ISSN: 2688-9323

Challenges and Responses to China's Participation in Cross-border Data Flows

Xu Wang

School of Law, Anhui University of Finance and Economics, Bengbu, China

Abstract

With the upgrading of Internet technology, the demand for cross-border data flow continues to increase. The importance of cross-border data flow in international trade is becoming increasingly prominent, and all countries are actively regulating cross-border data, on the one hand, to maintain a good international economic order, on the other hand, to achieve a leading position in the formulation of cross-border data flow rules, so as to determine their own dominant position. China's legislation on data started relatively late. There are many problems, such as the dilemma of cross-border data flow, the obstacle of the adequacy of the domestic regulatory legal system on cross-border data flow, and the exclusion and intervention of developed members on China's participation in the international rules on cross-border data flow. It should start from promoting legitimate and controllable cross-border data flow, conducting type supervision based on risk concerns, coordinating the rule of law within and outside the region to promote institutional compatibility, and building the Chinese path under the dimension of trust, which will provide a better plan for China's participation in cross-border data flow, and provide a Chinese plan and choice for the formulation of cross-border data rules.

Keywords

Cross-border Data Flow; Global Governance; Digital Trade; Data Security; Data Localization.

1. China's Legislative Status

All manuscripts must be in English, also the table and figure texts, otherwise we cannot China's regulation of cross-border data flows began with the Cybersecurity Law in 2017. Article 8 of the law clearly stipulates that the national cyberspace administration, The State Council's telecommunications authority, the public security department and other organs are jointly responsible for supervising cybersecurity issues in the network within their respective responsibilities.

The Data Security Law, which has been in effect since 2021, provides a clear definition of data from a legal perspective for the first time. The first sentence of Article 2 of the law states: "For the purposes of this Law, data means any record of information electronically or otherwise." In addition, Article 36 stipulates that no organization or individual in China may provide data stored in China to foreign judicial or law enforcement agencies without the approval of our regulatory authorities. For operators of critical information infrastructure and other data processors, Article 31 stipulates security assessment requirements for data leaving the country, and points out that the regulation methods for the cross-border flow of important data processed by the latter will be dealt with by the national Internetand information authorities to formulate normative documents separately.

The Personal Information Protection Law, which came into effect in the same year, focuses on the field of personal information protection and establishes a "triple path" for personal

ISSN: 2688-9323

information to leave the country, namely security assessment, certification and standard contracts. A security assessment must be carried out when the personal information processors meet certain circumstances, such as processing the personal information of more than one million people, or providing the personal information of 100,000 people or sensitive personal information of 10,000 people to overseas countries. For sensitive personal information to leave the country, individual consent must be obtained to fully protect individuals' right to know and decide on the cross-border flow of their information.

On March 22, 2024, the Cyberspace Administration of China (CAC) issued the Regulations on Promoting and Regulating Cross-border Data Flows, which broadened the scope of security assessment for data leaving the country. For example, exemptions from declaration include cross-border shopping, delivery and payment, which shows that the policy is dynamically adjusting to balance security and convenience. In addition, the Measures for the Management of Compliance Audit of Personal Information Protection, issued on March 31, 2025, further strengthened the supervision of personal information protection.

China has formed a legal regulatory framework based on the Cybersecurity Law, the Data Security Law and the Personal Information Protection Law to manage cross-border data flows. The framework divides the types of cross-border data flows that need to be regulated into personal information and important data. For specific industries, the competent authorities of their supervision make specific provisions through departmental rules such as "management measures", "management regulations" and "management rules".[1]

2. The Dilemma of Cross-border Data Flow

2.1. Disadvantages of Cross-border Data Flow

The sharing and circulation of data not only bring huge economic and social benefits, but also pose an unprecedented threat to national security. Especially with the expansion of data space and the progress of technology, the cross-border flow of data is becoming more and more frequent, and the data security problem is becoming more and more prominent. The continuous emergence of cyber attacks and hacker attacks directly affect the country's critical information and infrastructure. Various risks in the data space are highly amplified and transboundary, which is easy to generate systemic risks.

Due to the different information carried by the data, the degree of harm such as leakage is not the same, but on the whole, they pose a certain threat to our national security. For example, in order to seize market share, a large number of domestic Internet platforms have listed in the United States; The US requires foreign companies to disclose the data they store and use in a timely manner. Such platforms have the characteristics of large coverage and complex content,and the deep data among them is related to important national infrastructure, which can truly reflect the actual situation of China. Many of these data are important information related to China's important facilities and regions, if obtained by relevant foreign departments, illegal analysis and use, posing a huge threat to national security. With the rapid development of information technology, hacker attacks emerge in an endless stream, illegal data, sensitive personal data leakage and illegal transactions and other behaviors, is not only a violation of personal privacy, but also a violation of the legitimate interests of China's enterprises, a violation of China's data sovereignty, is also unfavorable to China's social stability.

2.2. The Defects of Digital Regulation

First of all, data itself has great economic value. All industries can understand the existing problems and needs in the current industry through data collection and analysis, and make appropriate decisions accordingly to maximize their own benefits and reduce their own losses. Whether it comes from individuals, enterprises or government entities, different data platforms

ISSN: 2688-9323

will collect and store data based on different economic objectives, and process and utilize data through special data analysis technologies. For example, online shopping applications such as Yibao can collect users' location information, browsing product information and historical shopping data, so as to analyze consumers' potential consumption desire and purchasing power level, and then form personalized push and put it on the application home page to improve consumers' consumption possibility and increase the flow of specific stores and products. In the Internet environment, most of the data is in the process of sharing and circulation, which is also the process of using and adding value to data. The pursuit of data value by data processing program is the demand of data circulation, and the process of data flow, collection, processing and use will promote the further development of data technology.

At present, in the face of unprecedented data security risks and the adverse effects that illegal use of data may cause, our country still controls them by localized means. The so-called "data localization" is a mandatory protection measure, which is stipulated by the governments of each country, and all data collected in their territory must be managed by the state. The implementation of a strict cross-border data flow guarantee mechanism for databases stored in China will inevitably affect the data flow and the development of the digital economy, and it is difficult to balance the interests of the two. In order to ensure data security and national security, it is necessary to regulate the cross-border flow of data to protect the security and use of data in the process of cross-border flow. Data localization is an important means to safeguard national data sovereignty, guard against transnational data risks and combat cybercrimes. However, the practice of data localization will cause certain restrictions on the free flow of data, which will not only lead to the expansion of the information gap, but also have an adverse impact on the domestic data market, and then have an adverse impact on the development of China's data technology.

Therefore, the cross-border flow of data requires not only the establishment of a sound data security protection mechanism to regulate the flow and guarantee the security, but also the adoption of flexible means to ensure the necessary degree of freedom of data flow. Under the background that countries all over the world are competing to improve data protection systems, seize data resources and build digital markets, how to balance the two activities of data flow and data protection is an urgent issue for us to consider.

3. Obstacles to the Adequacy of the Domestic Legal System for the Supervision of Cross-border Data Flow

3.1. The Domestic Legal System for Cross-border Data Flows is Compatible with International Rules

With the development of the digital economy, digital trade is bound to be affected by domestic legal systems and regulatory policies related to the digital field, and a country's legal system is an important factor in its participation in national activities. From the perspective of the issue of cross-border data flow, China's current trade agreement text and domestic legal system of cross-border data flow do not have the strength to fully implement higher standards of rules, and the new international digital trade rules and standards are likely to exceed the acceptable reality of China's existing legal system.[2]

With the development of China's digital economy, a legal system framework for cross-border data flows has emerged. First, the regulatory requirements for cross-border data flows have been clarified, and restrictions have been placed on cross-border data flows in specific industries and fields. Second, it establishes the basic principles for China's cross-border data flow. The Cybersecurity Law, adopted in November 2016, stipulates that personal information and important data collected and generated by operators of critical information infrastructure while operating within China should, in principle, be stored within China. If it is necessary to

ISSN: 2688-9323

provide data overseas, security assessments will be carried out in accordance with relevant laws and regulations. Third, China has improved its legal system for cross-border data flow, but there are still compatibility problems with high-level digital trade agreements such as CPTPP and DEPA.

3.2. There are Inconsistent Regulations on Cross-border Data Flow between Domestic Legislation

There are legal contradictions and coordination between the outbound country and the outbound country in data protection and cross-border supervision, which puts higher requirements on China's legal system. However, judging from China's existing legislation, laws at all levels in China have different norms for the cross-border flow of data. The "Data Security Law" and "Personal Information Protection Law" have been promulgated and implemented successively, providing a clear foundation for the cross-border flow of data. However, the existing regulatory rules in the industrial field have not been amended in a timely manner, which objectively leads to the contradiction between legal provisions and regulations and departmental rules. For example, important data and personal information can be provided cross-border under conditions such as security assessment and standard contracts, and certain types of data are not completely prohibited from leaving the country. However, some industries or fields adopt a one-size-fits-all model, completely prohibiting certain types of data from leaving the country.

3.3. China's Regulatory Capacity and Level of Security Protection are Facing a Major Test

The movement of data across borders has a natural global character, breaking traditional physical borders and national jurisdiction, but at the same time, high-standard cross-border data flows will also pose new challenges to countries with relatively weak protection capabilities. At present, China's regulation of cross-border data flows, as well as its guarantee of cyber security, is a serious challenge.

First, high-standard cross-border data flow rules have higher requirements for supervision. Beyond economic considerations, countries that advocate free data flows, led by America, are confident that they can manage their own cross-border flows. There are a large number of Internet companies in the United States, which has a natural advantage in data storage and management. Data from all over the world flow to these Internet companies continuously, so the United States does not need to consider the problem of data outbound. In addition, the US government has decentralized, hidden but effective control over the cross-border flow of data in key sectors, industries and fields. [3]Regulations in China are relatively weak compared to those in developed countries.

Second, when the relevant domestic legal system and data flow supervision are not mature, forcing the acceptance of the free flow of data clauses is highly likely to cause threats in the data field. On the one hand, the free flow of data is extremely unfavorable to the development of our country's digital industry. If data is allowed to flow freely, opportunities for domestic enterprises to develop and use it will be harmed, thus weakening their competitiveness in the digital economy. At the sametime, the flow of large amounts of data across borders also poses huge risks to national security, including data security issues. With the integration and development of the Internet with all aspects of economy and society, data of People's Daily life, work, life, work, life and other aspects are widely saved and stored, and the cross-border flow of these data is directly related to the safety of people's lives and property, as well as the political and economic security of a country. Without effective control, it is easy to lead to transnational network attacks, user information leakage, and terrorist information diffusion, which brings severe challenges to China's network information security.

ISSN: 2688-9323

4. The Exclusion and Interference of China's Participation in International Rules on Cross-border Data Flow by Developed Members

4.1. Promoting the Establishment of Regional Interoperability Mechanisms among Developed Members that Exclude China

In terms of the development trend of cross-border data flow, due to the slow free flow of data under multilateral frameworks, developed countries such as the United States, the European Union, Japan and the Republic of Korea have begun to explore new cooperation models and build cross-border data flow mechanisms thatfacilitate advanced economies to participate more, while excluding China and other developing countries. To form a transnational data flow network with developed countries as the center.

The US and the EU have differences in data protection, but the two sides have held many consultations and tried to establish a cross-border cooperation mechanism. Moreover, the differences between the two sides are about the path of personal data protection, which will not substantively affect the cross-border data flow activities of the two sides. The United States and the European Union, as data powers, have adopted various measures to continuously enhance their voice in the field of cross-border data flow, with the aim of increasing the scope of cross-border data flow cooperation to enhance their voice in the field of cross-border data flow, so as to build international rules in line with their national interests. Because of its particularity, the EU can reach restrictions on those countries that rely on the development of the EU, and require them to meet the high standards of the EU, so as to expand the scope of cooperation in the cross-border flow of data. The United States is more inclined to use the rules of the agreement, such as using the United States-Mexico-Canada Agreement (USMCA) to hold contracting States hostage to its own rules on cross-border data flows.

4.2. Interference by the United States and its Allies with China's Participation in Rules Governing Cross-border Data Flows

In the traditional international economy and trade, the US government attaches great importance to the use of international rules to pressure and intervene in China. [4]At the same time, member states led by the United States intentionally isolate and interfere with China's participation in international economic and trade activities. Although Article 15 of the Protocol on China's Accession to the WTO explicitly requires the termination of the "surrogate country" practice after December 2016, the US continues to use third-country costs to calculate the normal value of Chinese products in anti-dumping investigations on the grounds of "government interference in the market". For example, the launch of the fifth anti-dumping sunset review on Chinese persulfate in 2024 still used India as the surrogate country, resulting in an overestimation of the dumping margin by more than 300 percent. China won the DS515 case, but the US refused to implement it on the grounds that "domestic law takes precedence", exposing the nature of its instrumentalization of WTO rules.

5. China's Response to Rules on Cross-border Data Flows

5.1. Promoting Proper and Controllable Cross-border Data Flows

From the point of view that data flows facilitate trade flows, it seems that the free flow of data should be promoted unconditionally. From the point of view that data flows facilitate trade flows, it seems that the free flow of data should be promoted unconditionally. However, just as there are exceptions to free trade, data flows also need to be regulated. Due to non-economic considerations such asnational security, privacy protection and sovereign jurisdiction, countries have different ways of regulating the flow of data across borders, so the flow of data around the world is not entirely free from restrictions. In this context, it is based on this concern

ISSN: 2688-9323

that China has put forward the concept of cross-border "secure flow". It should be pointed out that traditional data security can no longer meet the needs of data development, including data utilization security, which emphasizes the legitimacy and controllability of large-scale data flow and utilization in the era of digital economy. [5]However, the understanding of "data security" from outside the region is more like an excuse for "pan-security", which easily leads to the misunderstanding from outside the region that China creates obstacles and barriers on the grounds of "security". Therefore, in order to avoid misunderstanding, "legitimate controllable flow" should be replaced by "secure flow" in the literal sense, so as to promote the understanding and application of "legitimate controllable flow" on a global scale. Compared with the 2019 G20 Osaka Declaration on Digital Economy on "trust-based cross-border data flows", "proper and controlled data flows across borders" emphasizes objectivity and inclusiveness.[6]

5.2. Type-based Supervision based on Risk Concerns

Manageable cross-border data flows emphasize the controllability of risks, which requires a risk-based regulatory approach. Risk control is generally considered to include four strategies: accepting risk, avoiding risk, controlling risk and transferring risk. No matter what kind of strategy and regulation can achieve absolute security, so the development of cross-border data flow rules must accept the existence of risks, which is why the relationship between security and development is coordinated. From this perspective, both the Clean Net Initiative in the United States and extreme data nationalism in India are irrational measures driven by the pursuit of data security. The governance of cross-border flows of global data is actually about achieving relative common security through multilateral cooperation.

Risk-based regulation requires classification of different control methods. On the types of controls, we propose to take into account, in addition to the classification of types of data, the issue of controlling the movement of data across the boundary should also be considered comprehensively. The OECD summarizes the four basic types of controls on cross-border data flows: no control, post-hoc accountability, conditional on safeguards and conditional on specific authorization, forming a "gradual spectrum" of controls from weak to strong. [7]For different types of cross-border data flows, we should choose appropriate ways in the regulatory spectrum to cooperate with each other, and establish a pre-event, in-event and post-event regulatory system. While preventing a "one-size-fits-all" approach to prior regulation, we should also avoid undue obstacles to data flows. Therefore, we need to differentiate on a case-by-case basis and adopt appropriate regulatory measures to ensure the legal, secure and controllable cross-border flow of data.

5.3. Coordinate the Rule of Law at Home and Abroad to Promote Institutional Compatibility

Cross-border data flows include both "outbound" and "inbound" flows, so they involve both domestic and international law. Countries differ in national conditions, culture and history, as well as in their perceptions of cross-border data flow rules, but they all pay close attention to national security, protection of private rights and sovereign jurisdiction. In addressing these common concerns, countries should seek common ground while reserving differences and learn from each other's experience in data governance.

There is no universally applicable regulatory model, even for the same concerns. When countries have different institutional designs on the same issue, institutional compatibility should be promoted as far as possible. Promoting institutional compatibility can be divided into two types: First, there is consensus on specific systems, and common rules can be reached through consultation, such as bilateral agreements on judicial law enforcement data access; Second, if there is consensus only at the value level, it should be realistic to admit that it is not

ISSN: 2688-9323

possible to achieve compatibility at the system level, but it can maintain consultation and dialogue on common concerns, such as discussions on national security data. Therefore, it is particularly important to design a compatible framework for global regulation of cross-border data flows. Such a framework should be based on common concerns, reflect the consensus on values, integrate the consensus on basic principles, and guide the discussion towards institutional consensus.

5.4. Building a China Path from an Institutional Perspective

Although in the field of digital technology and digital trade market, China still has some room to improve its position as a "great power", but in the scale of digital economy, China has grown into a big country comparable to the United States. In view of this, it is necessary for China to carry out in-depth exchanges and discussions with target countries on the key issues of cross-border data flow, so as to lay a solid foundation for the subsequent consensus on cross-border data flow regulation, data cooperation and data sharing. In addition, countries' economic dependence on China is far less than that of the United States, which directly affects China's right to speak in participating in cross-border data flows. The stronger the persuasive, influential and authoritative power of data discourse, the easier it is to form special trust and occupy an important strategic position in the digital game. [8]China should open its domestic market in an orderly way in the future to promote other countries' exchanges and cooperation on China's digital economy. At the same time, we need to step up efforts to build regional cooperation to achieve the goal of mutual benefit and win-win results. In terms of institutional building, we need to fully consider the needs of countries for cross-border data flows, and on this basis, with interests as the bond, provide mutually beneficial suggestions and programs for our cooperation partners.

First, in order to promote the development of digital economy and enhance mutual trust among countries, it is necessary to weaken the restrictions on data flowimposed by local data storage. An institutional framework should be put in place to enable the secure and orderly flow of local data. In bilateral and regional cooperation, consensus should be reached on a system of cross-border data rules, and in-depth coordination should be made on security assessment standards, cross-border access routes and data access routes, so as to reduce the risk of data leaving the country and enhance trust and interoperability among countries. Optimizing data localization measures can stimulate the free flow of data and boost regional economic development.

Second, we need to strengthen the institutional framework for cross-border data flows in key areas and enhance trust among countries in accordance with the principle of reciprocity. Cooperation between governments and small and medium-sized enterprises is a new breakthrough. DEPA and the EU Data Act focus on the interests of smes and advocate collaboration. In the digital age, data governance has become increasingly critical for businesses, with cross-border compliance costs higher for smes, and emerging network and technology companies, most of which are smes, in urgent need of government support. DEPA is more focused than other digital trade rules on creating opportunities for smes. The Chinese Ministry of Commerce official said that China is in consultation with DEPA signatories to strengthen cooperation in the digital economy. The cooperation between the government and small and medium-sized enterprises has become a new demand for the development of digital trade. Through multi-party coordination, countries can enhance mutual trust and ensure cross-border data flow, cooperation and sharing, which will help China to enhance its voice in the international digital game and promote the formation of unified rules for cross-border data flow.

ISSN: 2688-9323

6. Conclusion

Data cross-border flow, as a core issue in the digital economy era, is both a key driver of global value chain restructuring and an important intersection of national sovereignty, security, and development interests. China faces complex internal and external challenges in governing data cross-border flow: internally, it needs to balance the tension between data security protection and digital economic development, resolve the compatibility issues between legal systems and international rules, and enhance regulatory capabilities to address the global nature of data cross-border flow; externally, it confronts rule exclusion and intervention led by developed countries, with regional interoperability mechanisms increasing the risk of marginalization for China.

After years of exploration, China has established a legal regulatory framework centered on the "three laws." Through institutional designs such as categorized supervision, safety assessments, and standard contracts, it has initially achieved "safe and controllable" cross-border data flow. However, in the face of the high-standard evolution of digital trade rules, China needs to deepen reforms from three aspects: innovation in concepts, institutional compatibility, and international cooperation. It should replace traditional security narratives with "legitimate and controllable flows" to enhance the international community's understanding of China's governance logic; break through the "one-size-fits-all" dilemma by implementing tiered risk-based regulation, promoting alignment between domestic rules and international mechanisms like the CPTPP and DEPA; and rely on the "Belt and Road" initiative and regional cooperation platforms to build an inclusive and mutually beneficial institutional framework, enhancing China's voice in data governance.

In the future, China should position itself as a major player in the digital economy. While upholding national security, it should engage with an open attitude in the construction of global rules. By fostering institutional innovation and international collaboration, China can develop a solution that emphasizes both development and security. This not only helps break the deadlock in cross-border data governance but also contributes to a new paradigm for global digital economy governance that balances efficiency and equity. It will promote the formation of a new order for cross-border data flows based on trust and supported by rules.

References

[1] S.Zheng:The regulation path and optimization of cross-border data flow in China(MS.,Jilin University,China 2023), p.10.

[2] B.He:China's challenges and responses to international rules governing cross-border data flows,Administrative Law Review, Vol.7(2022)No.4,p89-103.

[3] M.N.Zhang:We will accelerate the improvement of China's overall data security governance capacity,Social Governance Review,Vol.5(2020,)No.2,p81-85.

[4] P.Qi:Legal regulation of "Belt and Road" cross-border data transmission under the background of digital economy,Law Review,Vol.40(2022)No.6,p165-179.

[5] J.R.Liu:Data security paradigm innovation and its legislation,Global Law Review, Vol.43 (2021) No.1,p5-21.

[6] Y.Sun:Study on the legal regulation of national security risk of data exit in China(MS.,Jilin University,China 2024), p.25.

[7] J.R.Liu:Towards a global regulation of cross-border flows of data,Administrative Law Review,Vol.8 (2022)No.4,p73-88.

[8] X.H.Lu:Data discourse power: the focus of strategic competition in international communication, Modern Communication(Journal of Communication University of China),Vol.42 (2020)No.10,p1-6.