JOURNAL OF INTELLECTUAL PROPERTY AND HUMAN RIGHTS

Volume: 3 Issue: 7 | July–2025 ISSN: 2720-6882
http://journals.academiczone.net/index.php/jiphr

Study on the Dilemma of Legal Regulation of Cross-border Flow of Personal Information

Wang Cong
Doctoral Student at the University of World Economy and Diplomacy
Tashkent 100174,Uzbekistan
Suqian University, Suqian 223800, China

Muattara Rakhimova
DSc in Law, Professor,
Professor of the International Law and Human Rights Department of the Tashkent State University of Law,
Tashkent, Uzbekistan

Аннотация: The cross-border flow of personal information around the world faces multiple legal regulation dilemmas. There are fundamental differences in the legislative concepts of various countries. The trend of regional agreements (such as CPTPP and RCEP) has exacerbated the conflict of rules, and the lack of participation of developing countries has further widened the "digital divide". The contradiction between technological iteration and legal lag has led to enforcement difficulties such as jurisdictional conflicts and a surge in compliance costs. The root causes of these dilemmas lie in the value conflicts caused by the multiple attributes of data, the differences in the level of development of the digital economy, and the defects of the international governance system. In the future, a more inclusive coordination mechanism needs to be established to balance the freedom of data flow, the protection of rights and national security to promote the sustainable development of the global digital economyh.

Ключевые слова: Cross-border flow of personal information Digital divide Value conflict Data sovereignty.

At present, a unified regulatory framework for cross-border data flows has not yet been established globally, which leads to a lack of stable and predictable legal protection for the international transmission of personal information. At present, the international community mainly coordinates the issue of cross-border transmission of personal information through multiple mechanisms such as domestic legislation, regional agreements, and bilateral arrangements. From the review of the legislative practices of various countries, there are obvious differences in the formulation of cross-border transmission rules for personal information. Through comparative analysis of the existing legal systems and legal practices of various countries, we can find several common problems in the legal regulation of cross-border personal information flow, reflecting the common dilemma of legal regulation of cross-border flow of personal information.

ANALYSIS AND RESULTS

1. Problems with existing rules on cross-border flow of personal information

1.1 Fragmentation and division of legal rules

Although the legal regulation of cross-border flow of personal information presents the status quo of domestic law and international law in parallel, the domestic legal regulation of each country still

occupies a dominant position, and a global and unified regulatory system for cross-border flow of personal information has not yet been formed. The international rules in this field show obvious regionalization and fragmentation characteristics, which restrict the interoperability of cross-border information flow. Against the background of the booming digital trade, smooth cross-border data flow has become an important foundation for international economic and trade cooperation and cultural exchanges. However, although international soft laws such as the OECD Privacy Protection Guidelines and the APEC Privacy Framework have a certain influence, they lack legal binding force; and the relevant agreements under the WTO framework have failed to fully respond to cross-border data flows. Therefore, the international community has to rely on legally binding regional agreements to coordinate supervision, such as USMCA, CPTPP, RCEP and DEPA. These regional rules are often deeply influenced by geopolitics, reflecting the core interests of the dominant countries, and showing a clear trend of camp formation. At present, the positions of major economies in the world on the issue of cross-border flow of personal information are significantly different: the United States emphasizes the free flow of data, the European Union focuses on personal information protection, Russia emphasizes data sovereignty, and China pays more attention to data security. As it is difficult to reconcile the interests of all parties, multilateral coordination mechanisms are difficult to advance, which ultimately leads to the further regionalization and fragmentation of the rules for cross-border flow of personal information. Regionalization and fragmentation have rendered the multilateral mechanism ineffective.

In this context, the policy choices of various countries are often constrained by existing and emerging international economic law commitments, which may limit a country's autonomy to impose restrictions on cross-border data transfers or force data localization. For developing countries, there are three main policy path options in the field of data governance: First, adopt the "Silicon Valley Consensus" model, represented by agreements such as CPTPP and DEPA, which advocate the free flow of data, oppose local storage, require only minimum standards for personal information protection, and tend to reduce government intervention. [1] Second, learn from the EU regulatory model, take the General Data Protection Regulation (GDPR) as a model, and emphasize the human rights value orientation of personal information protection. Third, adopt the RCEP flexible model, allowing member states to retain a wide range of policy exceptions and enjoy the right of self-determination. In addition, some countries, such as India, choose to avoid making new international commitments, which further exacerbates the differentiation of the global data governance system. Institutional competition and policy differences between different camps have led to a continued deepening of the fragmentation trend of the regulatory framework for cross-border data flows.

The factionalization and fragmentation of existing rules hinder the interoperability of cross-border flows of personal information and the cross-border flow of data. The “digital divide” will continue to widen. The fragmentation of national laws and regulations forces multinational companies to adopt differentiated compliance strategies in cross-border transmission of personal information, increasing the compliance burden on companies. [2] Conflicts in rules force countries to make difficult choices.

Take the conflict between APEC's CBPR system and RCEP as an example. The CBPR system (9 members including the United States, Canada and Mexico) advocates the free flow of data, while the RCEP (15 countries including China, Japan and South Korea) adopts a relatively strict regulatory stance. [3] Since countries such as Japan and Australia participate in multiple mechanisms at the same time, they have to face the problem of rule compatibility. Similarly, Latin American countries are often caught in a dilemma between the EU GDPR model and the US free flow model. [4] This pressure to "choose sides" further strengthens the trend of regulatory camps.

1.2 Huge differences in legislative models

The fundamental challenge facing the current global cross-border flow of personal information rules system lies in the deep value conflict of legislative concepts in different legal jurisdictions. This conflict

is not a technical disagreement or a difference in the details of the rules, but stems from a fundamental cognitive difference in the essential attributes of data - whether data is a basic human rights carrier that should be absolutely protected, a production factor that needs to flow freely, or a strategic resource that must be placed under the control of national sovereignty. This cognitive difference has formed a variety of competing legislative paradigms, and the tension between them constitutes the most stubborn structural obstacle in the current international rule coordination.

The first is the conflict and balance between human rights protection and market efficiency. The EU regards personal information protection as a basic human right. Its rules system emphasizes the absolute control of individuals over data and requires that cross-border data flow must meet the standard of "substantially equivalent" to domestic protection. This concept has formed a strict "adequacy recognition" mechanism in practice, automatically excluding countries that do not meet its standards from data flow partners. The United States, on the other hand, advocates the free flow of data through industry self-discipline and departmental supervision based on the efficiency of the market economy, and its rules focus more on promoting business innovation and international cooperation. The conflict between these two concepts was vividly demonstrated in the case where the "Privacy Shield" agreement was rejected twice by the European Court of Justice - the European Court of Justice believed that the US surveillance laws could not protect the data rights of EU citizens, while the United States believed that the EU's standards hindered the development of the digital economy. This value conflict exists not only between Europe and the United States, but also faces doubts from emerging market countries when the EU tries to promote its standards globally.

The second is the institutional contradiction between sovereign control and global flow. Countries represented by China and Russia, starting from the principle of network sovereignty, regard data as a national strategic resource and emphasize the ultimate control of the state over cross-border data flows. The data localization requirements and security assessment systems generated under this concept are in direct conflict with the principle of free flow of data advocated by Europe and the United States. What's more complicated is that when a country faces the dual pressures of human rights protection requirements and sovereign control requirements at the same time - for example, multinational companies need to comply with both the EU GDPR and China's data localization regulations - they will fall into an irreconcilable compliance dilemma. According to a survey report released by the International Chamber of Commerce in 2023, 78% of multinational companies said that meeting the data rules of different jurisdictions at the same time has become one of the biggest compliance challenges for their global operations.

The third is the governance dilemma of rule output and institutional competition. The differences in these legislative models not only remain at the conceptual level, but also form institutional competition through rule output. Major economies have tried to promote their own data governance models through regional agreements and bilateral arrangements, resulting in the fragmentation of the global rule system. The EU has expanded its influence through the "adequacy recognition" mechanism, the United States has promoted Asia-Pacific regional cooperation through the APEC cross-border privacy rules system, and China has proposed alternative solutions through the Global Data Security Initiative. Although this institutional competition has promoted rule innovation to a certain extent, it has also caused the complexity of the rule system and the surge in compliance costs.

1.3 Blurred boundaries of restrictions on cross-border flow of personal information

How to scientifically define the boundaries of freedom for cross-border flow of personal information remains an important unresolved issue. With the exponential growth of global data flows, the contradiction between the free flow of data and security protection has become increasingly acute. The tension between the free flow of personal information and security protection is essentially the eternal dialectic between the value of freedom and the value of security. As the Enlightenment thinker Locke

said: "The purpose of the law is not to abolish or restrict freedom, but to protect and extend freedom." [5] This legal philosophy principle also applies to the field of data governance. The healthy development of the digital economy requires both sufficient flow of data elements and a sound security mechanism. The two are not a simple zero-sum relationship, but a mutually reinforcing symbiotic relationship: data flow drives economic growth, while sound security protection can enhance the confidence of all parties in participating in data flow.

In the current international rules system, exception clauses based on data sovereignty provide a legal basis for countries to implement regulatory measures, but their vague expression also brings uncertainty in practice. For example, Article 14.11.3 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) allows contracting parties to restrict cross-border data on the grounds of "legitimate public policy objectives", but does not clearly define the concept. Similar problems also exist in Article 12.15.3 of the Regional Comprehensive Economic Partnership (RCEP). Although this legislative technique reserves policy space for countries, it may also lead to inconsistency in the application of rules. Different countries may have significant differences in their understanding of "public policy objectives" and "basic security interests" due to factors such as political systems and cultural traditions. Therefore, future improvements in international rules should focus on clarifying the applicable boundaries between the principle of free flow of data and exceptions, and establishing a more operational balance mechanism.

1.4 Insufficient representation of participants in regional rules

In the international regulatory system for cross-border flow of personal information, the influence of regional rules is still relatively limited, with few participating countries, insufficient democracy and representation, and this may further aggravate the global "digital divide". Taking USMCA, CPTPP, RCEP, and DEPA as examples, these important regional trade agreements have limited coverage and can only constrain the cross-border data flow rules of a few countries and regions. In addition to the above-mentioned regional trade agreements, there are also few participants in other binding cross-border data flow rules. According to the standards of the United Nations Conference on Trade and Development, none of the 47 least developed countries in the world have signed regional agreements involving digital trade. Although 36 of them have joined the WTO, the WTO has not yet formulated complete cross-border data flow rules. Therefore, for these countries, the regionalization and fragmentation trend of data flow regulation may further widen the gap in digital trade development.

It can be seen that the current formulation of cross-border data flow rules is mainly dominated by a few developed countries, and developing countries and least developed countries are not sufficiently involved, resulting in doubts about the representativeness and legitimacy of the rules. Dominant countries often design rules based on their own interests, which may further widen the existing "digital divide" and hinder the balanced development of the global digital economy.

1.5 Enforcement difficulties lead to practical paradoxes in the regulation of cross-border flow of personal information

The legal enforcement of cross-border flow of personal information is facing unprecedented systemic challenges. This dilemma does not stem from the ineffective supervision of a single country, but is rooted in the fundamental contradiction between the transnational nature of data flow and the territorial limitations of law enforcement power. When data shuttles between servers in various countries at the speed of light, the traditional law enforcement mechanism is still firmly bound within the framework of territorial boundaries. This time and space dislocation has created multiple dilemmas in current regulatory practice.

The most prominent enforcement difficulty of cross-border flow of personal information lies in the overlap and conflict of jurisdiction. A simple cross-border data transmission behavior may trigger the EU GDPR, the US CLOUD Act and China's data outbound security assessment requirements at the same

time, and these legal systems have fundamental differences in the standards for determining jurisdiction. The EU adopts the "target-oriented" principle, asserting jurisdiction as long as the data processing behavior involves EU residents; the United States expands its extraterritorial effect through the concept of "data controller"; China uses "data processing activities that affect national security" as the basis for jurisdiction. [6] This difference often causes multinational companies to fall into the paradox of "compliance is illegal" - complying with the laws of one country may mean violating the regulations of another country.

The disconnect between technical architecture and legal tools. The distributed storage characteristics of cloud computing have completely overturned the logic of evidence location in traditional law enforcement. A piece of user data may be split and stored on servers in different countries, and synchronized through blockchain technology. This technical reality makes the traditional legal concept of "data location" meaningless. This technical complexity has also spawned new regulatory avoidance strategies. Some technology companies have begun to adopt a "data nomadic" architecture to circumvent regulatory requirements in specific jurisdictions by migrating data storage locations in real time.

The limitations of cross-border cooperative law enforcement are obvious. The existing cross-border law enforcement cooperation framework seems to be unable to cope with the challenges of new data flows. The traditional mutual legal assistance treaty (MLAT) takes an average of 10.5 months to complete a cross-border data retrieval, which is completely inefficient in the digital economy era. Although some regions have tried to establish fast mechanisms - such as the arbitration system under the EU-US "Privacy Shield" framework and the cooperation arrangements under the APEC cross-border privacy rules system - these mechanisms are often limited by the number of participants or the scope of application.

2. Multi-dimensional analysis of the root causes of the problem

The difficulties faced by legal coordination on cross-border flows of personal information are by no means simple technical differences or differences in rules, but are rooted in deep contradictions in the transformation of national governance paradigms in the digital age. These contradictions reflect both the objective differences in the development stages of the digital economy and the differences in the essential cognition of data rights among different civilizations and traditions, and highlight the structural defects of the global governance system in dealing with new production factors.

2.1 The fundamental difference between values and interests

There are irreconcilable philosophical differences among major economies in the understanding of the nature of data rights. Europe regards the protection of personal information as an important part of basic human rights, a concept derived from its profound humanistic tradition. From the European Convention on Human Rights to the Charter of Fundamental Rights of the European Union, the right to privacy has always been placed at the core of the rights system. This value is projected into the field of data governance, forming a strict protection model represented by GDPR. [7] The Declaration on Digital Rights and Principles issued by the European Commission in 2023 once again emphasized that the protection of basic rights in the digital age should not be weakened by technological development, but requires stronger protection.

In sharp contrast is the pragmatic governance philosophy of the United States. In the legal tradition of the United States, data is more regarded as a market element than a carrier of rights. This cognitive difference has led to the United States and Europe, although both are developed economies, going in opposite directions in data governance. The 2024 Data Flow Assessment Report of the U.S. Department of Commerce bluntly pointed out that over-emphasizing the protection of data rights will undermine innovation vitality, and the United States is more concerned about how to maintain its technological leadership through the free flow of data. This difference exists not only between Europe and the United States. When the European Union tried to globalize its standards, it also encountered doubts from

emerging market countries. Officials from the Indian Ministry of Electronics and Information Technology made it clear at the 2023 World Internet Conference that directly transplanting GDPR standards would hinder the development of the country's digital industry.

Even more complicated is the governance thinking of countries such as China and Russia that include data in the scope of sovereignty. This cognition elevates the issue of cross-border data flow from the commercial field to the level of national security. These three governance philosophies - rights protection, market efficiency and sovereign control - constitute the deepest value obstacles in the current coordination of international rules.

2.2 Objective gap between development stage and digital strength

The disparity in the level of digital economic development has further amplified the ideological differences. The United Nations Conference on Trade and Development's "Digital Economy Report 2023" shows that the United States and China account for more than 70% of the world's hyperscale data centers and top AI researchers, while the Internet penetration rate in Africa is still less than 40%. [8] This digital divide has led to different interests among countries on the issue of cross-border data flow.

Developed countries, relying on their technological advantages, are more inclined to promote the free flow of data. Research by the United States International Trade Commission shows that restrictions on data flow will cause the US cloud computing industry to lose about $12 billion annually. Therefore, the United States has vigorously promoted its data flow agenda through trade agreements such as the USMCA. In contrast, developing countries face a dilemma. An internal report of the Brazilian Ministry of Economy in 2023 estimated that if data flow is fully opened, the country's digital service trade deficit may expand by 35%. This realistic consideration has led developing countries to often adopt defensive legislation and protect immature industries through measures such as data localization.

The technological generation gap also creates an asymmetry in rule-making capabilities. The EU, relying on its single market advantages, is able to transform GDPR standards into de facto global norms. Data from the Center for European Policy Studies show that in the past five years, at least 47 countries have referred to the GDPR framework when revising their data protection laws. In contrast, although African countries passed the Malabo Data Protection Convention in 2023, it is difficult to exert actual influence due to the lack of market bargaining chips. The Matthew effect of this rule-making ability further solidifies the existing inequality.

2.3 Institutional defects in the governance system and power structure

The current international governance framework seems to be unable to cope with the challenges of data flow. On the one hand, traditional international organizations have insufficient representation. In the WTO e-commerce negotiations, the participation of the least developed countries is less than 30%, which makes it difficult for their concerns to be reflected in the text of the rules. On the other hand, emerging governance mechanisms are facing the dilemma of fragmentation. As of 2024, there are 23 regional data flow arrangements in the world, and there is a lack of effective connection between these mechanisms.

The game between major powers has further exacerbated the shortage of institutional supply. The competition between the United States and Europe for the dominance of data rules has risen from a simple struggle for commercial interests to a competition of value systems. The "Transatlantic Data Governance Report" released by the German Marshall Fund in 2024 pointed out that Europe and the United States have obvious differences on 108 data governance issues. Although this competition has spawned innovations such as APEC-CBPR and the EU's "adequacy determination", it has also led to the increasing complexity of the international rules system.

More fundamentally, the existing international legal framework is difficult to adapt to the transnational characteristics of data flow. Research by the Hague Conference on Private International Law shows that 78% of cross-border data disputes currently face unclear applicable laws. When data flows in real time in the cloud, the traditional principle of territorial jurisdiction can no longer provide definitive guidance.

This institutional lag forces countries to turn to unilateral measures, further exacerbating the fragmentation of rules.

The governance dilemma of cross-border flow of personal information is essentially a manifestation of the pain of the digital transformation of the global order. As a new production factor, the governance rules of data have not yet formed a stable paradigm like goods trade. As countries grope forward, they will inevitably project existing governance concepts, development demands and strategic considerations into this emerging field.

The concept of "Digital Westphalia" proposed by the Cambridge University Digital Governance Research Center in 2024 is quite inspiring. The theory holds that countries are trying to impose traditional sovereignty logic on Internet governance, and through data localization, content review, technology decoupling and other means, replicate "territorialization" control in digital space. Data flow governance is undergoing a process of order reconstruction similar to the formation of the modern nation-state system. In this process, ideological conflicts, power gaps and institutional defects together constitute the deep-seated motivations of the current dilemma.

The EU's Digital Sovereignty Strategy (2020) and China's "cyber sovereignty" advocacy are both considered by scholars as practical cases of "Digital Westphalia". This concept profoundly reveals the core contradiction of current global Internet governance: the conflict between technology without borders and politics with territories. Only by recognizing these structural factors can we find truly effective solutions.

Conclusion

Through a systematic review of international practices and existing problems in the legal regulation of cross-border flow of personal information, we can clearly see that the global rule system is facing profound fragmentation, value conflicts and enforcement difficulties. The differences in legislative concepts, regulatory frameworks and law enforcement logic in different jurisdictions not only reflect the strategic choices of countries in the field of digital governance, but also reveal the fundamental tension between data globalization and sovereign control. Research shows that the current international community has not yet found a governance path that can effectively balance the free flow of data, the protection of individual rights and national security. The root cause of this dilemma lies in both the structural contradiction between technological iteration and legal lag and the inherent defects of the international rule coordination mechanism.

In the face of these challenges, the future governance path needs to break through traditional thinking and conduct innovative exploration in the following aspects:

First, a hierarchical and classified regulatory framework should be established. Differentiated flow rules should be designed for data types with different risk levels: a loose "accountability system" can be adopted for general commercial data; "adequacy protection" requirements should be implemented for sensitive personal information; and special control should be applied to key data involving national security. This refined governance model can not only protect important interests, but also avoid the efficiency loss caused by "one size fits all".

Secondly, promote the formation of a "modular" international rules system. Learn from the "positive list" approach of the WTO's General Agreement on Trade in Services, allowing countries to independently choose the degree of commitment according to their development level. At the same time, establish interoperable institutional modules in specific areas such as certification mechanisms (such as APEC-CBPR) and dispute resolution, so that the rules of different camps can be gradually connected.

Third, strengthen capacity building and technical assistance in developing countries. Through platforms such as the United Nations Conference on Trade and Development, help countries with weak digital infrastructure to improve their regulatory capabilities and avoid being marginalized in the rule-making

process. In particular, support the least developed countries to establish a personal information protection system that adapts to their development stage, rather than simply transplanting the standards of developed countries.

Fourth, innovate cross-border law enforcement cooperation mechanisms. Explore the establishment of a permanent "data governance dialogue platform" to provide daily communication channels for regulators; develop an electronic judicial mutual assistance system to shorten the time cost of cross-border data retrieval; and pilot "fast track" procedures in areas such as cybersecurity incident response.

Finally, it should be emphasized that the ideal cross-border data flow governance framework should have dynamic adaptability. With the advancement of technology and the deepening of cognition, the rules system needs to maintain the necessary flexibility and make timely adjustments through a regular evaluation mechanism. The evolution of the EU-US privacy framework shows that even if there are fundamental value differences, a balance can still be found through continuous dialogue and pragmatic compromise.

In short, solving the regulatory dilemma of cross-border flow of personal information is not only related to the development potential of the digital economy, but also affects the fairness and sustainability of the global digital governance order. This requires the international community to transcend zero-sum thinking and jointly explore a new governance paradigm that is both principled and flexible on the basis of recognizing multiple values. Only in this way can we truly achieve the global optimization of data elements while safeguarding the multiple value goals of individual rights, corporate interests and national security.

.

REFERENCES

1. Chander, A. How Law Made Silicon Valley [J]. Emory Law Journal, 2014, 63(3): 659.
2. UNCTAD. Digital Economy Report 2021: Cross-border Data Flows and Development: For Whom the Data Flow [R/OL]. https://unctad.org/system/files/official-document/der2021_en.pdf/2025-04-12.
3. Song Yunbo. Review of DEPA’s Rules on Cross-border Flow of Personal Information and Adaptation of Chinese Law [J]. Legal Science, 2024(1): 136-137
4. Aguerre, C. Digital Trade in Latin America: Mapping Issues and Approaches [J]. Digital Policy, Regulation and Governance, 2019, 21(1): 14.
5. Yao Xu. EU Cross-border Data Flow Governance - Balancing Free Flow and Regulatory Protection [M]. Shanghai: Shanghai People's Publishing House, 2019: 53.
6. Cai Yacen. Game of rules on cross-border data flow between the United States and Europe from the perspective of data sovereignty and its implications for China [J]. Journal of International Law, Issue 2, 2025, pp. 81-88.
7. Wu Xuan. Construction of cross-border rules for personal information from the perspective of data sovereignty [J], Tsinghua Law Review, 2021. Vol. 15. (3): 86-87