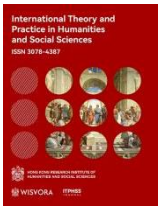
WISVORA

International Theory and Practice in Humanities and Social Sciences
2024 Volume1,Issue1 ISSN 3078-4387



The Regulatory Framework, Practical Challenges, and Solution Pathways for Cross-Border Data Flow

YaJun Wan
School of Law, Anhui University of Finance & Economics, Anhui Bengbu 233041, China

Accepted
2025-03-18
Keywords
Religious Pluralism;
Dai People; Theravada Buddhism;
Bai Pala Ritual; Individual Belief;
Agency
Corresponding Author
YaJun Wan

http://doi.org/10.70693/itphss.v2i5.252

Abstract
To date, the global community has yet to establish a unified and widely acknowledged framework for data flow standards. Given the role of cross-border data flow in advancing globalization, this study examines the collaborative governance approach to cross-border data flow in China, aiming to offer insights that can enhance the efficiency of such governance in the country. By comparing and analyzing the regulatory models employed by the United States, the European Union, and China in the formulation of cross-border data flow regulations, this paper suggests practical revisions to the rules of each jurisdiction. Furthermore, it outlines a pathway to alleviate the challenges associated with the collaborative governance of cross-border data flow in China, by addressing the existing dilemmas. The paper recommends several concrete measures to ensure the mutual protection of sovereignty and data security through enhanced multilateral agreements, to develop comprehensive cross-border data regulations via the establishment of pertinent international legal frameworks, to facilitate seamless cross-border data flow through the widespread adoption of international data laws, and to take into account the broader implications of technological advancements in resolving cross-border data flow issues. The ultimate goal is to foster the long-term, sustainable, and healthy development of China's collaborative governance of cross-border data flow.

1. Introduction

Strengthening the construction of foreign-related rule of law and fostering a favorable legal environment for advancing reform, development, and stability are paramount tasks both now and in the future. In light of global economic integration, the Chinese government has unequivocally articulated its commitment to unwaveringly promoting a new phase of high-level openness. This commitment not only underscores China's proactive engagement and contribution to the global economy but also highlights our resolve and confidence in addressing global challenges. To realize this objective, China must delineate and enforce pertinent measures at the legal level to ensure the seamless progression of external openness(Xiang Liet al.,2025).Within this framework, the trend of cross-border data flows has gained increasing prominence and has emerged as a critical phenomenon in the evolution of the global economy. However, as cross-border data flows intensify, their governance issues have become a focal point for governments and international

organizations. Cross-border data flows entail barriers and conflicts of interest among different nations, and ensuring data security while facilitating the free flow of data has become an urgent issue that requires resolution(Jing Cheng & JingJing Dai,2024).

This study examines the cross-border flow of data, elucidates the specific challenges associated with it through a comparative analysis, contrasts the institutional frameworks of major countries such as the United States and Europe, identifies the practical obstacles to cross-border data flows in China, and analyzes the underlying causes. Subsequently, it proposes a legal optimization pathway to address the challenges of cross-border data flows, thereby contributing to the theoretical research and systemic development in the domain of cross-border data governance in China.

2. Rules and Patterns of Cross-border Data Flow

To date, the global community has yet to establish a unified data flow standard system, resulting in the cross-border data flow regulations exhibiting a decentralized nature. These regulations can be categorized into three primary models: the United States model, the European Union model, and the Chinese model. For instance, Reidenberg highlights the dual nature of regulatory approaches between the United States and Europe concerning cross-border data flows. Beyond the United States and Europe, China, as a significant player in the global digital economy, has seen its data flow regulatory framework increasingly attract domestic and international attention and scrutiny.

2.1 The United States

As a data technology power, the United States uses its technological advantages to efficiently acquire data resources on a global scale. In terms of the legal regulation of cross-border data flow, the United States has unlimited internal data flow, adopted a free flow mode, established a framework system such as the Cross-border Privacy Protection Rules, and strengthened the protection of domestic data enterprises by expanding its jurisdiction. The legal regulation features of cross-border data flow in the United States include: no internal restrictions, free flow mode, CBPR framework system and jurisdictional expansion(Yan Lu,2024).

First, adhere to the "data absolute freedom theory". This is crucial because the US has a double standard approach when it comes to data localization. Specifically, the United States has implemented extremely strict localization legislation within its own country to ensure local storage and processing of data. However, when it comes to international affairs, the United States strongly opposes the adoption of data localization policies by other countries, and advocates the free flow of data. This double standard not only violates the principle of fair competition, but also poses a challenge to the data sovereignty of other countries.

Second, it emphasizes the principle of "market dominance". The United States has long believed that market mechanisms are the best way to address the cross-border flow of data. They advocate market competition and corporate self-regulation to ensure data security and privacy protection. As a result, the U.S. government has largely avoided direct intervention in data flows, instead encouraging companies to address the challenges posed by cross-border data flows through technological innovation and self-management. This practice, while promoting the development of technology to a certain extent, can also lead to vulnerabilities in data security and privacy protection(Monika ,2022).

Third, pay attention to the principle of "technology neutrality". In developing legal regulations for cross-border flows of data, the United States tries to avoid favoring specific technologies or platforms. This approach helps maintain a level playing field in the market while encouraging

technological innovation and adoption. However, there are certain problems with the principle of technology neutrality, for example, it can lead to certain technologies or platforms dominating the market, thus weakening the market share of other competitors. Therefore, when implementing the principle of technology neutrality, we need to carefully weigh various factors to ensure the fairness of the market and the healthy development of technology.

2.2 European Union

In the EU's cross-border data flow model, in addition to setting basic principles and clarifying the rights and obligations of the parties, there is a special emphasis on high standards of data protection. In order to ensure the security and privacy of data during cross-border transfers, the European Union has put in place strict data protection regulations, such as the General Data Protection Regulation (GDPR). These regulations require that data processors and controllers must take appropriate technical and organizational measures to prevent data leakage, misuse or loss.

First, the EU has established an independent legislative mechanism to promote standards of personal data protection. The EU's GDPR does not only apply to EU member states, but also has a profound impact on businesses worldwide. Any business offering goods or services within the EU, regardless of where it is registered, must comply with the GDPR. This means that companies must ensure that their data processing activities comply with the requirements of the GDPR or face hefty fines. The implementation of GDPR has prompted companies to re-examine their data processing processes and privacy policies. Companies must ensure data transparency and security to protect individual privacy. This includes taking appropriate technical and organizational measures during data collection, storage, processing and transmission to prevent data breaches and other security incidents from occurring.

Second, the EU limits foreign access to data in the region. This policy aims to protect personal privacy and data security and prevent misuse of information by external forces. The European Commission has proposed a series of strict regulations that all businesses operating in the EU must comply with. These rules apply not only to local EU companies, but also to any foreign company that has user data in the EU. In order to ensure the effective implementation of these regulations, the EU has also set up a dedicated data protection authority responsible for monitoring and enforcing the relevant laws. The agencies have the power to impose penalties on companies that break the rules, including heavy fines and business restrictions. In addition, the EU is actively promoting data protection cooperation with other countries and regions in order to form a uniform global data protection standard. The implementation of this policy has undoubtedly brought new challenges to global technology companies. Many multinational companies have had to review their data management strategies to ensure compliance with EU requirements. At the same time, it also provides a competitive advantage for local EU companies, making them more attractive in terms of data processing and privacy protection.

3. The Realistic Dilemma of Cross-border Data Flow in China

3.1 Data Barriers Exist in Cross-border Data Flows

Data barrier is the main content of restricting the cross-border flow of data. At present, a kind of barrier based on the relationship between data and sovereignty has gradually emerged between various countries. Data barriers are mainly embodied in two conflicting legal principles - data sovereignty theory and data liberalism. The former advocates that data should be governed by national sovereignty and emphasizes the localization of data storage and processing to protect national security, public interests and citizens' privacy. The latter believe that data should flow

freely to promote global trade, innovation and economic development. The conflict between these two principles has led to the difficulty of countries to reach an agreement on the cross-border flow of data, which in turn has formed data barriers.

With the deepening of globalization, the existence of data barriers has a significant impact on international economic and technological cooperation. In order to safeguard their national interests, governments have introduced corresponding data protection regulations, such as the European Union's General Data Protection Regulation (GDPR) and China's Personal Information Protection Law (PIPL). These regulations have played a positive role in protecting personal privacy and data security, but they have also created compliance challenges for multinational corporations and international organizations. In order to cope with data barriers, multinational companies have to set up data centers in different countries to meet the local storage requirements of each country. This not only increases the operating costs of enterprises, but also may lead to the generation of data silos, affecting the integration and analysis efficiency of data. In addition, data barriers can hinder scientific cooperation and public health response, such as in epidemic prevention and control, making it more difficult for countries to share epidemic data.

In the future, with the continuous progress of technology and the deepening of international cooperation, data barriers may be gradually lowered. However, in this process, countries need to find a balance between protecting data sovereignty and promoting the free flow of data, so as to achieve a win-win situation of rational use of data and global cooperation.

3.2 Inadequate technical responses to cross-border flows of data

Technology can, to some extent, ease the dilemma of cross-border data flows. By means of encryption technology, anonymization processing and blockchain, the security and privacy of data in the cross-border transmission process can be guaranteed to a certain extent. However, technology cannot fully solve the legal and regulatory problems. Still, technology is valuable in dealing with the dilemma of cross-border data flows. For example, the adoption of end-to-end encryption technology can ensure that the data is not intercepted and read by unauthorized third parties during transmission, thus protecting the confidentiality of the data to a large extent. In addition, data anonymization processing technology ensures personal privacy to a certain extent by removing or replacing personally identifiable information, making it difficult to trace data back to specific individuals during cross-border transmission and use. The introduction of blockchain technology has also brought new solutions for the cross-border flow of data. The distributed ledger features of blockchain can ensure the immutability and transparency of data, thereby enhancing the trust of cross-border data transmission to a certain extent. Through smart contracts, the automated management of cross-border data transfers can be achieved, ensuring that the data complies with established rules and protocols during transmission.

Technology, however, is not the master key. The legal and regulatory issues of cross-border data flows involve national sovereignty, data protection regulations, international treaties and other levels. For example, different countries have different requirements for data protection, which makes it a complex legal environment for businesses to conduct cross-border data transfers. In addition, the technical means themselves may also be vulnerable and need to be constantly updated and upgraded to deal with increasingly complex security threats. Therefore, technology and legal regulation need to work together to address the challenges of cross-border data flows. On the one hand, technological means should continue to advance to adapt to changing security needs; On the other hand, countries should strengthen cooperation and promote the development of uniform or compatible data protection standards to reduce legal barriers to cross-border data flows. Only in this way can we promote the healthy development of the global digital economy while safeguarding data security and privacy.

3.3 Rules on Cross-border Data Flows are Costly to Conclude

Digital trade issues involve multiple governance mechanisms, such as multilateral, regional, transnational and inter-governmental cooperation. The diversification of data storage, ease of transmission and fragmentation of service subcontracting lead to the problem of multiple jurisdictions. A piece of data may be governed by the laws of the place where it is stored, the place where it is transmitted, and the country of nationality of the owner. In the absence of a unified international system or coordination mechanism, countries propose data governance programs that suit their national interests for national security and surveillance purposes. This situation makes multinational enterprises face many challenges when carrying out digital trade. Companies must not only deal with the laws and regulations of different countries, but also ensure that the cross-border transfer of data complies with the privacy protection and data security requirements of each country. To address these challenges, companies have to invest significant resources in compliance reviews and risk assessments to avoid potential legal disputes and financial losses. At the same time, international organizations and multilateral institutions are working to promote a global governance framework for digital trade. For example, the World Trade Organization (WTO) and the Digital Economy Working Group are exploring ways to develop uniform rules and standards in the area of digital trade. However, due to the differences in the interests of various countries and the complexity of the negotiation process, there are still many difficulties in reaching consensus.

At the regional level, several groups of countries have begun to develop their own rules for digital trade. For example, the Asia-Pacific Economic Cooperation (APEC) Cross-border Privacy Rules (CBPR) system aims to provide a common framework for data flows in the Asia-Pacific region. However, these regional rules are often difficult to cover the global scope, and there may be conflicts between different regional rules. Transnational and inter-governmental cooperation provides a possible way to solve these problems. Through bilateral or multilateral cooperation, countries can reach consensus in specific areas, such as fighting cybercrime, protecting intellectual property rights, and promoting data security. However, such cooperation often requires countries to make a certain compromise on their interests, and in the process of implementation, there may be problems of different implementation intensity. In the context of increasingly prominent multi-jurisdictional issues, the establishment of an international unified data governance mechanism is particularly urgent. This requires the concerted efforts of governments, international organizations, enterprises and all sectors of society to gradually form a fair, transparent and operational global digital trade governance framework through dialogue and consultation. Only in this way can we provide a solid institutional guarantee for the healthy development of digital trade.

4. Analysis of the Causes of the Difficulties of Cross-border Data Flow

The formation of legal regulatory barriers to cross-border data flow is caused by many factors. Under the influence of the international political and economic pattern, various countries and regions have adopted different attitudes and positions on the new production factor of data, which are reflected in the legislation of various countries and regions, and eventually lead to the conflict of legal regulations on cross-border data flow.

4.1 International Environmental Reasons

International environmental reasons: Differences in the positions of different countries and regions aggravate the formation of barriers

In the international environment, the difference of political and economic interests is an

important factor that leads to the formation of legal barriers to cross-border data flow. First, countries differ in their considerations of data sovereignty and national security. Some countries see data as an important strategic resource for their countries and are concerned that cross-border flows of data could threaten national security and sovereignty. Therefore, these countries restrict the flow of data through strict legal regulations to ensure the control and protection of data within the country.

Secondly, the tendency of the international political and economic landscape to become camp has led countries to adopt different strategies in terms of data governance. Taking the United States and the European Union as examples, the United States is relatively open in terms of cross-border data flow, emphasizing market freedom and technological innovation, while the European Union is more focused on personal privacy and data protection, and has enacted strict data protection regulations. This difference in stance has led to conflicts between the two sides on the legal regulation of cross-border data flow, which has brought obstacles to the global data flow. In addition, there are significant differences between the positions of developing and developed countries on data governance. Developing countries often lack sound legal systems and technical capacity to deal with the challenges posed by cross-border data flows, and therefore tend to adopt more conservative regulatory measures. However, developed countries pay more attention to the free flow and commercial use of data, which further intensifies the legal regulatory barriers to cross-border data flow.

4.2 Value Factor Reason

The cross-border flow of data faces many obstacles, one of which is the rise and establishment of the concept of data sovereignty in the context of the digital age. The concept of data sovereignty asserts that each country has full control and jurisdiction over the data within its territory. With the rapid progress of information technology, data has evolved into a resource with great economic value and strategic significance. Therefore, countries have adopted legislative means to safeguard their own data sovereignty and ensure that the collection, processing and use of data comply with national laws, regulations and policy guidance. This emphasis on the principle of sovereignty has made the legal regulation of cross-border data flows more complex and stringent.

At the same time, the emphasis on data security is increasing globally. With the frequent occurrence of data breaches and cyber attacks, governments and the public are increasingly concerned about data security. In order to protect personal privacy and corporate confidentiality, many countries have enacted strict data protection regulations that require specific security standards to be met when data flows across borders. This not only increases the legal costs of cross-border data flows, but can also lead to delays or disruptions in data flows. In addition, the issue of data security has also attracted the attention of international organizations, which have issued a series of guidance documents and standards to regulate the security of global data flows. In order to comply with these regulations, enterprises have to invest significant resources in technology upgrades and personnel training to ensure security during data processing and transmission. At the same time, public awareness of data privacy is also increasing, and more and more people are concerned about whether their personal information is properly protected. This heightened focus on data security has not only driven the development of related technologies, but also prompted companies and governments to adopt more rigorous and responsible measures in data management.

4.3 Legislative Reasons

In the context of today's globalization, the cross-border flow of data has become an important part of exchanges and cooperation between countries and regions. However, due to the significant

differences in the legal rules of countries and regions in the regulation of cross-border data flow, and even contradictions and conflicts in some cases, this has become an important reason for the construction of legal barriers to cross-border data flow. From a global perspective, the current rule system regulating cross-border data flow is mainly represented by the United States, the European Union and China, and the legal regulation system of these three countries and regions affects the legal environment of global cross-border data flow to a large extent.

In the process of cross-border data flow, enterprises or individuals often face complex issues of legal application and jurisdiction, which become the key factors of legal regulatory barriers. The main points of contention include differences in the scope of applicable laws in different countries and regions, which have led to uncertainty in the application of laws for cross-border data flows. For example, the laws of some countries only apply to data within their borders, which means that the laws of these countries are only valid for data generated within their territory. Other countries require their laws to apply to citizen or corporate data worldwide, regardless of whether it is generated or stored within their borders. This difference makes it extremely difficult for companies to process cross-border data because they have to operate under different countries' legal frameworks, which not only increases compliance costs, but can also lead to legal risks. In addition, jurisdictional disputes are an important issue. When cross-border data flows involve multiple countries, there may be situations where multiple countries all claim jurisdiction over the data. In such cases, companies need to determine which country's laws have priority over their data flows, which is complex and challenging. Differences in legal systems and enforcement in different countries make it difficult for companies to grasp the boundaries of compliance in cross-border data flows, increasing legal risks and operational costs. Therefore, resolving these disputes over the application of law and jurisdiction is of great significance for breaking down legal regulatory barriers to cross-border data flows.

5. The Legal Solution to the Dilemma of Cross-border Data Flow

5.1 Closer International Cooperation to Ensure the Two-way Security of Sovereignty and Data

Due to the significant differences in the understanding of data sovereignty in different countries and regions, this difference has led to the establishment of various barriers in the cross-border flow of data, which further aggravates the dilemma of cross-border data flow. Differences in national laws on data protection and privacy have created many challenges for cross-border data flows. To combat this problem, countries need to strengthen international cooperation and work together to develop uniform data protection standards and rules. Through international organizations and multilateral agreements, countries can reach consensus on cross-border data flows, ensuring two-way protection of data sovereignty and data security. In this way, countries can work together to promote the healthy development of cross-border data flows while respecting each other's data sovereignty, while ensuring that data security and privacy are adequately protected. While strengthening international cooperation, governments and enterprises should also actively take measures to address the challenges of cross-border data flows. First, governments can develop clearer and more flexible policies on cross-border data flows to adapt to the rapidly evolving digital economy. These policies should take full account of legal differences in different countries and regions, while providing clear guidance and guarantees for domestic enterprises.

Enterprises should strengthen their data governance capabilities to ensure compliance with national laws and regulations in the process of cross-border data flow. Enterprises can establish a

multinational data compliance team to research and interpret data protection laws in different countries, so as to develop a data management strategy that meets the requirements of each country. In addition, companies can adopt advanced data encryption technology and access control measures to ensure the security and privacy of data during cross-border transmission. At the technical level, countries can jointly promote the research and development of technical standards and solutions for cross-border data flows. For example, by establishing uniform data formats and interface standards, technical barriers to cross-border data flows can be lowered. At the same time, countries can jointly invest in research and development of data security technologies to counter increasingly sophisticated cybersecurity threats. Education and training are also important aspects of addressing the challenges of cross-border data flows. States should strengthen education and training in data protection and privacy protection to raise public and professional awareness of data sovereignty and data security. Through international seminars, training courses and academic exchanges, countries can share best practices and experiences to improve the overall level of data protection worldwide.

5.2 Establish Systematic Data Cross-border Rules by Constructing Relevant International Law Systems

In terms of legislation, due to the fragmentation of rules and the lack of international uniform rules, the legal rules of various countries and regions on the regulation of cross-border data flow are different, resulting in the current cross-border data flow. In short, to deal with the challenges of cross-border data flow requires the joint efforts of governments, enterprises and international organizations. By strengthening international cooperation, developing unified data protection standards and rules, strengthening data governance capacity, promoting research and development of technical standards and solutions, and strengthening education and training, countries can jointly promote the healthy development of cross-border data flows on the basis of respecting each other's data sovereignty, and ensure that data security and privacy are fully protected.

There are many differences in the regulatory system. For example, the European Union has set strict data protection standards through the General Data Protection Regulation (GDPR), which requires businesses that process personal data within the EU to comply with a number of regulations, including data minimization, data portability rights, and data subject consent. In the United States, there is no national data protection law, and states have different data protection regulations based on their own circumstances, such as California's Consumer Privacy Act (CCPA). This discrepancy leads to complex compliance challenges for businesses when conducting cross-border data flows. To address this challenge, enterprises need to build flexible data governance architectures that can adapt to the legal requirements of different countries and regions. At the same time, enterprises also need to strengthen internal data protection measures to ensure the security of data during transmission and storage.

In addition, technological solutions are evolving to address the challenges of cross-border data flows. For example, blockchain technology can provide a decentralized way of managing data, ensuring that data is transparent and immutable. Encryption technology can protect the confidentiality and integrity of data in the process of data transmission. In terms of education and training, countries need to increase public awareness of data protection and privacy protection, and improve the understanding and compliance of businesses and individuals with rules on cross-border data flows. Through regular training and publicity, the whole society can increase the importance of data security and privacy protection. In short, the challenges of cross-border data flow are multifaceted and require governments, enterprises and international organizations to work together to build a secure and orderly environment for cross-border data flow through the

formulation of uniform rules, strengthening technology research and application, improving data governance capabilities, and strengthening public education. Only in this way can we make full use of data resources to promote the development of the global digital economy while protecting personal privacy and data security.

5.3 Promote the Smooth Flow of Data Across Borders Through the Universal Application of International Data Laws

Enforcement issues such as the application of laws and jurisdictional disputes will also lead to barriers to data flows. Where international data law has been established, the application of international law should take precedence over the application of domestic data law. In the absence of international data legal provisions, when the domestic laws of the negotiating parties conflict, they should try to avoid the escalation of contradictions, and conduct equal consultations based on the principle of mutual benefit, rather than set higher data barriers to the other side. When resolving disputes over the application of law and jurisdiction over international data flows, countries should actively seek consensus and promote the establishment of a unified international data legal framework. This will not only help reduce the uncertainty of the application of the law, but also promote the healthy development of the global data market(Huang Gui & Lei Yin,2022).

To achieve this goal, countries may consider establishing a dedicated international data law coordination body responsible for developing and monitoring the implementation of international data law. In addition, through bilateral or multilateral agreements, countries can clarify rules and standards for data flows, ensuring the security and privacy of data during cross-border transfers.

In the absence of a fully established international data legal framework, countries should strengthen information exchange and cooperation, share best practices, and jointly address the challenges of data security and privacy protection. At the same time, countries should respect the legal systems and cultural differences of other countries and refrain from imposing unilateral application of laws on other countries based on their own laws. In addition, international organizations such as the United Nations, the World Trade Organization (WTO) and the International Telecommunication Union (ITU) can play an important role in promoting international data law harmonization. Through these international platforms, countries can jointly explore and develop international data legal standards, providing a more stable and predictable legal environment for global data flows. In conclusion, the resolution of legal application and jurisdictional disputes in international data flows requires the joint efforts of all countries to establish a fair, open and secure global data market through dialogue, cooperation and the development of international standards. Only in this way can we truly realize the global sharing and utilization of data resources and promote the sustainable development of the global economy.

6. Conclusion and Suggestion

In China, the current situation of cross-border data flow suffers from three major problems. First of all, the problem of data barriers is prominent, which mainly stems from the conflict between the principles of data sovereignty and free flow in different countries. The contradiction between countries' commitment to their own data sovereignty and their desire for data to flow freely has led to the formation of data barriers. Second, while technical responses can enhance data security, they do not address legal regulatory issues. The limitations of technical means mean that even if data security is guaranteed to a certain extent, regulatory issues at the legal level remain, which creates additional challenges for the cross-border flow of data. Third, rule-making is costly, with compliance costs increasing significantly due to multiple jurisdictions and legal differences. These difficulties are rooted in differences in the international political and economic

landscape, the emphasis on data sovereignty and security, and the fragmentation of rules at the legislative level.

In order to effectively address these challenges, synergy between international cooperation and legal regulation becomes essential. Promoting uniform or compatible data protection standards is key to addressing these issues. Governments and international organizations must work together to develop a single set of data protection standards. Such a standard would help ensure the sovereignty and security of data and prevent its misuse or illegal access. In this process, countries need to clarify their own data cross-border policies and provide clear guidance to businesses and individuals so that they can better adapt to and comply with these policies.

For enterprises, strengthening data governance is an important measure to address the challenges of cross-border data flows. Enterprises should adopt advanced encryption technology and other security measures to ensure the security of data during transmission and storage. At the same time, companies need to pay close attention to the development of international data legal frameworks in order to adjust their data management strategies.

Promoting an international legal framework for data is a crucial step. This requires coordination and efforts by international organizations to reduce uncertainties in the application of laws in different countries. Through these measures, we can promote the healthy development of the global data market and lay a solid foundation for the prosperity of the digital economy. In the current international environment, the cross-border flow of data has become a key factor in the development of the global digital economy. However, the existence of data barriers, the mismatch between technology and legal regulation, and the high cost of rule-making pose obstacles to the free flow of data. These problems not only affect the free flow of data, but also create constraints on the further development of the global digital economy. Therefore, to solve these problems, the international community needs to work together to promote the formation of unified data protection standards through strengthening international cooperation, as well as the development of clear data cross-border policies to provide clear guidance for enterprises and individuals.

In the process of promoting harmonized data protection standards, governments and international organizations need to jointly confront and resolve the contradiction between data sovereignty and free flow. By developing a compatible legal framework and regulatory measures, the legal risks of cross-border data flows can be reduced while safeguarding data security and privacy. In addition, clear cross-border policies for data will help companies better understand international rules, rationally arrange data flows and avoid compliance risks arising from legal differences.

As the subject of cross-border data flows, enterprises must take a more proactive approach to data governance. This includes adopting the latest encryption technologies, implementing strict data access controls, and establishing a comprehensive data security management system. At the same time, companies need to constantly update their understanding of the international data legal framework in order to adjust their data management strategies in a timely manner to ensure that they operate globally in compliance.The establishment of an international data legal framework is essential to promote the healthy development of the global data market. International organizations should play their coordinating role to promote consensus among countries on data protection standards and reduce uncertainties in the application of laws. This will help build a more open and transparent international data environment and provide legal guarantees for the continued growth of the global digital economy.

In the realm of cross-border data transfer, the foremost objective of global collaboration is to construct an international data governance framework encompassing the essential aspects of data

protection, privacy, data security, and data utilization. Governments must play a proactive role in urging international bodies to establish consistent standards and regulations for cross-border data transfer, with the aim of mitigating legal conflicts and regulatory obstacles. Concurrently, it is imperative to encourage the involvement of the private sector and non-governmental organizations in the rule-making process to ensure the comprehensiveness and practicality of the guidelines. Moreover, through periodic international conferences and forums, nations can share best practices, harmonize policies, and collaboratively tackle the challenges associated with cross-border data transfers. Looking ahead, as technological advancements continue and international cooperation deepens, cross-border data transmission is poised to become more secure and efficient, thereby providing a robust impetus to the growth of the global digital economy. Additionally, a more in-depth exploration of the role of technology in addressing the issues of cross-border data transfer warrants further research.

Funding

This study was supported by grant from theAnhui Law Society (2024ZCKT-12) and The Graduate Research Innovation Fund of Anhui University of Finance & Economics (ACYC 2023239).

References

1. Gao Hongwei.(2024). RTAs Data cross-border Flow rules Network and value chain tr ade in digital industry.International business studies(6),66-81. https://doi.org/10.13680/j.c arol carroll nki ibr.20241008.001.
2. Qiao Wang.(2024). An Exploration of the Challenges of Cross-border Data Flow for I nternational Investment Law by Counting and Fuzzy Numerical Analysis Algorithms.A pplied Mathematics and Nonlinear Sciences,31(1),74-87.
3. Sekgoka,C.,Yadavalli V.,&Adetunji O.(2022). Privacy-preserving data mining of cross-b order financial flows.Cogent Engineering,29(4),101737.
4. Jain,N.,Acosta S.,&Checchia A.(2022). Comparison of Laboratory and Hemodynamic T ime Series Data Across Original,Alpha,and Delta Variants in Patients With Multisyste m Inflammatory Syndrome in Children.Pediatric Critical Care Medicine,18(4),49-57.
5. Gregory V.(2022). Cross-Border Data Flows,the GDPR,and Data Governance.Journal of Database Management,31(2),74-87.
6. McLaughlin P.(2018). Cross-Border Data Flows and Increased Enforcement.IEEE secur ity&privacy,12(5),58-61.
7. Gyanchandani V.(2024). Cross-border flow of personal data(digital trade)ought to have data protection.Journal of Data Protection&Privacy,18(1),61-79.
8. Monika Z.(2022). Transborder Data Flows and Data Privacy Law.Computer Law&Secu rity Review:The International Journal of Technology Law and Practice,23(1),104-108.
9. LeSieur F.(2019). Regulating cross-border data flows and privacy in the networked di gital environment and global knowledge economy.International Data Privacy Law,14(2),

93-104.

10. Ben-David,I.,Graham,J.R.,&Harvey,C.R.(2019). Transborder Data Flows and Extraterritoriality:The European Position.Journal of International Commercial Law and Technology. 128(4),1547-1584.
11. Pandej C.(2017). The determinants of cross-border equity flows:a dynamic panel data reassessment.Applied Financial Economics Letters,12(3),181-185.
12. Schlingann,F.P.,&Stulscz,R.M.(2022). Regulating Cross-Border Data Flows in a Data-Driven World:How WTO Law Can Contribute.Journal of International Economic Law,31 (3),389-416.