. When legislating on data flow, countries choose different connection points, and various models such as territorial principle, personal principle, effect principle, and closest connection principle emerge. Legislative jurisdiction among different countries may conflict or compete, or conflict with relevant provisions of international law. Different jurisdictions claim different principles for the same type of data, leading to disputes over jurisdiction and triggering jurisdictional conflicts. Taking the Microsoft data lawsuit case in 2013 as an example, the US Department of Justice requested Microsoft to hand over personal emails and related communication content of Microsoft users stored in Ireland to assist the US Drug Enforcement Administration in investigating drug smuggling cases. However, Microsoft believed that according to the Stored Communications Act, the US Department of Justice had no right to access data of American companies located in foreign countries, and publishing personal data stored in Europe would violate EU data protection regulations. The two parties engaged in back-and-forth litigation over the issue of data ownership and jurisdiction.

With the expansion of the extraterritorial application of governance rules for cross-border data flows in Europe and the United States, almost all cross-border data flows are subject to the jurisdiction of multiple countries, resulting in widespread issues of overlapping jurisdiction. The "long-arm jurisdiction" provisions of the General Data Protection Regulation (GDPR) clearly stipulate that even if a data controller or processor does not have a physical presence within the European Union, they are still subject to EU regulation as long as they engage in business activities within the EU. Meanwhile, the United States adopts a "nationality jurisdiction" approach, exercising data flow monitoring and jurisdiction over all American companies both domestically and abroad. The United States introduced the "Clarifying Lawful Use of Data Abroad Act" (Cloud Act) in 2018, which advocates for data jurisdiction through the "data controller standard," meaning that the United

States has jurisdiction over data controlled by American data service providers, even if the data storage location is abroad. The long-arm jurisdiction of the United States and Europe will undoubtedly intensify sovereignty conflicts with countries where data is stored.

In the context of overlapping jurisdictions, cloud computing service providers will compare different legislative policies across countries and then transfer data to circumvent the domestic legal regulations on data protection imposed by sovereign states, thereby affecting a country's data security. In response to this situation, sovereign states will impose legal restrictions on the location of data infrastructure on the grounds of data sovereignty, incorporating mobile data into their territorial jurisdiction through localization requirements for data infrastructure, in order to achieve actual control over data. It is evident that the boundaries of jurisdiction among countries are not clear for cross-border data flows. The unilateral expansion of long-arm jurisdiction by Western countries has exacerbated mistrust among nations, further stimulating "follow-the-trend legislation" among countries, indirectly leading to a proliferation of jurisdictional conflicts.

4 Legal governance models and approaches for cross-border data flow disputes

Currently, there is no unified global governance rule for cross-border data flow. To prevent various disputes arising from cross-border data flow, countries are actively legislating to regulate the flow of cross-border data. Represented by the United States, the European Union, and China, three distinct governance models for cross-border data flow have emerged. These diverse data governance models reflect different national interests in digital economy development, data sovereignty, national security, and human rights values.

4.1 The American model oriented towards free trade

The United States values the economic benefits brought by data flow and believes that excessive regulation is not conducive to innovation and vitality in the digital economy market. It promotes its advocacy of "prohibiting data localization measures" and "encouraging free cross-border data flow" by signing bilateral or multilateral trade agreements with other economies, in order to suppress the barriers set up by other countries for cross-border data flow, thus achieving the goal of gathering global data in the United States. In 2004, the United States led and promoted the Asia-Pacific Economic Cooperation (APEC) to adopt the APEC Privacy Framework, requiring member countries to "take all reasonable steps to avoid and eliminate any unnecessary obstacles to data flow". In subsequent years, the United States continued to expand and deepen its free value concept in the market field during FTAs negotiations, advocating for the inclusion of free cross-border data flow as a principled clause to break down data export barriers in other countries. For example, the United States and South Korea reached the US-Korea Free Trade Agreement in 2012, requiring both parties to avoid setting unnecessary obstacles to cross-border data flow. In 2013, the Cross-Border Privacy Rules (CBPRs) advocated and supported by the United States were officially adopted, forcing participating countries to agree to the lower protection level of the United States in cross-border data flow and give up insisting on high protection levels for data domestically, in order to attract data inflow into the United States and facilitate American companies' access to global data.In 2015, the United States led the adoption of the Trans-Pacific Partnership Agreement (TPP), which specifically set up the "Commercial Information Cross-Border Free Transmission Clause" to relax restrictions on cross-border flow of commercial data, reflecting the United States' pursuit of fully realizing free data flow. Not only that, the United States also demanded more freedom in cross-border data flow and strictly limited data localization in the USMCA it signed.

Although the United States advocates "cross-border free flow of data" when acquiring

extraterritorial data, it does not mean that the United States ignores the national security risks posed by the free transmission of data. The United States adopts relatively strict restrictive measures for data involving U. S. national security on the grounds of protecting national security and preventing privacy leaks. In 2018, the United States passed the Foreign Investment Risk Review Modernization Act (FIRRMA Act), which considers sensitive personal data as an important part of national security and authorizes the Committee on Foreign Investment in the United States (CFIUS) to conduct investment security reviews on cross-border transfers and transactions of sensitive personal data to prevent these data from being acquired by foreign governments or entities. In 2019, the United States issued an executive order titled "Ensuring the Security of Information and Communications Technology and Services Supply Chain" and implemented the "Clean Network Plan", prohibiting the trading and use of information and communications technology and services from other countries that may pose a threat to national security, foreign policy, and the economy. In 2021, the United States issued another executive order titled "Protecting Sensitive Data of Americans from Foreign Adversaries", to prevent sensitive data involving U.S. national security from leaving the country. From this, it can be seen that the purpose of the United States implementing the above measures is to restrict a country's government from being able to access U. S. data through the business presence of its enterprises in the United States.

In addition, the United States will leverage its economic and technological advantages to impose long-arm jurisdiction on cross-border data flows, in order to meet the law enforcement needs of cross-border data retrieval under the new circumstances. In 2018, the U. S. Congress passed the "Clarifying Lawful Overseas Use of Data Act" (CLOUD Act), which, by applying the "controller principle," authorizes U.S. law enforcement agencies to require data service providers to store, back up, and disclose data under their regulatory control, even if such data is stored overseas. In summary, with the aim of promoting the free cross-border flow of data and guided by economic interests and free trade, the United States hopes to continuously attract global data convergence through its industrial and technological advantages, while also restricting the cross-border flow of data in important areas, reflecting a trend of emphasizing the security of data flow.

4.2 The EU model, which prioritizes the protection of data subjects' human rights

Due to historical, geographical, political, and other factors, the European Union places particular emphasis on protecting the rights of data subjects, defining personal data protection as a basic human right. This right is closely related to the human dignity of data subjects, It is an extension and development of traditional privacy rights. After World War II, the Universal Declaration of Human Rights protected privacy as a fundamental right, prompting countries around the world to recognize this right through active legislation. Article 8 of the 1953 European Convention on Human Rights stipulates that individuals have the fundamental right and freedom to have their private and family life respected. Later, the Charter of Fundamental Rights of the European Union, based on the European Convention on Human Rights, clarified that individuals have the right to personal data protection.

In 1981, the European Union introduced the "Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data," aiming to strengthen data protection, prevent the abuse of personal data during collection and processing, and protect the individual data security of each contracting state. Later, in 1995, the "Directive on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of Such Data" (hereinafter referred to as the "95 Directive") was introduced, establishing high data protection standards and providing unified regulations for the protection of individuals' fundamental rights and freedoms in personal data processing. In 2018, the EU passed the "General Data Protection Regulation" (GDPR) to fully

replace the "95 Directive," continuing to strengthen the protection of data subjects' rights. Based on further confirmation and improvement of existing rights of data subjects, many new rights were added, such as the right to be forgotten and the right to data portability, aiming to enhance data subjects' control over their personal data and keep it in their hands. Not only that, the GDPR also added obligations for data processors, such as data protection obligations, data breach reporting obligations, data system protection, and default protection obligations, further strengthening the protection of data subjects.

With the implementation of GDPR, the entire EU has achieved a high level of protection for personal data, while also promoting the free flow of data within the EU. Regarding the flow of personal data from the EU to other regions of the world, the EU requires that the level of protection for personal data abroad should be equivalent to that of GDPR. Otherwise, it is not allowed. There are mainly two situations where data is allowed to flow outside the EU: First, when a third country is recognized by the EU as being able to provide "adequate protection" for personal data, data can be transferred to that third country. Article 25 of Directive 95 stipulates the conditions for the transfer of personal data to a third country, which is only allowed when the third country has achieved a sufficient level of protection in terms of personal data privacy. In practice, the EU and the US signed the Safe Harbor Agreement and Privacy Shield Agreement on cross-border data transmission in 2000 and 2016 respectively, but these two documents were ruled invalid by the EU Court of Justice in 2015 and 2020 respectively, due to the failure of the US to provide the same level of personal data protection as the EU. Countries and international organizations that have been recognized as adequate will be included in the "white list" for free cross-border data transmission by the EU Commission. Currently, only a few countries or regions have received this recognition from the EU. Second, in cases where a third country cannot provide "adequate protection", if the controller or processor of personal data can provide "appropriate safeguards" and provide enforceable rights and effective legal remedies for data subjects, the controller or processor can transfer personal data to that third country. The so-called "appropriate safeguards" include signing legally binding documents between government agencies, following codes of conduct or certification mechanisms approved by relevant EU institutions, and adopting standard data protection clauses by the EU Commission or regulatory agencies. In addition, in the absence of an adequacy decision and appropriate safeguards, Article 49 of the GDPR stipulates exemptions for cross-border data transfers in specific circumstances, such as "explicit consent of the data subject", "necessary for the conclusion or performance of a contract", "public interest", "legal claims", and "significant interests". This means that cross-border data transfers are also permitted in these situations.

4.3 The Chinese model that prioritizes safeguarding data sovereignty

Compared to the strict protection of personal data rights in the EU, China places greater emphasis on the overall maintenance of national security. In recent years, guided by the overall national security concept, China has gradually improved the construction of the legal regulatory system for cross-border data flow, gradually forming a governance system for cross-border data flow rules with the Cybersecurity Law, Data Security Law, and Personal Information Protection Law as the main content, supplemented by a series of administrative regulations and departmental rules.

However, compared to Europe and the United States, China, as a latecomer in data security governance, lacks technological advantages and institutional guarantees for data development. It is difficult to resist the data security risks caused by ineffective data regulation, especially the uncontrollable risks of malicious monitoring by foreign countries or forces. It is also difficult to effectively deal with the judicial risks brought by the expansionary extraterritorial data law enforcement jurisdiction in the current international arena. Therefore, there is still some room for

improvement in the legal regulation of cross-border data flow in China.

First, we must adhere to the integration of development and security. Cross-border data flow is the core driver of the global digital economy development
Strength. According to statistics, the contribution rate of cross-border data flow to global GDP has reached 10%. Economic research shows that data is a liquid asset, and only data that flows rapidly between countries, organizations, objects, and people is valuable. The World Bank's "Data Restriction Index" indicates a negative correlation between restrictions on cross-border data flow and economic development. Excessive restrictions on cross-border data flow may increase corporate costs, weaken international competitiveness, inhibit innovative development, and seriously endanger national economic security; while unordered data flow also poses security risks, which can seriously endanger national security, the national economy, people's livelihood, and public interests. Therefore, China should be guided by national overall security, and under the premise of ensuring national data security, carefully balance the needs of free data flow and protection. We cannot absolutely pursue one value and give up another, and we must promote a dynamic balance between high-quality development and high-level security. We should adhere to the rational use of personal data on the basis of fully protecting the personal rights of data subjects and data sovereignty and security, and reduce unreasonable data localization restrictions. On the one hand, China should attach importance to protecting personal data rights and maintaining national security, and put forward restrictive requirements for foreign entities obtaining Chinese data; on the other hand, China should align with the current development needs of the digital economy and international trade, reasonably set data flow barriers, reasonably assign responsibilities and obligations to enterprises, coordinate the interests of all parties, and achieve a balance between data protection and free flow.

Secondly, we should improve relevant legislation on cross-border data flow to counteract. Both the EU's GDPR and the US's CLOUD Act seek to expand their data sovereignty beyond their borders, aiming to strengthen control over extraterritorial data. This may not only affect Chinese enterprises but also infringe on China's national sovereignty. Therefore, China should actively formulate corresponding laws to counteract them. For example, when Europe and the United States require Chinese enterprises to provide data they possess based on the extraterritorial effect of their domestic laws, China can refuse cross-border transfer of data in accordance with the data localization requirements of the "Cybersecurity Law" and "Personal Information Protection Law", thus blocking the effectiveness of other countries' law enforcement. Another example is Article 55 of the "Personal Information Protection Law", which stipulates that impact assessments must be conducted for providing personal information overseas. This provision can also block the long-arm jurisdiction of Europe and the United States when necessary.

Thirdly, international cooperation on cross-border data flow should be strengthened. Currently, the trend of cross-border data flow is inevitable, and no country can isolate itself from the global community. A path of cooperation for mutual benefit is the path to security. The overall national security concept is a "cooperative security concept," advocating for national security through cooperation with both state and private entities. Therefore, countries cannot implement unilateral regulations on cross-border data flow, but should also participate in negotiations and cooperation on bilateral and multilateral cross-border data agreements at the international level. However, China currently lacks effective international cooperation mechanisms, with low international participation and influence. Therefore, China should actively participate in bilateral or multilateral dialogues on cross-border data flow, promote consensus among countries on cross-border data flow governance through bilateral or multilateral cooperation mechanisms, and thereby enhance the interoperability of cross-border data flow.

5 Conclusion

While promoting global economic development, cross-border data flow also poses severe challenges to privacy protection, data security, and national sovereignty. Countries have to balance different values such as national security, data sovereignty, digital economy development, and personal data privacy protection, and implement cross-border data flow governance rules according to their own preferences. After years of development, Europe and the United States have gradually formed two dominant patterns and led the rules and camps of global cross-border data flow governance with advanced governance experience, providing positive reference for China to improve its cross-border data flow governance rules. In the future, China should be based on the overall national security concept, take "coordinating the relationship between development and security" as the starting point and end result of cross-border data flow governance, and focus on advocating the orderly flow of cross-border data on the basis of maintaining national security, data sovereignty, and personal privacy security.

About the Author

Jing Lin, Juris Doctor, specializing in constitutional and administrative law, as well as human rights law.

References

[1] Yan Feng, Pan Feifei, Song Jinjin, et al.: "The 'Safe Harbor' Incident Reflects the National Cross-Border Data Management Game", China Information Security, 2016, Issue 3, pp. 64-65.

[2] Cao Wei: "Strategic Gaming after GDPR", China Information Security, 2018, Issue 6, P. 13.

[3] Chen Bing and Xu Wen, "Construction of a Governance System for Cross-Border Data Flows", Studies on Socialism with Chinese Characteristics, 2021, Issue 4, pp. 68-71.

[4] Deng Song, Huang Lan, Ma Botao: "A Comparative Study on Data Cross-Border Management Based on Data Sovereignty", Journal of Information Science, 2021, Issue 6,p120-123.

[5] Song Jingjing and Wu Jianhua: "Research on the Strategies for Addressing Data Cross-Border Governance in China", Library and Information Service, 2022, Issue 3,p.129.

[6] Sun Pengpeng: "Comparative Study on the Regulation and Security of Cross-Border Data Flow", Journal of China Academy of Electronic Science, 2023, Issue 1,p.91.

[7] Wen Ming and Tan Rong: "Regulatory Cooperation on Cross border Data Flow from the Perspective of Data Sovereignty and China's Response", International Trade, 2024, Issue 6, p. 7.

[8] Zhang Qianwen: "Regulation of International Investment Agreement Exception Provisions on Cross border Data Flow", Law Journal,2021, Issue 5, p. 99.

[9] Xie Zhuojun and Yang Shudong: "Regulation of Cross-Border Data Flows in Global Governance and China's Participation - A Comparative Analysis Based on the WTO, CPTPP, and RCEP", International Observations, 2021, Issue 5, p. 105.

[10] Wei Yuan shan: "Research on Issues and Countermeasures of Cross-border Data Flow from the Perspective of Game Theory", Journal of Xi'an Jiaotong University (Social Sciences Edition), 2021,Issue 5, P.120.

[11] Wang Yan: "National Models and Reflections on Cross border Data Flow Governance", International Economic and Trade Exploration,2022, Issue 1, p. 102.

[12] Guo Xue jiao and Gao Tian shu: "Data Cross-Border Flow: Realistic Dilemmas and Solutions", Southern Finance, 2024, Issue 4, P. 80.

[13] Ran Cong jing, Chen Gui rong, and Wang Huan: "Research on the Jurisdictional Model of Cross-Border Data Flow in the United States and Its Implications for China", 2020, Issue 6, p. 140.

[14] Cui Jing: "Experience and Practices of Regulating Cross-Border Data Flow in Europe and the United States and China's Strategic Choices", "Economic System Reform", 2021, Issue 2, P. 175.