# Under National Security Conflicts: A Balanced Model for Cross-Border Data Free Flow and Privacy Protection

Tong Kang
*Faculty of Law, Zhongnan University of Economics and Law, Wuhan, Hubei, China*

Keywords: National Security Conflicts, Cross-Border Data Free Flow, Regulation, Privacy Protection.

Abstract: The free flow of cross-border data possesses significant economic growth implications. As in-dividual rights awareness strengthens and nations increasingly prioritize sovereignty, the free movement of cross-border data faces impediments under the context of national security conflicts. This paper employs a literature review method to summarize scholars proposed solutions for balancing the conflict between cross-border data protection and free flow. Through comparative analysis and case studies, it examines the regulatory models of the United States, the European Union, and China regarding cross-border data governance. Key cases analyzed include the invalidation of the EU-US Privacy Shield Agreement and the subsequent Trans-Atlantic Data Privacy Framework. Building upon these analyses, the study proposes a balanced cross-border data governance model aimed at achieving a tripartite equilibrium among privacy protection, national security, and digital economic development. This model seeks to reconcile data flow efficiency with security, safeguard the rights and interests of all stakeholders.

## 1 INTRODUCTION

E-commerce, financial services, healthcare and public health, scientific research and education, artificial intelligence and big data analytics, among others, have seen the pervasive integration of cross-border data applications across diverse domains. Furthermore, with the advancement of technologies such as the internet, cloud computing, big data, 5G, artificial intelligence, and blockchain, coupled with the acceleration of globalization and digitalization, cross-border data, as an extension of national sovereignty in cyberspace, is playing an increasingly pivotal role. However, cross-border data flows are caught in the fragmented international rules concerning data sovereignty, privacy protection, and national security. A balance between privacy protection and the free flow of data still needs to be struck. The research report utilizes literature review, comparative analysis, and case study methodologies to synthesize the discussions on cross-border data issues by various scholars. It also summarizes and analyzes the regulatory frameworks for cross-border data protection in the United States, the European Union, and China, highlighting their functionalities. Currently, case analyses are conducted based on the invalidation case of the Privacy Shield Agreement in Europe and the United States, as well as the Transatlantic Data Privacy Framework. These analyses aim to explore the definitions and relationships of cross-border data sovereignty and cross-border data privacy rights, and to elucidate the significant issues currently faced by cross-border data privacy rights. Summarize the relief mechanism, balance the free flow of data and privacy protection, and propose the construction path of the balance model based on the difficulties faced.

## 2 LITERATURE REVIEW

With the acceleration of the information age and globalization process, cross-border data privacy protection, as an extension of national sovereignty at the information level, faces the main problem of fragmentation of relevant international rules. Many scholars have proposed different coping methods. Building upon John Jackson's concept of 'modern state sovereignty,' scholars have proposed a multi-layered governance framework for cybersecurity under modern sovereign decision-making. This approach emphasizes state sovereignty over critical



Kang, T.
Under National Security Conflicts: A Balanced Model for Cross-Border Data Free Flow and Privacy Protection.
DOI: 10.5220/0014385000004859

In *Proceedings of the 1st International Conference on Politics, Law, and Social Science (ICPLSS 2025)*, pages 482-487
ISBN: 978-989-758-785-6

domains in data protection, allocating different cybersecurity decision-making powers by delineating the relationships between governance entities and security requirements (Chu, 2025). To some extent, its viewpoint can address the fragmentation of privacy protection rules for cross-border data circulation in the international arena. However, due to the complexity of the subjects and the uncertainty of the international situation, their practicability is rather weak. Some scholars have put forward the idea of employing blocking statutes (laws at a higher hierarchical level) to restrict unilateral cross-border data enforcement actions and long-arm jurisdiction.

This viewpoint can be effective in addressing relevant issues, but at the same time, considerations such as legal compliance and international recognition need to be taken into account, as a singular legislative approach cannot systematically and effectively resolve practical problems (Liao, 2025). Some scholars have proposed that non-traditional security should be applied as an exception clause for the protection of cross-border data security (Chen, 2024). However, existing data protection frameworks have limitations in addressing the divergent health privacy regulations across EU member states and ensuring compliance with the U.S. Health Insurance Portability and Accountability Act. This limitation necessitates a cautious and informed approach to data compliance practices, particularly where strict adherence to the General Data Protection Regulation is required. To address this, it is advisable to integrate relevant provisions from EU Standard Contractual Clauses, Model Data Use Agreements, and Business Associate Agreements to establish a more complementary compliance framework. Such integration would help bridge existing gaps in the current system and ensure more comprehensive compliance in data sharing (Tschider, 2024). It is believed that in the EU data protection law, as long as these rights are guaranteed, data transmission is allowed. This implies that the EU's data transmission regulation based on fundamental rights can be reasonably regarded as data protection rather than data protectionism (Naef, 2023). Building on the above, under the theory of sovereign concession for international cooperation, it is imperative to adopt a long-term perspective in calibrating the extent of sovereignty relinquished. Core sovereign interests must be safeguarded, with particular attention paid to defining the boundaries for cross-border data free flow within this framework.

# 3 BALANCING CROSS-BORDER DATA FLOWS AND PRIVACY RIGHTS

## 3.1 Cross-Border Data Privacy Rights and Cross-Border Data Sovereignty

The relationship between cross-border data privacy rights and cross-border data sovereignty is characterized by both contradiction and consistency. Its contradiction lies in the fact that for the purpose of safeguarding the overall interests of the nation, such as maintaining social order, ensuring public safety, promoting economic development, and protecting national security, the state may acquire individuals' private data in areas like energy, transportation, and healthcare, or access necessary personal data in cases involving illegal crimes. Moreover, data free flow is possible, including for individuals and enterprises, which may be subject to some degree of restrictions by the authorities. Consistency is reflected in three aspects. Firstly, cross-border data privacy rights and cross-border data sovereignty have overlapping goals. Both are centered on security, with personal privacy protection aiming to prevent data abuse that leads to damage to individual rights and interests, while data sovereignty aims to maintain social order, national security and economic stability.

Secondly, there are overlapping areas between the protections afforded by cross-border data privacy rights and national sovereignty. These overlaps are evident in aspects such as the handling of personally sensitive information, data pertaining to critical infrastructure, and data related to national security. Thirdly, the two approaches have a synergistic effect in terms of protection methods. For instance, there is an overlap in the legal framework, and through the sharing of technical means such as anonymization or de-identification, valuable data can be provided for public research while protecting personal privacy. It is worth noting that purely personal data within individuals' privacy that does not involve national security interests, such as consumption habits, daily chat records, media/social activity data, as well as enterprise data involving trade secrets and belonging to corporate assets, constitute non-overlapping parts with the primary protection scope of national sovereignty. When it comes to data cross-border flow, given that protecting the data sovereignty of one's own country often restricts the free cross-border flow of data, while protecting the cross-border data sovereignty can largely safeguard the cross-border data privacy rights.

### 3.2 In the Context of National Security Conflicts, the Contemporary Predicament Faced by Cross-Border Data

With the advent of the digital age and the acceleration of globalization, data application scenarios penetrate all aspects. As individuals' awareness of rights has increased and countries have placed greater emphasis on autonomy, under the conflict of national security, the free flow of cross-border data is hindered and mainly faces the following two problems. First, the fragmentation of cross-border data privacy protection rules. Different countries have adopted distinct protection models, primarily forming three representative approaches exemplified by the United States, the European Union, and China. Meanwhile, there are currently 237 data protection frameworks globally (OECD, 2023), giving rise to an institutional competition between the Brussels Effect and the "Washington Consensus. The issue has resulted in unilateral mechanisms dominating, regional agreements fragmenting, and multilateral mechanisms being absent. The fragmentation of international rules on cross-border data forces multinational enterprises to comply with varying standards for data storage, transmission, and usage during their global operations. This significantly increases compliance costs, with even minor mistakes potentially leading to hefty fines.

Meanwhile, the addition of cross-border data approval procedures and time delays have hindered real-time data interaction, reduced the efficiency of cross-border business, and restricted the global coordinated development of the digital economy. Second, on the basis of prioritizing national sovereignty, when data flows involve national security concerns, the protection of privacy rights often yields to national interests, resulting in restrictions on the free cross-border movement of data. For instance, China's Data Security Law mandates security assessments for the outbound transfer of important data, which has sparked concerns among multinational enterprises (MNEs) regarding the usability and accessibility of their data. Under the intensification of sovereignty claims, extraterritorial jurisdiction has led to conflicts. For instance, the U.S. CLOUD Act permits accessing data stored on overseas servers, which directly clashes with the territorial principle of the EU's GDPR. A typical case is the Microsoft Ireland Server Data Case.

### 3.3 Comparison of Cross-Border Data Flows Among the United States, the European Union and China

The United States adopts pragmatism and long-arm jurisdiction as its legislative philosophy, asserting that data sovereignty equates to control. Its policy is characterized by double standards, externally advocating for free data flows to absorb global data, while internally strengthening cross-border data regulation under the pretext of national security. Advocates of data free flow, leveraging technological superiority and perceived data hegemony, prioritize economic interests by extending jurisdictional reach through legislation such as the CLOUD Act to govern extraterritorial data. Concurrently, they employ export controls and foreign investment reviews to restrict access to and transfer of sensitive data, thereby solidifying U.S. dominance in the global data ecosystem. The European Union advocates rule-based governance and privacy sovereignty, emphasizing strict privacy protection and regulatory export. At its core, the General Data Protection Regulation (GDPR) underscores the adequacy decision for personal privacy and data (European Commission,2025). The extraterritorial application expands the influence of rules, including Standard Contractual Clauses (SCCs), and strengthens compliance requirements for multinational enterprises by coordinating member state actions through the one-stop supervision mechanism (European Commission,2010). China advocates prioritizing data sovereignty security and achieving independent controllability. Based on the Cybersecurity Law, Data Security Law, and Personal Information Protection Law, it emphasizes localized data storage and outbound security assessments to balance national security with digital economic development. Furthermore, it explores projects such as East Data West Computing to optimize data distribution, while promoting international data cooperation rules through frameworks like the "Belt and Road" initiative. Different models are constructed based on their historical traditions, core values, and national interests.

The ongoing clash between regulatory frameworks has been starkly demonstrated through the annulment of the EU-US Privacy Shield and its subsequent replacement by the Trans-Atlantic Data Privacy Framework (Fefer & Archick, 2022). In a pivotal 2020 judgment (Case C-311/18), the CJEU revoked the Privacy Shield's adequacy status, determining that US surveillance laws—notably Section 702 of FISA permitting non-citizen

monitoring without judicial warrants—created disproportionate risks for EU data subjects. This judicial determination highlighted fundamental incompatibilities between American intelligence-gathering practices and GDPR's stringent requirements for data protection enshrined in Articles 45-49 (European Parliament & Council, 2016). Despite diplomatic assurances regarding surveillance limitations, critics note that Section 702's authorization of bulk data contravenes GDPR's principles of proportionality and purpose limitation. This regulatory upheaval precipitated significant operational challenges for transatlantic commercial exchanges, forcing organizations to adopt alternative compliance strategies under Chapter V GDPR provisions (U.S. Congress, 2024). The Schrems II decision essentially created a compliance vacuum that persists despite the new framework's implementation, underscoring the need for legislative alignment between jurisdictions. The EU implemented alternative measures like Standard Contractual Clauses (SCCs) and Binding Corporate Rules (BCRs) to fill the regulatory gap created by the invalidation of Privacy Shield. Rather than hastily implementing Privacy Shield 2.0, the European Commission would have been more prudent to persist in discussions with US counterparts to resolve the documented deficiencies. Any new framework should only be established when the adequacy determination demonstrates sufficient legal durability to survive potential legal challenges before the Court of Justice of the European Union-a standard that Privacy Shield 2.0 ultimately failed to meet (Gerke & Rezaeikhonakdar, 2023). Furthermore, enacting comprehensive data protection legislation in the US that aligns with CJEU standards could help ensure the continuity of data transfers across the Atlantic (Fahey & Terpan, 2023).

# 4 CONSTRUCTION PATHWAY OF THE BALANCED MODEL

## 4.1 Governance Framework: A Risk-Based Hierarchical Dynamic Control System

### 4.1.1 Data Classification and Tiering Mechanism

The data classification and grading model is designed to ensure the security and compliance of data during cross-border flow. Data is classified into three categories based on their importance and potential harm, core data, important data and general data. In terms of national security red lines, core data has clearly defined data types prohibited from being transferred abroad. Through the negative list, strict boundaries are drawn for data prohibited from being transferred across borders. Core data typically involves the nation's core interests and major security concerns, such as military deployments, biological genetic information, nuclear facility data, etc. For sensitive data, this system has established a list of sensitive data and requires that these data must undergo security assessment before being exported. Data in key fields such as finance and energy are usually classified as sensitive data because they are related to the economic lifeline and social stability of the country. The purpose of the security assessment is to ensure that the data can be adequately protected after being exported, preventing data leakage or abuse. For general data, the system establishes a whitelist mechanism that allows compliant enterprises to freely transfer data. These enterprises typically need to meet certain data protection standards and certification requirements, such as obtaining certification under the Cross-Border Privacy Rules system. Through the whitelist mechanism, these enterprises can freely engage in cross-border data flows in compliance with relevant regulations, thereby facilitating international trade and cooperation.

### 4.1.2 Dynamic Risk Assessment Model

Based on the classification of data into core data, sensitive data, and general data, risk levels are delineated with reference to the European Union's EDPB classification system, followed by differentiated control measures. The construction of a national data protection level index should focus on core indicators such as the legal environment, enforcement intensity, and international cooperation to dynamically assess the data protection capabilities of various countries. Based on the evaluation results, adjustments should be made to the scope of cross-border data transmission. This index can draw on the adequacy decision mechanism of the EU's GDPR and requires data recipients to obtain international certification, or deploy technologies such as encryption and blockchain traceability, to reduce the risk of data leakage. On this basis, introduce artificial intelligence for real-time monitoring and early warning, use machine learning to analyze abnormal patterns in data flows, identify potential abnormal phenomena such as high - frequency cross - border

transmissions and unconventional accesses, and recognize potential abusive behaviors. We can refer to the CDM project of the US CISA. It continuously diagnoses network traffic and marks suspicious activities in real time. Through sensors and tools deployed in the networks of federal agencies, the CDM project continuously collects data such as network traffic, device status, and user behavior, and integrates them into a unified federal control panel. The control panel provides host-level visibility, enabling CISA to identify anomalous traffic patterns and flag potential threats within minutes. It can also generate incident reports and push remediation recommendations, forming a monitoring-response-remediation closed loop (Michael, 2023).

### 4.2 Market Mechanism: Data Elementization Reform with Incentive Compatibility

The core of the data element reform that is compatible with market mechanism incentives is to build a system that not only conforms to the laws of market economy but also can effectively incentivize the efficient allocation and rational use of data elements. The reform emphasizes establishing a legal foundation for data circulation by clarifying data property rights and defining the rights and obligations among data owners, users, and managers. On this basis, a market pricing mechanism is introduced to form reasonable market prices that reflect the true value of data based on factors such as data quality, scarcity, and application value, thereby promoting data's participation in market distribution as a production factor. Meanwhile, the reform focuses on establishing a fair and competitive data trading environment, breaking data monopolies, encouraging multiple entities to participate in the data market, enhancing data service quality through competition, reducing data acquisition costs, and stimulating market vitality. In order to achieve incentive compatibility, the reform also includes the design of a reasonable revenue distribution mechanism to ensure that data creators, processors, users and the public can receive corresponding returns according to their contributions, forming a positive incentive mechanism to promote the continuous investment and innovative application of data resources. In addition, it is essential to strengthen data security and privacy protection, establish a sound data supervision system, ensure the legality and compliance of data circulation, maintain market order, and enhance the confidence of market participants.

## 5 CONCLUSION

With the advent of the digital age and the acceleration of globalization, data application scenarios have penetrated into all aspects, personal rights awareness has strengthened, and countries have placed greater emphasis on autonomy. This article first clarifies the relationship between cross-border data privacy rights and cross-border data sovereignty, and explains the main problems faced by the free flow of cross-border data when it is hindered due to national security conflicts. These problems mainly include two aspects: one is the issue of data ownership, and the other is the issue of data access rights. Through the literature review method, some scholars summarized the solutions to the balance and contradiction between cross-border data protection and free flow, and The paper focuses on analyzing the structural differences in legislative concepts and implementation paths among the three major regulatory paradigms of the United States' "market-dominant type", the European Union's "rights-based type", and China's "security-priority type". The case analysis part focuses on the iterative process of the data transmission mechanism between the United States and Europe, especially the judicial rejection of the "Privacy Shield" agreement by the Court of Justice of the European Union based on Article 45 of the General Data Protection Regulation (GDPR) in the Schrems II case, as well as the fundamental flaws that persist in the determination of regulatory equivalence in the "Transatlantic Data Privacy Framework" in the subsequent period. Based on the challenges faced, this paper proposes a balanced model construction pathway, establishes a risk-based hierarchical dynamic control system, and promotes incentive-compatible data element reform. It classifies cross-border data into core data, sensitive data, and general data while conducting risk assessments for different data categories. A cross-border data trading market is established, divided into primary and secondary markets, with increased emphasis on privacy protection technologies. Special attention is given to strengthening legal regulations governing the use and circulation of artificial intelligence in cross-border data contexts. At the same time, we will strengthen international cooperation through regional and multilateral agreements and reach more international consensus to form common values to deal with the fragmentation of international rules in this regard, as well as the balance between cross-border data facilitates unrestricted flow and privacy protection. In the future, it is hoped that by contemplating human rights and dignity, responsibility and safety, shared

responsibility, fairness and inclusivity, innovation and efficiency, international cooperation and coordination can be achieved, ultimately realizing the tripartite balance of privacy protection, national security, and digital economic development.

## REFERENCES


Chen, S.Y. 2024. Applicability dilemma of CPTPP security exception clauses under data sovereignty and approaches to mitigate. Cybersecurity and Data Governance 43(7): 95–101.

Chu, T. 2025. Cybersecurity governance in digital trade: Normative framework, practical challenges, and improvement strategies. International Economics and Trade Exploration Advance online publication.

European Commission.2025. Adequacy decisions: How the EU determines if a non-EU country offers adequate data protection. European Commission. https://commission.europa.eu/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en.

European Commission. 2010. Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC of the European Parliament and of the Council. Official Journal of the European Union L 39: 5–18.

European Parliament & Council of the European Union. 2016. Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation). Official Journal of the European Union L 119: 1–88.

Fahey, E. & Terpan, F. 2023. The future of the EU-US privacy shield. In The Routledge Handbook of Transatlantic Relations 221–236. Routledge.

Fefer, R.F. & Archick, K. 2022. U.S.-EU trans-Atlantic data privacy framework (Report No. IF11613). Congressional Research Service. https://crsreports.congress.gov/product/pdf/IF/IF11613.

Gerke, S. & Rezaeikhonakdar, D. 2023. Privacy Shield 2.0: A new trans-Atlantic data privacy framework between the European Union and the United States. Cardozo Law Review 45: 351.

Liao, M.Y. et al. 2025. Security risks in cross-border data law enforcement under the U.S. CLOUD Act and China's response strategies. Library Tribune 45(1): 128–137.

Michael, D. 2023. Evolving CDM to transform government cybersecurity operations and enable CISA's approach to interactive cyber defense. Associate Director for Capacity Building, CISA.

Naef, T. 2023. Data protection without data protectionism: The right to protection of personal data and data transfers in EU law and international trade law. Springer Nature.

Organization for Economic Co-operation and Development (OECD). 2023. Digital security and privacy in the global economy 2023. OECD Publishing.

Tschider, C. et al. 2024. The new EU–US data protection framework's implications for healthcare. Journal of Law and the Biosciences 11(2): lsae022.

U.S. Congress. 2024. Foreign Intelligence Surveillance Act (FISA) Section 702 Reauthorization Act of 2024. Public Law No. 118-XX. https://www.congress.gov/bill/118th-congress/house-bill/XXXX.