Exploring Legal Differences and International Harmonization Paths of Cross-Border Data Flows

Hongfan Jin
East China University of Political Science and Law, Shanghai, China

Abstract: Taking the similarities and differences in the legal regimes of cross-border data flows and their international harmonization as an entry point, this project takes China, the United States and the European Union as examples to study the key differences in data protection and cross-border flow regulation, and to reveal the intrinsic causes of their cultural values, economic structures, legal traditions and national security sovereignty. The analysis shows that although there is some room for collaboration between different countries in terms of basic security boundaries and tools, the hierarchical contradiction of values and the competition between digital countries and "digital nations" make it very difficult to completely eliminate the existing legislative differences. This project intends to explore the governance challenges faced by AI, blockchain and other emerging industries from the perspective of international organization coordination, mutual recognition of regional rules, vertical industry cooperation and technical norms, and to establish an international governance system that coordinates "science and technology, legal system and morality", so as to achieve the coordination of multiple goals, such as innovation incentives, national security and balanced interests.

Keywords: Cross-Border Data Flow; Legal Differences; International Coordination; Data Sovereignty

1. Analysis of Legal Differences

This article adopts a comparative analysis, using case studies and literature reviews to investigate the legal differences among the three economies.

1.1 European Union: Privacy-First Human Rights Protection Model

The European Union has constructed a "privacy-first" human rights protection model with the General Data Protection Regulation (GDPR), which grants data subjects the core rights of access, rectification, and deletion through the framework of "express consent+ broad authorization," and sets a penalty mechanism of up to 4% of global annual revenue or 20 million euros, which will be the maximum penalty for the data subject to access, correct, and delete data. With a penalty mechanism of up to 4% of global annual revenue or 20 million euros, the GDPR establishes personal privacy as a non-transferable fundamental right. Typical cases such as GDPR penalized Facebook for transmitting data to its parent company in the U.S. without explicit authorization from users, highlighting its strict regulatory logic. On this basis, the EU realizes cross-border data governance through a multi-level compliance system of "whitelisting+ Standard Contractual Clauses (SCCs)+ Business Rules for Constrained Companies (BCRs)": only countries such as South Korea and Japan, which have obtained "adequacy determinations", are required to open up their data flows, while non-whitelisted countries are required to open up their data flows through the white-listed countries. Non-whitelisted countries are required to fulfill GDPR requirements through standard contracts or internal compliance mechanisms. 2020's Schrems II decision completely rejected the U.S. Privacy Shield, requiring companies to refuse to cooperate with U.S. government data access requests, further strengthening the judicial system. The "Schrems II" ruling in 2020 completely rejected the U.S. "Privacy Shield Agreement" and required enterprises to refuse to cooperate with the U.S. government's data access requests, further strengthening the tension between judicial sovereignty and the free flow of information, and embodying the European Union's logic of human rights protection as the core of data governance[1].

1.2 U.S.: Market-Driven Model with Industry Autonomy

The U.S. data protection model is centered on industry autonomy and market-driven, emphasizing privacy governance through industry self-regulation and technical means. In specific areas such as medical data (e.g., HIPAA) and online privacy for minors (e.g., COPPA), the state supports industry self-regulation (e.g., advertising industry organizations) with the role of a "night watchman" and relies on privacy-enhancing technologies (e.g., Apple's "Program Tracking Transparency" (ATT) feature) to confer privacy protection on minors. The state supports industry self-regulation with a "watchdog" role (e.g., advertising industry organizations) and relies on privacy-enhancing technologies (e.g., Apple's "App Tracking Transparency" feature) to give users optional tracking privileges, reflecting the logic of privacy protection driven by market competition. Remove data localization requirements under Section 19.17 of the U.S.-Mexico-Canada Agreement to facilitate cross-border data flows and reduce cross-border barriers by relying on DEPA's principle of non-discriminatory data access. Enterprises need to pass the "mutual recognition" mechanism to enter the U.S. market (e.g., AWS, Microsoft cloud service certification), but the Restriction Act's polarizing controversy between "free flow of data" and "national security" is a major concern for the U.S. market. However, the Restriction Act's polarizing controversy over "free flow of data" and "national security" is still widely discussed [2].

1.3 China: A Sovereign Governance Model that Emphasizes Both Security and Development

China has constructed a governance framework combining "classification and sovereignty supervision" through the Personal Information Protection Law and the Data Security Law, requiring data processors to fulfill security obligations such as encryption and auditing, and safeguarding data sovereignty through the Data Exit Security Assessment Mechanism, so as to incorporate the protection of personal information into the national security system. For example, processors with more than one million users' information are required to undergo cybersecurity review if they are listed outside the country. On this basis, a compliance path of data exit security assessment, third-party certification, and signing of standard contracts has been formed: critical data exit must be assessed by the Ministry of Industry and Information Technology (MIIT), and non-critical data can be verified for compliance by signing a Standard Contract for the Exit of Personal Information or by a certification body. Pilot regions such as Beijing and Shenzhen have explored mechanisms to facilitate cross-border data flow, allowing enterprises certified by the National Financial Certification Center to be exempted from security assessment, reflecting the governance concept of "risk control, openness and innovation"[3].

2. Reasons for Legal Differences

The legal differences in transnational data flow stem from the multiple collisions of cultural values, legal traditions and security demands: the EU is centered on the human rights protection of "privacy first", and influenced by Enlightenment thinking, the right to privacy is regarded as a basic human right (e.g., the right to self-determination of information established by the German Constitution), and the right to self-determination is recognized by the GDPR through the GDPR. "The EU has built a strict data governance framework through the GDPR, giving data subjects the right to access and delete data, and reinforcing compliance with fines of up to 4% of global revenue[4]. Its legal system reflects the codification tradition of the Roman law system (e.g., Article 88 of the GDPR), requiring companies to embed privacy protection (Privacy by Design) in the design phase, and delineating "digital boundaries" through the Digital Services Act, requiring multinational platforms to submit algorithmic training data, and using "regional sovereignty" as the basis for compliance. The logic of "regional sovereignty" restricts the cross-border flow of data and strengthens the defense of data sovereignty. In contrast, the U.S. pursues a "market-driven" pragmatism model, with privacy protection aimed at balancing individual freedom and commercial efficiency (e.g., the "reasonable expectation of privacy" established in Katz), and relying on Silicon Valley's "reasonable expectation of privacy"[5]. Its privacy protection is aimed at balancing individual freedom and commercial efficiency (such as the "reasonable expectation of privacy" established in the Katz case), and it relies on the

Silicon Valley tech giants (Meta, Amazon) to build a mechanism of "rule spillover", and it has passed the Cloud Act and other laws to require foreign companies to provide overseas data to the U.S., which has essentially legitimized the implementation of data hegemony. The law traditionally adopts the case law model of the common law system, and promotes privacy protection with state-level legislation such as California's CCPA/CPRA, forming a flexible legislative path of "issue orientation", and at the same time, the Foreign Corporation Accountability Act (PCAOB) is used to regard information flow as a strategic weapon, forcing enterprises to hand over competitors' information, reflecting the logic of sovereignty expansion by using market power as a tool. The PCAOB is also used as a strategic weapon to force companies to hand over information about their competitors, reflecting the logic of sovereign expansion using market power as a tool. As the world's second-largest digital economy (with a GDP of more than $7 trillion), China has built a data governance system through the legalization of policies based on the principle of "equal emphasis on both development and security". The legal system integrates the features of civil law with the policy orientation, and the Data Security Law establishes a categorization and grading system for protection, with standards dynamically formulated by the net information department, reflecting the combination of flexibility and controllability. The Law on Data Security establishes a categorized and graded protection system, with standards dynamically formulated by the net information department, reflecting a combination of flexibility and controllability. At the level of security and sovereignty, China has incorporated data sovereignty into the national security framework, stipulating that national security assessment is required for the exit of major data through the Network Data Security Management Regulations, and requiring the State Council's approval for the exit of geographic information data in the Outline of the Plan for the Ecological Protection and High-Quality Development of the Yellow River Basin to strengthen data sovereignty with the concept of "new borders". The concept of "new border" reinforces data sovereignty. Its governance logic emphasizes the "homogeneity of the family and the state" and prioritizes social order and the public interest, such as in the case of DDT, where regulation was strengthened on the grounds of the public interest, reflecting governance choices in the context of a collectivist culture. This difference is essentially a concentrated manifestation of the multiple value conflicts between individualism and collectivism, codification and case law tradition, and national security and commercial interest priority[6].

3. Exploration of Coping Strategies and Coordination Paths

To address the conflict between the EU and the U.S. over privacy protection and business efficiency, this article proposes solutions through regional cooperation and technological platform innovation.

3.1 Strengthening Domestic Legislation and Regulation

In the conflict between individual privacy, commercial freedom and national security, a hierarchical governance framework needs to be constructed through domestic legislation. For core sensitive information such as military, biological and geographic information, a "one-vote veto" mechanism should be established, such as China's "Measures for the Management of Data Security" which prohibits the cross-border transmission of military geographic information; for non-confidential business data, the "principle of proportionality" should be used to balance the interests of the business, such as the European Union's "Digital Marketplace Act" (DMA). For example, the EU's Digital Markets Act (DMA) allows large platforms to share customer information with competitors, but requires that privacy risks be mitigated through technical means such as information desensitization and anonymization. In terms of remedies for individuals' rights and interests, the Hague Convention on Choice of Court Agreements can be used as a reference to set up an arbitration mechanism for cross-border data disputes, allowing data processors to independently choose the court of jurisdiction and giving the decision extraterritorial effect, thus providing a predictable judicial path for global data disputes. This legislative design not only strengthens the bottom line of national security and privacy protection, but also realizes the reasonable space for commercial freedom through hierarchical governance and technical rules, and ultimately achieves a dynamic balance of multiple interests[7].

3.2 Promoting Regional Cooperation and Integration

Establish a "World Data Development Fund" led by the World Bank and the International Monetary Fund, with developed countries contributing a certain percentage of their GDP, mainly to support developing countries' data infrastructure (e.g., building regional data centers in African countries) and compliance capacity (e.g., training data managers in Southeast Asian countries)[8].

By establishing a new model of "technology transfer, capacity building and regulation implementation", China's Digital Silk Road can connect with the European Declaration on Digital Rights and Principles, provide technical support for information security in Central Asia and the Middle East, and participate in the relevant ISO/IEC norms, so as to change the situation in which "the rules of international trade are monopolized by developed countries". International trade rules are monopolized by developed countries"[9].

3.3 Corporate Compliance and Self-Regulation

Deloitte's Global Data Compliance Platform has integrated regulatory rules from over 140 countries and territories, and is up-to-date with the latest regulatory changes (e.g., UK-GDPR in the context of the UK's post-Brexit GDPR). Through the API interface, organizations can embed regulatory requirements into their own databases to "automatically trigger regulatory scrutiny of financial flows".

Data moving across borders is managed through a third party (e.g. Data Trust Center in Singapore), with rights divided according to the respective jurisdictions: GDPR for users in Europe, CCPA in the U.S., and the Personal Information Protection Act in China, in a way that reduces compliance with the "centralized storage of physical+ logical authorization separation". " approach to reduce the complexity of compliance[10].

4. Summarizing

Legal differences in cross-border data flows stem from the intersection of cultural values, legal traditions, and security concerns. The EU takes "privacy first" as the core, builds a strict human rights protection framework through GDPR, and closely integrates data sovereignty with judicial sovereignty; the U.S. relies on market-driven, balances commercial efficiency and privacy protection with industry self-regulation and technical means, and strengthens digital hegemony through "rule spillover"; and the United States relies on market-driven, industry self-regulation and technical means to strengthen digital hegemony through "rule spillover". The United States relies on market-driven, industry self-regulation and technical means to balance commercial efficiency and privacy protection, and strengthens digital hegemony through "rule spillover"; while China takes the sovereignty governance model of "equal emphasis on security and development" to embed data sovereignty into the national security system, and realizes openness with controllable risks through the classification and grading system and pilot innovation. This difference not only reflects the value conflict between individualism and collectivism, but also highlights the institutional divide between codification and case law paths, and reflects the tension between national sovereignty and global data flow in the digital era. In order to cope with this challenge, it is necessary to explore the possibility of coordination through the strengthening of domestic legislation (e.g. hierarchical governance and arbitration mechanism), the promotion of regional cooperation (e.g. technology transfer and mutual recognition of rules), and the innovation of corporate compliance (e.g. technology platforms and data trusts). In the future, only through the coordination of international organizations, technological innovation and balancing of interests under the framework of "science and technology, rule of law and morality" can we achieve a dynamic symbiosis of privacy protection, national security and the development of digital economy.

References

[1] Lu, Chunyi. Cross-border Data Flow Restrictions, Trade Costs and Digital Service Exports [D]. Nanjing University of Finance and Economics,2024.

[2] Drozd A. Cross-border data sharing: implications for the legal profession in the context of government access to data and protection of legal professional privilege[J]. Journal of Cyber Policy,2024,9(1):52-62.

[3] Zhao, J.. The boundary of legal regulation of

cross-border data flow[D]. People's Public Security University of China,2023.

[4] Bai Fangyan. International governance of digital trade and its response [D]. University of International Business and Economics,2023.

[5] Wang Lingdong. Research on the Improvement of the Legal System of China's Outbound Data Evaluation [D]. East China University of Politics and Law,2022.

[6] Alexia P ,Elena P R .Cross-Border Data Protection Through Collective Litigation: an EU Legal Maze?[J]. European Data Protection Law Review,2021,7(4). 550-559.

[7] Wu Yi. Comparative Study on the Rules of Cross-border Flow of Personal Data between Europe and the United States [D]. Southwest University of Political Science and Law,2020.

[8] D A M, Neha M. Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute[J]. Journal of International Economic Law,2019,22(3):389-416.

[9] Zhang Rudder. Research on legal regulation issues of cross-border data flow[D]. University of International Business and Economics,2018.

[10] BDO Consulting; Legal Concern Over Cross-Border Data Privacy Regulations Spikes-BDO Survey[J].Information Technology Newsweekly,2017,46-.

