zeitgeschichte
ZEITGESCHICHTE
ISSN / eISSN 0256-5250 / 2569-5304
Publisher BRILL DEUTSCHLAND GMBH,
VIENNA UNIV PRESS, ROBERT BOSCH BREITE 6,
GOTTINGEN, GERMANY, D-37079
Volume 25-Issue 1-(2025)
https://doi.org/10.63386/620111

Orientation of international legal regulation of cross-border data flow

Nan Dai

Law School, Jiangxi University of Science and Technology, Ganzhou, PR China

3396600841@qq.com

Abstract

In the era of cross-border data flow, differing legal regulations among countries limit effective governance. Consequently, conflicts over these regulations are central to international disputes. Addressing cross-border data flow requires not only consideration of national sovereignty and international legal frameworks, but also a focus on improving the construction orientation of these regulations.

Keywords: Orientation of international legal construction of cross-border mobility in the data age

Introduction

As we enter the era of cross-border data flow, a digital economy characterized by the "digitalization of all things" and a blended digital reality has emerged. This transformation has altered traditional production and life relationships, necessitating significant adjustments and adaptations in legal methods and frameworks [1]

The international legal regulation of cross-border data flow is complex and multi-faceted, involving many unresolved multilateral issues. This regulation should prioritize human dignity and orientation. Currently, there is no consensus on how international legal regulation should be shaped, highlighting the need for a global response to guide the approach to cross-border data flow.

The advancement of digital technology and the widespread use of the Internet have made data a fundamental foundation for the functioning of human society [2] ,and gradually evolved into a new context of cross-border data flow. Differences in religious culture, political systems, and levels of economic and technological development among countries create challenges in establishing multilateral legal regulations for cross-border data flow. Some nations prioritize economic interests over data security, undermining the integrity of legal regulation and straining international relations. Moreover, cross-border data encompasses not only citizens' personal information but also government, economic, and industrial data, all of which are vital to a country's economic well-being and the independence and security of the international community [3] . The PRISM scandal illustrates the challenges in establishing international legal regulations for cross-border data flow. While countries recognize the need for a unified approach, they have yet to reach a mutually beneficial consensus, resulting in ongoing issues with the orientation of these regulations.

1 raise a question

The information age marks a period where human civilization and legal development progress together. In our shared world, humanity has established a data civilization that enhances survival by providing convenience and quick value orientation while also fostering a desire for legal regulation and protection. From primitive communication to today’s Internet data era, legal regulations have evolved through numerous iterations, often driven by greed and the desire to maintain a laissez-faire approach to survival. As data flows globally across time and space, it becomes essential for humanity to seek legal regulations for protection. Times have changed, and the reform has

eliminated previous interpretations. Due to varying geographical and religious cultures, the application of multilateral legal regulations differs, often adhering to a conservative legal framework that does not align with international standards. This discrepancy creates challenges in regulating cross-border data flows across different countries and regions. Operating independently, some

entities may ignore cross-border data flow regulations and engage in the unlawful collection of data from other countries, infringing on their sovereignty and compromising personal information. This leads to conflicts over economic interests and highlights the clash of divergent legal regulations globally, underscoring the need for a collaborative approach to international legal regulation in the data age.

2 Orientation of the construction of international legal regulation

In the data age, the orientation of international legal regulation regarding cross-border data flow raises important questions. The current scattered legal frameworks across countries indicate that a cohesive international approach is lacking. To enhance this orientation, humanity must transcend its "self-interest" and act as moral advocates for all species on Earth. Only then can we shed the notion of "selfishness" and exemplify a higher purpose, akin to "being as long as heaven and earth and being as bright as the sun and the moon." This profound reflection holds epoch-making significance for the future of human society. [4]

During this period, various countries enacted legal provisions regarding the collection, storage, transmission, and processing of data. However, there are no specific international regulations governing the free movement of human data across borders. Consequently, the global flow of data rarely aligns with international legal frameworks, limiting their applicability and creating challenges in establishing effective regulations for cross-border data transfers.

3 The dilemma of the orientation of international legal regulation

The global cross-border data flow is characterized by fragmented and inadequate legal regulation. Local laws in different countries are inconsistent, and the regulations imposed focus more on national economic interests than on a cohesive global framework. This approach fails to adequately address the complexities of legal application across various nations.

TABLE.1 Core differences in international legal regulations regarding cross-border data flow between China and the United States [5]

National Agreements: Differences	China：RCEP	United States：USMCA
Cross-border flow of financial information	The cross-border provision of such financial information is prohibited, and in principle, financial data localization is implemented	Allowing the cross-border flow of financial data and removing the requirement for financial data localization
Data flows across borders	We respect the different legal forms adopted by each country to protect personal information	Promote the self-regulatory model of American enterprises
Protection of Personal Information	The principles and guidelines for the development of the legal framework are not specified, allowing for a diversity of compatibility mechanisms	It clarifies that the principles and guidelines for the development of the legal framework are CBPRs and the OECD Guidelines, and clarifies the compatibility mechanism to guide CBPRs
Exceptions to the Cross-Border Data Movement Clause	Allow Contracting Parties to take localized measures to achieve what they consider to be legitimate public policy objectives and expand the Contracting Party's planting rights	Allow Parties to adopt localized measures for cross-border data flows to achieve legitimate public policy objectives, emphasizing the limits of localized measures
Exceptions in the Computer Setup Terms	Allow Parties to take localized measures to achieve what they consider to be legitimate public policy objectives	The legitimate public policy objective exception has been removed entirely

Currently, global legal regulations governing cross-border data flow largely lack a unified international framework. This absence often leads to unfair practices and mutual accusations when addressing related issues. The application and direction of these legal regulations significantly impact harmonious bilateral relations and could expose serious deficiencies in the regulatory framework. Thus, establishing a coherent international legal framework for cross-border data flow has become an urgent practical challenge.

TABLE.2 View cross-border data flows differently [6]

Variance analysis	China	United States
The impact of cross-border data flows on the development of digital trade	Take a cautious stance in view of the impact on the domestic industry	More emphasis is placed on the cross-border flow of data Business value
Cross-border data flows pose a threat to national security	It may lead to national security risks, and data localization measures are taken based on specific goals	Double standards: Domestic data flows to foreign countries are seen as a national security risk, leading to strict restrictions, while not interfere with the data of other countries entering the United States.
The relationship between cross-border data flows and personal information protection	A Protect personal information and take into account social information sharing, and adopt classified protection	Pay attention to business interests and relax the protection of personal information

4 Insufficient emphasis on cooperation and consultation

In the data age, peaceful development and win-win cooperation have become the common goals of all countries. This pursuit emphasizes not only data security and international collaboration but also cross-border communication and consultation. To enhance global cooperation, we must effectively address the mechanisms established by international legal regulations. If these mechanisms for legal regulation, cooperation, and consultation are inadequate, it can create conflicting interests among nations, hindering collaboration and mutual benefits. Thus, the current challenge is to improve cooperation and consultation in the framework of international legal regulations governing cross-border data flow.

In the spaces where humans live, legal regulations vary significantly, leading to conflicts in their construction. A global consensus on applicable laws and regulations has yet to be achieved. Consequently, in the international legal framework governing cross-border data flows, discrepancies arise in legal applications and negotiation mechanisms, undermining human protection in legal regulations. This situation contributes to the slow resolution of cross-border data issues and fosters conflicting orientations, complicating the cooperation and negotiation.

5 The international legal regulation of cross-border data flow is balanced and oriented

As humanity navigates the realm of cross-border data flow, the development of international legal regulations remains nascent. This situation has led to a disruption in our approach to legal frameworks. Humans are not only innovators and beneficiaries of the data era but also guardians of order. Over the years, cross-border data flow has emerged as a transformative technology in our

interconnected world, yielding economic benefits and revealing deeper insights into order. Some Western scholars have aptly noted, "Our laws are like struggling fish on the deck." [7] "Modern law will inevitably align with the legal regulatory frameworks of the digital age, reflecting the historical evolution of traditional, modern, and digital social law[8].

As countries navigate the legal regulation of cross-border data flow, influenced by the U.S. monopoly in the data industry and divergent economic interests in Europe, various nations have implemented their own laws. Examples include the Swedish Data Act, the Federal Data Protection Act, and the UK Data Protection Act. These developments signify the evolution of global legal frameworks governing data flow and mark a significant step towards international legal regulation in the data age.

The iterative changes over the past few decades have led to a global framework for the legal regulation of cross-border data flow involving the United States, the European Union, and China. Due to differing national perspectives, a complex and diverse set of legal regulations exists, lacking binding authority across various regions. This disparity inevitably impacts the development of cross-border data flow regulations and the balance of international order.

6 Disputes over the orientation of legal regulation

To preserve the unrestrained survival, countries have opened the Pandora's box of legal regulations governing cross-border data flow, which vary significantly and overlap. The United States adopts a market-oriented approach, the European Union a rights-oriented one, and China seeks a balance between security and development[9] .

（一）The law regulates the construction orientation of each country

1、United States.

We will enhance cross-border economic benefits from data while focusing on legal regulations, promoting a strategic vision of data freedom and civilization, and fostering a balance between free interests and legal oversight globally.

TABLE.3 Major U.S. international agreements on cross-border data flows[10]

agreement	Key Principles/Clauses
U.S.-Korea Free Trade Agreement	Unnecessary barriers to the cross-border flow of electronic information should be avoided as much as possible.
USMCA Agreement	In 2020, a series of prohibitions on localization were added, including a ban on data taxes
APEC Privacy System	Take all reasonable and appropriate steps to avoid and remove any unnecessary obstacles to the flow of information
Agreements on trade in services Trade in Services Agreement)	Improve market access and remove barriers to cross-border trade
U.S.-Japan Digital Trade Agreement	Data localization measures that restrict server geolocation and data processing activities are prohibited

The Uniform Trade Secrets Act, informed by U.S. regulations on cross-border data flows, clarifies information security provisions to enhance global data interests and legal frameworks. Recently, legal instruments like the Privacy Protection Framework, the Privacy Shield Agreement, and the EU-US Data Privacy Framework have guided the development of a globally regulated free order for cross-border data flows.

TABLE.4 The main domestic policies and regulations for cross-border data flow in the

United States[11]

Policies and regulations	Measure
Electronic Communications Privacy Act	Public administrations can only obtain data stored abroad through mutual legal assistance treaties, and surveillance of people's communications is prohibited (which has been replaced)
Network Security Agreements, NSAs	A package agreement between the supplier and the U.S., where the government requires access to the supplier's database, while imposing local storage requirements for certain customer data
USA Patriot Act	Authorize law enforcement and intelligence agencies to listen to and review suspects' communications and request data from service providers. Lifting restrictions on the interception of people's communications
Federal Trade Commission Act	The U.S. Federal Trade Commission is broadly mandated to enforce federal privacy and data protection regulations and to prescribe financial penalties and criminal measures for violations
Tax Information Security Guidelines for Federal, State and Local Agencies	Federal agencies must limit the location of information systems that receive, process, store, or transmit (federal tax information) to U.S. territories, embassies, or military facilities
Supplemental provisions to the Department of Defense Procurement Regulations(DFRAS)	The Cloud Computing Services (DFARS 252.239-7010) clause states that all CDIs shall be maintained on cloud servers within the United States. Contractor shall maintain government data within the United States, except as specified
Export Administration Regulations/International Traffic in Arms Regulations	Requires U.S. persons to seek and obtain authorization from the U.S. government before exporting U.S.-controlled technology data to foreigners

2. European Union.

The European Convention on Human Rights is a key legal framework for the fundamental rights and freedoms of European citizens. This was succeeded by the Charter of Fundamental Rights of the European Union and the Digital Services Act. Consequently, the EU's regulations on cross-border data flows prioritize the protection of rights and interests, emphasizing data rights[12].

In 2017, the European Union released "Exchanging and Protecting Data in a Globalized World," which outlined the legal framework for international data transfers and acknowledged the United States' leadership in data liberalization. This document highlights a strict approach to cross-border personal data flow, emphasizing the importance of protecting citizens' human rights and prioritizing personal interests[13].

The EU's legal regulation of cross-border data flow fosters data market unification within the EU by establishing a governance framework that enables data from non-EU enterprises to return to the EU via "long-arm jurisdiction." However, other countries exhibit varying degrees of alignment with these legal norms and regulations regarding cross-border data flow.

3. Japan.

Japan has established the Basic Law on the Promotion of the Use of Public-Private Data and Guidelines for Cross-border Data Flows to regulate cross-border data flows. The country advocates

for the free flow of trusted data as part of its strategy for a data-driven economy[14].The facilitation of free government and private data flow across borders has enhanced the integration of these data types and improved the regulation of cross-border data movement. This is characterized by a legislative focus on establishing a "trust-based free flow of data [15] ."

4. Russia

The legislation prioritizes data localization to safeguard against cross-border data flow risks, establishing asystem for cross-border data transmission that favors national and public interests [16] .

6. Singapore

Singapore's Personal Data Protection Act and Regulations establish a comprehensive system for regulating cross-border data flows, requiring data controllers to adhere to local disclosure and transfer regulations [17] .

7. China

Protect national data sovereignty and security. This has been achieved through the enactment of the Cybersecurity Law, Data Security Law, Personal Information Protection Law, guidelines for cross-border data transfer assessments, measures for cross-border personal information assessments, and regulations on critical information infrastructure protection.

TABLE.5 Comparison of regulations on cross-border data flows [19]

Compare content	America	EU	China
Core features:	Market-oriented	Equity-oriented	Security and development balance
Regulatory means	It is mainly based on market regulation	Geographical discrimination	Strong government regulation
Goal 1: National security	Adopt measures to restrict the flow of data that endangers national security	Member States are directly responsible; The EU has the right of veto in exceptional cases	Attach importance to data sovereignty and security; Emphasis on security assessments
Goal 2: Privacy protection	California and Virginia have laws	A strong focus on privacy; Protect the fundamental rights and values of the individual	Conduct a security assessment of personal data privacy protection supporting digital development;
Goal 3: Business interests	Specific data is strictly restrictive and requires an export license	Commercial companies have an obligation to protect the accuracy and integrity of their data	Emphasis is placed on the protection of intellectual property rights

The United States advocates for a non-discriminatory and less restrictive legal and regulatory framework for global data freedom. It emphasizes that cross-border data flow should not face prohibitions or restrictions as a general principle; however, any restrictions must not be arbitrary,

unreasonable, or disguised trade barriers, and should adhere to the principle of proportionality. This approach aims to establish a global standard for cross-border data freedom. [20].

The differing orientations of China, the United States, and the European Union regarding legal regulations for cross-border data flows—particularly the conflicts between data security, personal privacy protection, and the free flow of data—are unlikely to be reconciled quickly. [21].The Internet is inherently interconnected, whether through the European Union, American, or future Chinese models. Under globalization, it facilitates the free cross-border flow of data, conditioned by specific criteria. [22].

TABLE.6 Legal regulation of cross-border data flow in different countries (organizations). [23]

Country/Organization	Laws and Regulations	Legal regulation of cross-border data flows
European Union	《General Data Protection Regulation》《Framework Regulation on the Free Movement of Non-Personal Data within the European Union》	Strict protection of personal data privacy data; "Determination of Adequacy Protection"; advocating for the EU's single data market; Establish a "white list" system.
United States	《Safe Harbor Protocols》《Privacy Shield》《Cloud Act》	Leverage the Cloud Act to implement "long-arm jurisdiction" jurisdiction; "Competent Government" Criteria.
Japan	《Promote the Basic Law through the use of government and private data》《Personal Information Protection Act》《Action Guidelines for Cross-Border Data Flows》	Advocate the concept of free flow of databased on trust; The government and the private sector participate in governance.
Singapore	《Personal Data Protection Act》《Personal Data Protection Regulations》	Adopt conditional cross-border data transfer provisions

（二）The legal regulation is constructed in a consistent direction

The process differs by country due to factors like technology, economy, legal systems, and privacy protection. Nevertheless, both the US and EU models aim to promote the free flow of data to access information from abroad. [24] The foundation of international legal regulation for cross-border data flow is a consistent emphasis on free order.

The authority to establish international rules often rests with the great powers. [25] The interplay between Europe, the U.S., and China centers on establishing contextual rights of orientation. While the EU may lack the economic strength of the U.S., it wields significant influence in shaping the rules. All three entities— the U.S., EU, and China—are navigating the regulation of the principle that "data knows no borders, but sovereignty does.".[26] The legal regulation of cross-border data flows in Europe, the United States, and China is not strictly an either/or scenario; instead, a consistent and integrated approach can be pursued. Even without a shared value orientation in constructing these regulations, no single optimal legal framework exists due to varying environmental factors like political structures, traditional legal systems, social and technological advancements, and policy considerations. Furthermore, while international cooperation occurs, its outcomes have been notably limited. [27] Osaka Orbit, part of Japan's Initiative for the Free Flow of Trusted Data.

TABLE.7 A framework for data governance in Osaka Rail [28]

Transmission mechanism	Legal and Regulatory Cooperation	Technical standards and industry cooperation	Rules of International Trade
Unilateral opening (unlimited) with user consent or other lawful data transfer grounds (e.g., contractual obligations, public interest) and accountability mechanisms (e.g., Standard Contractual Clauses, Binding Corporate Rules).	Binding International Convention on the Harmonization of Law《Budapest Convention》	Standard-setting for multistakeholder forums	WTO Rules (General Agreement on Trade in Services, Telecommunications Reference Document and Annexes), including privacy and other exceptions, and two-tier testing (minimum trade restrictions and necessity) Ongoing WTO sub-business negotiations
Adequacy decisions, such as the EU and Japan reciprocal adequacy decisions Certification programs (implemented under government supervision, such as the APEC Cross-Border Privacy Rules	Regulatory cooperation at the regional level on e-commerce, cross-border data flows and privacy (EU, ASEAN) Principles and guidelines on data flow and privacy (OECD privacy guidelines, APEC privacy framework) Legal assistance through mutual legal assistance treaties or international conventions Judicial remedies and recourse to a range of countries under domestic law Diplomatic mechanisms and strategic partnerships (e.g. Australia-Singapore Digital Economy Agreement)	National and regional standard-setting, such as the United Nations Economic Commission for Europe Unique "data space" programs and alliances Bilateral mutual recognition agreements or reciprocal decisions	U.S.-Japan Digital Trade Agreement USMCAA EU Act Digital trade commitments in the Digital Economy Partnership Agreement (e.g. data flows, prohibition of localization, and source code rules)

This paper examines the legal regulation of global cross-border data flow amid intense competition for economic interests, highlighting the complexity of concepts such as freedom versus authoritarianism, governance pluralism (government, private sector, or civil society), various legal forms (treaties or informal arrangements), and differing regulatory constraints (hard or soft law). [29] .It is precisely for this reason that some countries support free cross-border data flow impose data localization requirements to ensure network security. [30] To clarify the current situation and trends in cross-border data flow regulation, it is essential to address the conflicting interests of different countries. The legal frameworks governing cross-border data flow vary widely, leading to issues of inconsistency and overlap. While the phenomenon of global data flow is universal, the interests of countries differ significantly, resulting in distinct regulatory approaches. For instance, countries with advanced digital technologies and robust digital service infrastructures have different priorities compared to those seeking to assert national sovereignty through regulatory measures. [31] .Countries still struggle to engage in the development of international legal regulations, exacerbating the challenges surrounding cross-border data flow.

（3）Practical challenges in the construction of legal regulation

The rapid development of cross-border data flow presents complex challenges for global legal regulations, particularly with varying data transmission laws across countries. Resolving regional cross-border data issues requires the establishment of local legal frameworks. However, when these local regulations are integrated into international legal standards, it results in complicated conflicts due to significant legal differences, making the establishment of international regulations for cross-border data flow a substantial challenge.

Most legal regulation issues surrounding cross-border data flow are region-specific, rooted in each country's sovereignty, security, and economic interests. Achieving a consensus on international legal regulations requires negotiation and communication among all countries, which face challenges in aligning their regional legal frameworks.

Countries specialize in developing their own legal regulations for cybersecurity to protect economic interests. When conflicts arise regarding cross-border data flow regulations, resolution requires mutual consultation of local laws, leading to regional solutions instead of a global consensus.

Regional legal regulation should align with global development trends rather than solely addressing problems. This alignment is essential for shaping the international legal framework. In the data age, the legal regulatory order will differ significantly from traditional systems, necessitating ashift in legal concepts and the establishment of a robust legal supply mechanism and guarantee system to solve the problem [32] .

4、Constructive orientation strategy for international legal regulation of cross-border data flow

The regulation of cross-border data flow in international law hinges on the quality and quantity of data, which are crucial for the digital economy. Ensuring data quality and quantity while balancing protection and utilization is essential [33] .International legal regulation should prioritize the interests and cooperation of countries by addressing security and economic concerns while minimizing contradictions and conflicts. This approach is a practical necessity, a global aspiration, and an essential direction for developing international legal frameworks.

TABLE.8 The international regulatory pathway for cross-border data flows between

China and the United States [34]

Country	Laws and Regulations	Legal regulation of cross-border data flows
General proposition	Respect the data sovereignty of all countries, take into account the needs of different countries, and promote the development of digital trade through cooperation	S Focusing on U.S. interests, promoting American-style rules, and working with allies to exclude other countries
Bilateral level	Bilateral FTAs contain provisions on cross-border data flows, but do not include specific provisions on cross-border data flows	Bilateral FTAs include specific provisions for cross-border data flows
Regional level	Clauses on cross-border data flows have been included in those who have acceded to the RCEP and those who have formally applied to join the CPTPP and DEPA	Promotes U.S.-style cross-border data flow clauses in CBPRs, TPP, USMCA, USJDTA, and TTIP.
Multilateral	Participating in the WTO e-commerce negotiations advocates respecting members'right to supervise cross-border data flows, and allowing data to flow safely, orderly and freely	Participated in the WTO e-commerce negotiations, advocated the free flow of data across borders, and opposed data localization

（1）Improve the orientation of the construction of international legal regulations for cross-border data flows

The orientation of international legal regulation requires that data innovation and legal frameworks be coordinated and unified among different countries without conflict. Furthermore, within the legal regulatory frameworks of various nations, it is essential to implement and supplement regulatory directions so that existing legal regulations and consensus mechanisms work together effectively. Moreover, while establishing rules should ensure order, it must also uphold the freedom of market transactions [35] .The primary objective in developing international legal regulations for cross-border data flow is not to eliminate differences among countries, but to establish a new cooperation mechanism that acknowledges these differences. This approach aims to facilitate the free flow of data while ensuring the protection of data rights [36] .It secures the interests of all countries, facilitates smooth cross-border data flow, and enhances the fairness of international legal regulations.

TABLE.9 Regulatory systems and institutions for cross-border data flows in different countries (organizations).[37]

Country/Organization	Characteristics of the regulatory regime	Regulatory Bodies
European Union	Relying on "adequacy protection determinations" to supervise data; Develop an integrated data governance institutional framework as a means	EU Data Protection Commission
United States	It advocates "wide entry and strict exit", mainly through "long-arm jurisdiction" and "qualified government" supervision, but strictly restricts the exit of relevant important information such as national security and citizens'personal information	Department of Commerce, Federal Trade Commission, Office of the Trade Representative, Department of Justice, etc
Japan	Relying on the "Personal Information Protection Commission" to supervise cross-border data; A government-led governance pattern with the coordinated participation of diverse civil society groups	Personal Information Protection Commission
China	It is mainly based on the security assessment system for data export and the hierarchical and classified management mechanism for data; Guided by national security, it is strictly forbidden to export core data	Cyberspace Administration of China, etc
Singapore	The pattern of multi-department co-management attracts multinational enterprises to establish data centers; Actively participate in the CBPR system	Personal Data Protection Commission, Information, Communication and Media Development Authority

（2）The consensus orientation of international legal regulation construction

Law emerges from global economic development and aims to establish a framework for international legal regulation that considers the security and economic interests of all nations. Therefore, regulations governing cross-border data flow should strike a balance in legal frameworks. It is essential to draw insights from the legal regulations of other countries to create a more effective liberal order. Addressing the challenge of inconsistent regulations hinges on fostering international consensus regarding the establishment of global legal frameworks that harmonize with the diverse legal systems of different countries.

（3）Consultation and cooperation is an inevitable orientation in the construction of international legal regulation

Countries worldwide share a desire for robust international legal regulation of cross-border data flow. With the European Union's Binding Corporate Rules (BCR) and the U.S.-led Cross-Border Privacy Rules (CBPR) as the two main regulatory frameworks, there is a need to establish a balanced order in global data flow regulation. As cross-border data flows rapidly increase, the regulatory approaches adopted by different nations may conflict, leading to clashes over concepts, systems, and specific measures. Since data regulation touches on national sovereignty, countries can only achieve regulatory coordination and cooperation by relinquishing or limiting their sovereignty, creating a significant barrier to international collaboration in data governance[38].The Earth serves as humanity's data home, embodying the vision of a free order that promotes improved international legal regulations for cross-border data flows.

The fragmentation of legal regulations and the absence of a global legal framework necessitate the establishment of a consultation and cooperation mechanism among countries. However, differing legal systems impose limitations on international regulation efforts. To effectively manage cross-border data flow, it is essential to align international legal regulations with the UN Charter, seek agreements that reflect our national interests, foster consensus through global cooperation, and mitigate conflicts in legal frameworks to protect global interests. Therefore,a coherent approach to international legal regulation of cross-border data flow is imperative.

TABLE.10 The United States, the European Union, and China have different orientations[39]

Region	Different orientations
United States	The USMCA, signed by the United States, includes detailed data regulation provisions that promote the free flow of cross-border data, reflecting "America First" principles. It also contains a "poison pill clause" requiring member countries to notify each other when negotiating with non-market economies, significantly limiting Mexico's and Canada's future trade autonomy. While presented as a global model, its "America First" framework and the poison pill clause hinder the possibility of a comprehensive international data treaty based on the USMCA.
European Union	The European Union's success hinges on its unique market and its strong extraterritorial jurisdiction, which enable the "Brussels effect" in data regulation. Unless significant compromises from the EU, reaching a comprehensive international data treaty will be challenging for major global players.
China	China has not exceeded the depth and scope of previous bilateral free trade agreements with South Korea and Australia. This aligns with the Chinese government's longstanding position that countries should reach multilateral agreements on e-commerce based on WTO guidelines, without fully integrating digital trade governance into these agreements. Consequently, the Chinese government is open to the possibility of a comprehensive data treaty and the methods (hard or soft law) for international cooperation on data governance, aiming to collaborate and propose specific execution strategies.

The definition and interpretation of trust in the "cross-border flow of trust-based data" should not be limited to a few developed countries; developing nations with diverse political and legal traditions also deserve a role in the discussion. Thus, the UN mechanism should serve as the primary platform for establishing international consensus[40].

In the interconnected cross-border flow of data, win-win cooperation should focus on establishing an international legal regulatory framework. This framework must prioritize international regulations for cross-border data flow over local laws, promoting compatibility among the legal systems of different countries. Additionally, while ensuring data security, it is essential to design coordinated legislation carefully[41], to build a comprehensive legal framework[42].We should strive for shared interests and common legal regulations to help harmonize the inconsistent global cross-border data flow and promote mutual recognition among countries.

Conclusion

The development of the data economy and the benefits for all countries depend on establishing international legal regulations. Relying solely on traditionally static legal frameworks will render such regulations ineffective for cross-border data flow. Incorporating open and inclusive technical perspectives into legislative processes can address the limitations of existing legal norms and enhance the synergy between legal frameworks and technological safeguards to mitigate risks. Ultimately, the construction of legal regulations should be guided by a multilateral consultation mechanism to achieve consensus on international governance of cross-border data. Thus, establishing international legal regulations for cross-border data flow has become an essential global priority.

NOTE：

（1）PRISM is a top-secret electronic surveillance program implemented by the National Security Agency (NSA) since 2007 during the George W. Bush era"Covert surveillance project, officially known as "US-984XN." Directly into the central server of the Internet Corporation of the United States, mining and collecting intelligence, including Microsoft, Yahoo, Google, Apple, etc., nine international Internet giants are involved.In May 2013, "Edward Snowden", an employee of the National Security Agency contract contractor, leaked top-secret documents

（2）Establishment of the Hesse Data Protection Commission, which regulates the storage and transmission of official documents of the State of Hesse and prevents unauthorized access, correction and destruction. With regard to the protection of personal data, the Act sets out the requirements that the Government of Hesse must comply with when processing personal data and ensures that the autonomy of personal data is not violated. The passage of this law marks the beginning of the legal level of personal data protection

（3）The Swedish Data Act is a legal regulation of consumer credit intelligence investigations, and it is also the first law in the world to comprehensively regulate the privacy protection of personal data

and （4）the Federal Data Protection Act (BDSG), such as the lawfulness, transparency and fairness of the collection, use and dissemination of personal data, as well as the right to information and objection of the data subject

（5）Personal information protection rules in the establishment of cross-border e-commerce

（6）The 2016 EU-U.S. Privacy Shield, which requires the U.S. to ensure that EU data subjects provide adequate data privacy protections

（7）DPF. The executive order imposes some new rules on mass surveillance in the United States and establishes administrative remedies for individuals subject to unlawful surveillance

（8）After the Second World War, in order to avoid the recurrence of similar human rights tragedies, the countries of Western Europe decided not to ensure the protection of human rights through international conventions

（9）1. Everyone has the right to protect personal data concerning them.2. Such personal data must be processed for a specific purpose. Everyone has the right to access the data collected and related to them, as well as the right to modify and revoke them.3 There should be separate departments and agencies to enforce the above rules.".

（10）It will come into effect in August 2023. It aims to establish a more open, fair and free competition European digital market, promote the innovation and growth of the EU digital industry, and provide EU consumers with safer, transparent and trustworthy online services

(11) In 2016, the Japanese government promulgated the Basic Law on the Promotion of the Use of Public and Private Data. It is a law enacted by the Japanese government to effectively utilize private funds, management capabilities, and technical capabilities for the development of public facilities. It aims to promote the healthy development of the national economy through efficient social capital development

(12) The Act regulates in detail the data protection rights of individuals and the collection, use and disclosure of personal data by enterprises, and publishes a series of regulations and guidelines to promote the implementation of the Act

References：

［1］马长山.数字法学教育的迭代变革[J].中国人民大学学报，2022（6）：36.

［2］华佳凡.美国跨境数据流动国际倡议与国内政策的差异及其成因[J].情报杂志,2024,43(1):98.

［3］张相君.易星竹.数字贸易中跨境数据流动的国际法挑战与中国因应[J].福州大学学报（哲学社会科学版），2023（3）：104.

［4］林灿铃.边境地区环境问题的法治之道[J].政法论丛，2017（4）：103.

［5.6］宋瑞琛.冯纯纯.中美数据跨境流动的国际法规制及中国的因应[J].法律，2022（7）：90－92.

［7］[美]尼葛洛庞帝.数字化生存.胡泳译[J].电子工业出版社，2017 版，237.

［8］马长山.数字何以生成法理？[J].数字法治，2023（2）：25.

［9］朱 勤.刘 玥.数字贸易发展背景下跨境数据流动国际治理及我国的探索[J].科技管理研究,2023（7）：153.

［10.11］华佳凡.美国跨境数据流动国际倡议与国内政策的差异及其成因[J].情报杂志,2024,43(1):100.

［12］肖宛晴.刘传平.欧美数字主权与数字贸易政策比较分析［J］.世界经济与政治论坛，2021(6):105-126.

［13］东方.欧盟、美国跨境数据流动法律规制比较分析及应对挑战的“中国智慧”［J］.图书馆杂志，2019（12）.

［14］李墨丝.欧美日跨境数据流动规制的博弈与合作［J］.国际商务，2021（2）：83－84.

［15.16]胡海波.耿骞.数据跨境流动治理研究:溯源、脉络与动向［J］.情报理论与实践，第 46 卷 2023 年(7) :181.

［17］周念利.姚亭亭.跨境数据流动限制对数字服务进口的影响测度及异质性考察［J］.国际商务,2021(2):1-15.

［18］周念利.姚亭亭.跨境数据流动限制对数字服务进口的影响测度及异质性考察［J］.国际商务,2021(2):1-15.

［19］朱勤.刘玥.数字贸易发展背景下跨境数据流动国际治理及我国的探索[J].科技管理研究,2023（7）：154.

［20.21］魏宁.美国数据出境管理体制及中国因应[J].国际经济法学刊，2022（4）：28.

［22］时业伟.跨境数据流动中的国际贸易规则：规制、兼容与发展[J].比较法研究，2020（4）：181 .

［23］胡海波.耿骞.数据跨境流动治理研究:溯源、脉络与动向［J］.情报理论与实践，第 46 卷 2023 年(7) :180.

［24］时业伟.跨境数据流动中的国际贸易规则：规制、兼容与发展[J].比较法研究，2020（4）：181 .

［25］翁国民.宋丽.数据跨境传输的法律规制［J］.浙江大学学报（人文社会科学版），第 50 卷 2020（2）：44.李墨丝.欧美日跨境数据流动规制的博弈与合作［J］.国际商务，2021（2）：86.

［26］马长山.数字智治理的法治悖论[J].东方法学，2022（4）：70.

［27］See generally Cass R. Sunstein, Incompletely Theorized Agreements， 108 Harv. L.Rev.1733(1995).

［28］李墨丝.欧美日跨境数据流动规制的博弈与合作［J］.国际商务，2021（2）：86.

［29］彭岳.数字贸易治理及其规制路径［J］.比较法研究，2021（4）:161.

［30］方滨兴主编.论网络空间主权［J］.科学出版社，（2017）：16.

［31］彭岳.数字贸易治理及其规制路径［J］.比较法研究，2021（4）:166.
［32］周佑勇.从部门立法到领域立法：数字时代国家立法新趋势［J］.现代法学 2024（5）.
［33］魏远山.博弈论视角下跨境数据流动的问题与对策研究［J］.西安交通大学学报（社会科学版），第 41 卷 2021（5）：116－117.
［34］宋瑞琛.冯纯纯.中美数据跨境流动的国际法规制及中国的因应[J].法律，2022（7）：91.
［35］池海江.沈励.李洁瑜.跨境数据流动的法律风险与治理建议［J］. 数字法治，2024（2）：136.
［36］陈少威.贾开.跨境数据流动的全球治理:历史变迁、制度困境与变革路径［J］.经济社会体制比较，2020（2）：122.
［37］胡海波.耿骞.数据跨境流动治理研究:溯源、脉络与动向［J］.情报理论与实践，第 46 卷 2023(7) :182.
［38］彭岳.数字贸易治理及其规制路径［J］.比较法研究，2021（4）:159.
［39］彭岳.数字贸易治理及其规制路径［J］.比较法研究，2021（4）:166.
［40］洪延青.数据跨境流动的规则碎片化及中国应对［J］.行政法学研究，2022（4）：71.
［41］李艳华.隐私盾案后欧美数据的跨境流动监管及中国对策——软数据本地化机制的走向与标准合同条款路径的革新［J］.欧洲研究，2021（6）.
［42］熊鸿儒.田杰棠.突出重围: 数据跨境流动规则的中国方案［J］.人民论坛·学术前沿，2021（1）.
［43］周佑勇.从部门立法到领域立法：数字时代国家立法新趋势［J］.现代法学 2024（5）.