

Research on the Security Issues of Enterprise Data Export in China from the Perspective of Foreign-related Rule of Law

Feng Chunyang, Shao Xin'ge*

Abstract: Global data is currently experiencing exponential growth, with its immense productive potential becoming a vital force driving innovation and reshaping public life. For China, advancing high-standard opening-up and stimulating innovation in the digital economy remain key priorities. However, as cross-border data flows have become increasingly frequent, issues of data sovereignty and security have grown more prominent, with international competition gradually extending into this domain. From the perspective of foreign-related rule of law and against the background of great power strategic competition, this study conducts an in-depth examination of the types and sources of security risks in China's enterprise data export. It argues that legal instruments represent the most effective means for data sovereignty competition among great powers. This article analyzes the conflicts of foreign-related rule of law during data export processes and proposes targeted countermeasures from four areas: improving the domestic legal and regulatory system, strengthening diversified international legal cooperation, enhancing corporate compliance capabilities, and advancing pilot innovations in "digital free trade zones". By employing interdisciplinary research methods, this study enriches the theoretical framework of data security and elevates the level of data governance in China.

Keywords: Foreign-related Rule of Law, Cross-border Data Flows, A Holistic Approach to National Security, Great Power Strategic Competition

I. INTRODUCTION

The modern information technology revolution represented by computing, networking and communications has given birth to the digital economy. This new economic form has enhanced efficiency and is emerging as a pivotal driver of global economic recovery. However, as cross-border data flows have become

* Feng Chunyang, Assistant Professor, School of International Police Studies, People's Public Security University of China. Email: 20247113@ppsuc.edu.cn.

Shao Xin'ge, Master Degree Candidate, School of National Security, People's Public Security University of China. Email: shaoxing2003@163.com.

This article is funded by the Fundamental Research Funds for the Central Universities "Research on the Criminal Liability System of US Economic Sanctions against China" (2025JKF02SK27).

increasingly frequent, issues of data security have grown more prominent. Internationally, great power strategic competition is gradually expanding into the realm of data sovereignty, with countries engaged in fierce competition over data ownership, rule-making authority and technological control. Domestically, there have been numerous incidents of critical data breaches in recent years, posing severe threats to national security. Thus, how to effectively regulate cross-border data flows has become an urgent challenge requiring resolution.

China currently stands at a crucial juncture in building a modern socialist country in all respects, and it is necessary to seize the new opportunity of the digital economy in industrial transformation. According to data released by the General Administration of Customs, China's total value of cross-border e-commerce imports and exports in 2024 was 2.63 trillion yuan, representing a year-on-year increase of 10.8%. Moving forward, more enterprises will expand overseas under policy incentives, integrating into the global supply chain of the digital economy to develop foreign trade and investment. Currently, China has established an initial protective framework through a series of laws and regulations, but its response strategy to sanctions and interference from other countries is still not comprehensive and systematic. To address current academic limitations such as a single research perspective and insufficient risk identification, this article starts from the perspective of foreign-related rule of law, combined with the background of great power strategic competition. It answers questions of "What are the security risks of Chinese enterprise data export?" and "How to apply a coordinated approach to the domestic and foreign-related rule of law?", to offer insights for refining data security governance system and advancing high-level opening-up.

II. THEORETICAL FOUNDATIONS OF ENTERPRISE DATA EXPORT

A. Definition of Core Concepts

1. Data Export

Data export is an important component of cross-border data flows, forming

a corresponding relationship with data import. At present, there is no unified definition of this concept internationally. For example, the General Data Protection Regulation (GDPR) of the European Union (EU) defines it as “transfer to a third country or to an international organization”. Broadly speaking, enterprise data export mainly involves the following four situations:

i) Data Transmission: which refers to the electronic transfer of data to overseas servers, such as multinational corporations sending order information to the overseas customers.

ii) Data Access: which refers to permitting overseas entities to remotely access data stored within the country, such as foreign law enforcement agencies requesting digital forensics.

iii) Data Storage: which refers to placing data on overseas physical media, such as using overseas cloud storage services like the Amazon S3 for long-term data preservation.

iv) Data Publication: which refers to releasing information overseas through public channels, such as submitting relevant materials for overseas initial public offering (IPO).

2. Foreign-related Rule of Law

In the Western context, the rule of law is divided into two levels: domestic and international, which are two relatively independent governance systems. However, foreign-related rule of law goes beyond this dualistic thinking, which refers to the legal framework for handling foreign and international affairs by public authorities such as legislative, executive and judicial bodies, as well as private entities including natural persons and legal entities.

In essence, foreign-related rule of law is an external extension of domestic rule of law and an internal manifestation of international rule of law. It encompasses both the aspects of the national legal system related to foreign and international affairs, and the nation's participation in shaping global governance rules. With the deep reshaping of global industrial chains, supply chains and innovation chains, China urgently needs to accelerate the construction of a favorable legal environment that is compatible with high-quality development and high-level opening-up. Therefore, to discuss the security issues of enterprise data export, it is necessary to integrate the background of great

power strategic competition and take a coordinated approach to the rule of law at home and in foreign-related affairs.

B. International Legal Basis for Enterprise Data Export

1. Overview of Relevant Rules of International Law

Currently, data export has become a core issue in international trade. International law, as the fundamental framework for regulating transnational legal relations, clarifies the legal basis and institutional boundaries for enterprise data exports. Its primary forms can be broadly categorized into four types:

i) Specialized international treaties and regional conventions: Such agreements, reached between two or more countries (or regions) regarding cross-border data flow rules, typically carry legal force.

ii) Data export clauses in trade agreements: As of October 2024, there are more than 340 trade agreements worldwide that contain cross-border data flow provisions.

iii) Technical data compliance standards: These standards are technical specifications developed by standard-setting bodies such as the International Electrotechnical Commission (IEC).

iv) Soft law initiatives of international organizations: Such initiatives exert tangible influence on governments and private entities through consensus, demonstration, or voluntary adoption.

Table 1: Examples of International Law Rules for Enterprise Data Export

Type	Name	Year	States/Regions Involved	Characteristics
Convention	The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Revision)	2018	Member States of the Council of Europe	First legally binding international privacy protection convention
Regional Framework	Cross-Border Privacy Rules (CBPR)	2011	APEC members	Requirement for enterprises to adhere to the nine principles of the APEC Privacy Framework
Trade Agreement	The United States–Mexico–Canada Agreement (USMCA)	2020	The United States, Mexico, and Canada	High-standard rules for the free flow of data
Technical Standards	2019 Privacy Information Management (ISO/IEC 27701)	2019	ISO members	A privacy protection management framework
Soft Law Initiative	Global Digital Compact	2023	The UN members	Advocacy for principles of openness, freedom, and security

2. Conflict Between the Data Sovereignty Principle and “Long-arm Jurisdiction”

Data sovereignty is a natural extension of national sovereignty, emphasizing a state's right to control, manage, and protect data within its territory and abroad. Domestically, the state may exercise the highest level of jurisdiction; internationally, it may independently govern data affairs. Correspondingly, “long-arm jurisdiction” refers to the doctrine of extending domestic regulations extraterritorially to govern foreign entities. It constitutes a unilateral abuse of jurisdiction by a sovereign state, essentially aimed at aggregating extraterritorial data resources for strategic advantage. For cross-border data flows, once “long-arm jurisdiction” extends beyond sovereign jurisdiction, it inevitably lacks international legal legitimacy.

3. Balance of Data Free Flow and “National Security Exceptions”

Data free flow refers to the unrestricted transfer of data across jurisdictions without unnecessary restrictions. This proposition is based on the “cyberspace public-domain doctrine”, which posits the virtual boundlessness, non-exclusivity, and openness of data. “National security exceptions” are a cornerstone of multilateral trade law. It permits states to take necessary measures restricting cross-border data flows under specific circumstances to safeguard public order or public interest. It can be said that this provision reserves flexibility for regulatory interpretation of cross-border data flows, while its abuse would create significant obstacles.

C. China's Current Legal Framework of Enterprise Data Export

1. One Fundamental Law

The National Security Law of the People's Republic of China, enacted in 2015, safeguards national security and social stability. It defines the protection scope, principles and responsibilities for national security. Article 25 stipulates that “The state shall build a network and information security guarantee system, improve network and information security protection capability, strengthen the innovation research, development and application of network and information technologies, realize the controllable security of core technologies, crucial

infrastructure, information systems, and data in important fields”. It lays the foundation for the legal regulations of China’s enterprise data export.

2. Three Pivotal Laws

The Cybersecurity Law of the People’s Republic of China, enacted in 2017, marked the first time in China that “data” was treated as a separate legal object. It requires enterprises to comply with data localization requirements. The Data Security Law of the People’s Republic of China, enacted in 2021, marked the first time that China confirmed the legal definition of “data”. It specifies the protection measures for “important data”. The Personal Information Protection Law of the People’s Republic of China, enacted in 2021, was the first comprehensive law in China specifically designed to safeguard personal information. It stipulates the rules for the use, processing and cross-border transmission of personal information.

3. Multiple Implementing Rules

On the basis of the above national laws, the Cyberspace Administration of China (CAC) has issued three administrative rules: Measures for the Security Assessment of Outbound Data Transfers, Implementation Rules for Personal Information Protection Certification, and Measures for the Standard Contract

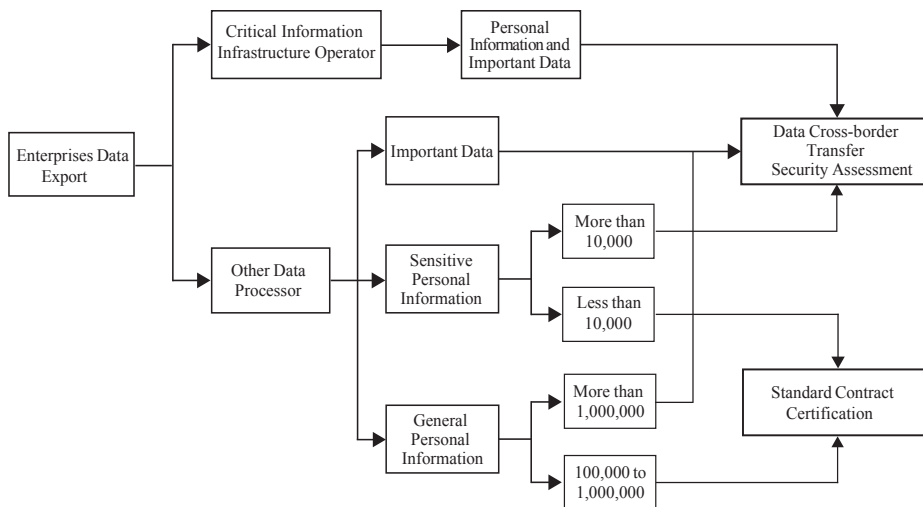


Figure 1: Three Compliance Pathways for China’s Enterprise Data Export

for the Outbound Transfer of Personal Information. These rules clarify three specific implementation mechanisms for data exports: security assessments, personal information protection certification, and standard contracts. Additionally, China has also issued a series of management measures in special industries, such as Interim Measures for the Administration of Online Taxi Booking Business Operations and Services, to supplement and operationalize the above administrative regulations.

III. PRIMARY SECURITY RISKS OF CHINA'S ENTERPRISE DATA EXPORT

A. The Defining Criteria for “Security”

Within the context of a holistic approach to national security, data security refers to “taking necessary measures to ensure that data is effectively protected and lawfully utilized, while possessing the capability to guarantee a sustained secure state”. From this conceptual foundation, the essence of data security encompasses two principal dimensions: “self-security” and “utilization security”. The former primarily concerns data confidentiality, integrity, and availability, ensuring data cannot be unlawfully accessed or altered by external personnel. The latter refers to employing relevant systems and technical means to safeguard the secure state of the data in the processes of production, circulation, and utilization.

Within the context of great power strategic competition, this study defines “enterprise data export security” in two aspects: firstly, data beyond the necessary scope shall not be subject to control by other states; secondly, enterprises’ legitimate data export activities shall not be obstructed by other states. Here, “beyond the necessary scope” denotes violations of the principles of data minimization and proportionality, where the actual data controlled by foreign governments, enterprises or other entities lacks reasonable correlation with their stated purposes of use.

Moreover, data security issues persistently affect economic and social development alongside public well-being. From a holistic perspective, safeguarding data security not only preserves citizens’ digital property rights

but also enhances national resilience, with contemporary significance for protecting privacy, ensuring stability, fostering development, and safeguarding the overall situation.¹ As a foundational strategic resource for national development, data plays a pivotal role in reshaping economic structures, and altering competitive landscapes. Only by safeguarding data security can the state consolidate progress across political, economic, social, and other fields, and further safeguard the national security.

B. Primary Categories of Risks

1. National Security Dimension

As a vital strategic resource, data underpins national development. Some enterprises hold critical data involving state secrets, primarily concentrated in the fields of energy, finance, communications, transportation, geographic information, and defense-related research. If such data falls under foreign control, it will severely jeopardize national strategic planning and infrastructure development. For instance, if oil and gas field data from energy companies falls under foreign control, the leakage of core information such as resource exploration directions and reserve distribution could place the state at a disadvantage in global energy competition. Similarly, if high-precision surveying data from navigation map companies is compromised, it may be exploited for military target localization. Exports of the personal data also pose security risks.

2. Industrial Security Dimension

In the course of operations, enterprises generate vast amounts of technical and operational information that possesses significant commercial value, including information on raw materials, samples, algorithms, and computer software. The control over critical data may lead to market monopolies, unfair competition, and supply chain disruptions, thereby constraining industrial development.² For instance, following the leakage of battery supply data from a new energy vehicle manufacturer, overseas entities analyzed its supply chain structure

1 Mehmet Kaya and Hamza Shahid, Cross-border Data Flows and Digital Sovereignty: Legal Dilemmas in Transnational Governance, *Interdisciplinary Studies in Society, Law, and Politics*, Vol. 4, No. 2, 2025, pp. 219–233.

2 OECD (2015), Data-driven Innovation: Big Data for Growth and Well-being, *OECD Publishing*, Paris, 2015, <https://doi.org/10.1787/9789264229358-en> (Last Visited on July 12, 2026).

and maliciously hoarded critical raw materials, causing the firm costs to soar substantially. Similarly, after the leakage of a pharmaceutical company's drug formulation data, proliferation of generic drugs emerged, causing a significant decline in the firm's market share. Particularly in emerging sectors such as semiconductors, chips, and artificial intelligence, the outflow of R&D data may force China to rely on foreign technology supplies for a long time, leading to a bottleneck in industrial upgrading.

3. Social Security Dimension

With the advancement of the digital economy, enterprises collect and process ever-increasing volumes of personal information, encompassing residents' identity details, contact numbers, residential locations, account access credentials, personal asset status, and travel itineraries. If the activities of specific individuals fall under such control, they would severely undermine legitimate rights and interests (such as privacy violations and threats to personal property security), potentially triggering social instability. For instance, overseas entities may exploit personal data for location-based scams, or non-compliant marketing, using big data to precisely target individuals with false information and inflammatory content, thereby subjecting them to severe harassment and financial losses.

C. Primary Sources of Risks

The compromise of critical corporate data may occur at any stage of cross-border data flows. The PESTEL analysis model, also known as macro-environmental analysis, identifies forces within the broader environment that impact organizations. Each letter of the acronym represents a distinct factor: Political, Economic, Sociocultural, Technological, Environmental, and Legal. Applying this methodology, the security risks associated with data export primarily stem from the following three factors.

1. Political Factors

This factor manifests through shifts in national policies arising from geopolitical rivalries. Major powers frequently leverage digital sovereignty as a bargaining chip, employing various means to vie for data control and

impose targeted restrictions on enterprises' data export activities in target states. Consequently, governments may frequently adjust data policies to align with their own interests.

One characteristic of such policy shifts is their instrumental nature, with certain states combining “data localization” with “cross-border transfer restrictions” as weapons in great power strategic competition. For instance, following the Ukraine crisis, Russia mandated localized storage for all social media platform data. The American Internet company Meta, unable to complete server migration in a short time, was compelled to exit the Russian market. Another characteristic is suddenness, meaning complete unpredictability. For instance, the United States (US) has frequently adjusted cross-border data rules in recent years, shifting from the Trump 1.0 “Free Flow” to the Biden “Small Yard, High Fence”, and ultimately to the Trump 2.0 era of “Comprehensive Securitized Decoupling” regarding sensitive data. In March 2024, the US Department of Commerce began requiring cross-border data transfer reviews for “smart connected vehicles containing Chinese information and communications technology or services”, forcing many Chinese enterprises to suspend overseas transmission of autonomous driving data.³ In summary, the discontinuity of data governance foreign policies makes it difficult for Chinese enterprises to establish a long-term and stable data circulation mechanism, leaving them unable to respond promptly to sudden risks. Furthermore, the legitimacy of policy adjustments requires legal support and is therefore usually associated with legal changes.

2. Technical Factors

Technical risks are the most immediate hazards in data export, as every link of data storage, transmission, processing, and protection is based on the reliability of technical tools. Technical deficiencies alone, without any policy restrictions or intervention, can instantly trigger data breaches, tampering, or service disruptions, spreading with alarming speed.

This factor is mainly reflected in two aspects: Firstly, vulnerabilities in data transmission channels. Some enterprises, seeking cost savings, process

³ US Department of Commerce, Securing the Information and Communications Technology and Services Supply Chain: Connected Vehicles, <https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain> (Last Visited on July 12, 2026).

data without encryption measures or employ outdated transmission protocols, resulting in interception during data flow. For instance, in 2024, a medical technology company in Shanghai deployed a database on an overseas cloud platform without implementing effective cybersecurity safeguards, resulting in the leakage of substantial amounts of personal information. Secondly, supply chain dependency issues persist, with Chinese enterprises broadly reliant on foreign technologies for both hardware and software in data processing. For instance, 90% of virtualization systems underpinning China's cloud computing infrastructure are foreign-branded, leaving enterprises perpetually exposed to risk. Furthermore, while emerging technologies such as big data and artificial intelligence enhance data processing efficiency, they also substantially increase leakage risks.

3. Legal Factors

Data export security issues stemming from legal factors are neither a single rule conflict nor a simple compliance challenge; instead, they represent the competitive collision between domestic and international legal systems, directly impacting enterprises' data control rights.

From a domestic perspective, China's legal framework governing data export exhibits characteristics of ambiguity and fragmentation. Firstly, certain provisions remain abstract with insufficient implementing regulations, such as lacking clear definitions of what constitutes "important data" or which data categories may circulate freely. Secondly, existing regulations exhibit gaps in coverage, such as the absence of a dedicated personal information regulatory body and the rigidly singular approach to data security assessment methodologies. These shortcomings hinder administrative enforcement and guidance for corporate operations, potentially leading to unregulated data outflows and consequent risks.

From an international perspective, differing political systems and societal values among states inevitably lead to variations in legislative approaches, resulting in conflicts between data export laws. Some states permit direct access to foreign data under domestic law, substantially increasing compliance costs for enterprises, and minor non-compliance with local legal requirements may result in severe penalties. Furthermore, certain states employ legislation as a

bargaining tool, granting their governments extremely broad jurisdiction. This exposes China's critical data to potential arbitrary control.

IV. LEGAL CONFLICTS OF CHINA'S ENTERPRISE DATA EXPORT

From the above discussion on security risks, it can be concluded that policy, technology, and law constitute the three primary avenues through which states engage in data sovereignty competition. Legal measures are generally regarded as the "most effective means", primarily for the following three reasons: Firstly, law possesses coercive force and enjoys long-lasting stable effectiveness. Secondly, legislation possesses broader coverage, capable of constraining the conduct of all foreign corporate entities. Thirdly, law offers proactivity, enabling nations to independently establish standards, erect barriers, and even align with international norms, and applying domestic laws globally. Consequently, it is imperative to systematically examine the manifestations of legal conflicts surrounding China's enterprise data export, thereby facilitating the development of more targeted countermeasures.

A. Conflicts Arising from Unilateral Assertions

Conflicts arising from opposing unilateral assertions occur when different states or regions, based on their own legal systems and sovereignty claims, impose jurisdictional demands on data activities conducted by foreign enterprises within their territories, leading to contradictions in the application of laws. Such conflicts represent an extension of national sovereignty into the data domain or, fundamentally, the struggle for control over data.

1. Fundamental Differences in Legislative Philosophy

Fundamental differences in legislative philosophy constitute one root cause of unilateral assertions conflicts. Currently, four primary models govern cross-border corporate data flows globally, with many rules diverging or even contradicting one another.

These models reflect different balances between openness and security.

a. Securitized openness model adopted by the US

Traditionally, the US championed a pure "open model" advocating for

unrestricted global data flows. However, this has pivoted toward “selective openness” driven by national security. Domestically, the 2025 “Final Rule” (Preventing Access to US Sensitive Personal Data and Government-related Data by Countries of Concern) restricts sensitive data transfers to “countries of concern”. Internationally, withdrawing from the WTO and the Indo-Pacific Economic Framework for Prosperity (IPEF) digital trade negotiations underscores this pivot.⁴

b. Restrictive model adopted by Russia and India

It prioritizes data sovereignty and national security through stringent controls on outbound data transfers. Specific measures include maintaining explicit “white lists” and “black list” for destination states and implementing rigorous internet access protocols.

c. Integrated model adopted by the EU

It advocates for a balance between rights protection and market development, promoting the free flow of data while ensuring adequate protection of personal data. When data flows to states outside the EU, the EU employs the “adequacy decision” mechanism as its assessment standard.

d. Security-oriented model adopted by China

It seeks to reconcile development with security, establishing “free data flow” as the foundation and “secure data flow” as the constraint to balance the dual goals of opening-up and national security.

Consequently, differing national priorities concerning data security, economic interests, and social governance produce divergent claims regarding data sovereignty and regulatory design. Table 2 summarizes these models and their differing balances among openness, privacy, and security.

For instance, the US emphasizes freedom of cross-border data flow, stipulating in Article 19.11 of the United States–Mexico–Canada Agreement (USMCA) that “each Party shall not prohibit or restrict the electronic cross-border transfer of information”; Conversely, Article 40 of the Personal Information Protection Law of the People’s Republic of China stipulates that “operators of critical information infrastructure and processors of personal

4 USTR, 2020 National Trade Estimate Report on Foreign Trade Barriers, https://ustr.gov/sites/default/files/2020_National_Trade_Estimate_Report.pdf (Last Visited on July 12, 2026); USTR, Summary of the Trans-Pacific Partnership Agreement, <https://ustr.gov/about-us/policy-offices/press-office/press-releases/2015/october/summary-trans-pacific-partnership> (Last Visited on July 12, 2026).

information reaching the volume specified by the national cyberspace administration shall store personal information collected and generated within China within the territory”. Consequently, Chinese enterprises seeking to operate in the US must comprehensively assess and prudently address this fundamental legal conflict arising from divergent data sovereignty philosophies, proactively developing compliance strategies to mitigate risks of data being controlled.

Table 2: Comparison of Major Global Cross-border Data Flow Governance Models

Type	Leading States	Key Features	Advantages and Disadvantages
Securitized Openness Model	The US	Conditional free flow with targeted security blockades	Advantages: Facilitating efficiency among allies Disadvantages: Intensifying global data decoupling and creating unilateral barriers
Restrictive Model	Russia, India	Mandatory domestic data storage with strict restrictions on data transfers abroad	Advantages: Effectively mitigating risks of foreign control Disadvantages: Hindering international cooperation and technological innovation
Integrated Model	The EU	Prioritizing privacy protection	Advantages: Setting high standards for protecting personal privacy Disadvantages: Exacerbating the fragmentation of data governance
Security-oriented Model	China	Balancing security and development	Advantages: Balancing data security with openness Disadvantages: Requiring further refinement of standards

2. The Abuse of Legal Sanctions

The second cause of such conflicts is the abuse of legal sanctions. When a state elevates its domestic rules above the international order, distorting laws into instruments of digital hegemony by expansively interpreting vague concepts such as “national security” and “public interest” to suppress competitors, it inevitably fractures the rules-based system, provokes confrontation, and creates legal antagonism with other states. The indiscriminate application of legal sanctions not only harms other states’ interests but also erodes the legitimacy of multilateral rules, thereby entrenching a cycle of “sanctions-countermeasures” that intensifies antagonism.

B. Conflicts Arising from Extraterritorial Jurisdiction

Conflicts of extraterritorial jurisdiction refer to the assertion of authority by one state to exercise jurisdiction over data stored within another state’s territory. This inevitably generates legal conflict and operational impediments, as it

infringes upon the data sovereignty of other states. The core concept here is “data retrieval”, a form of passive data export. Common scenarios include cross-border evidence gathering in international civil, commercial, and criminal judicial assistance, though this is now frequently abused as a means to expand extraterritorial data jurisdiction.

1. Extraterritorial Jurisdiction of Foreign Nations over Data Within China

Regarding foreign jurisdiction over data within China, certain states have enacted legislation to establish “long-arm jurisdiction” in this domain. Taking the US as an example, the 2014 “Microsoft case” exposed legal loopholes in cross-border data access. At the time, the US Department of Justice demanded that Microsoft provide user data stored on servers in Ireland, but the case became embroiled in prolonged litigation due to conflicts between the physical location of data and the scope of judicial jurisdiction. Subsequently, the Clarifying Lawful Overseas Use of Data Act (CLOUD Act) was enacted in 2018, permitting US law enforcement agencies to collect data stored abroad to assist criminal investigations, thereby addressing this deficiency. However, the US access to overseas data extends beyond the CLOUD Act. Following the 9·11 attacks, legislation including the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT) Act, the Foreign Corrupt Practices Act, and the International Emergency Economic Powers Act collectively formed an extensive framework for cross-border data retrieval. For instance, Section 215 of the USA PATRIOT Act stipulates that when pursuing foreign intelligence or combating international terrorism, the relevant US authorities may compel telecommunications and internet service providers to produce commercial records such as server logs via subpoena.

2. China's Extraterritorial Jurisdiction over Data in Foreign Territories

Firstly, China has established clear rules to block foreign “long-arm jurisdiction”, such as Article 36 of the Data Security Law of the People's Republic of China and Article 4 of the International Criminal Judicial Assistance Law of the People's Republic of China. The former requires that “no organization or individual within the territory of the People's Republic of

China may provide data stored within the territory of the People's Republic of China to foreign judicial or law enforcement authorities without the approval of the competent authorities of the People's Republic of China". While the latter requires that no institutions, organizations, or individuals within the territory of the People's Republic of China shall provide evidence materials or assistance as prescribed by this Law to foreign countries. However, to enhance the operational feasibility of these rules, numerous issues remain to be clarified. For instance, whether "law enforcement agencies" encompass judicial organs, administrative regulatory departments, and specific investigative bodies; whether transit data merely passing through networks within China without undergoing substantive processing or retention should be excluded; and so forth. Such countermeasures remain inadequate and require further elaboration. Comparative practice also offers useful guidance. The *Schrems II* ruling invalidated the EU-US Privacy Shield due to concerns regarding excessive foreign intelligence access, suggesting that similar protections can be incorporated into future bilateral or multilateral data-flow arrangements.

Secondly, China must clarify its principles for accessing data located within other states. In practice, such access is predominantly concentrated in the criminal justice domain, where law enforcement agencies may obtain cross-border evidence through both judicial assistance mechanisms and explicit provisions for unilateral data collection. For instance, Article 9(2) of the 2016 Provisions on Several Issues Concerning the Collection, Extraction and Review of Electronic Data in Criminal Cases issued by China's Supreme People's Court, Supreme People's Procuratorate and Ministry of Public Security stipulates, "Electronic data stored on original storage media located overseas or on remote computer information systems may be extracted online via the internet". Correspondingly, when data processing activities by foreign enterprises threaten China's security, sanctions may be imposed through extraterritorial jurisdiction. For instance, Article 2 of the Data Security Law of the People's Republic of China stipulates: "Where data processing activities conducted outside the territory of the People's Republic of China harm national security, public interests, or the lawful rights and interests of citizens or organizations of the People's Republic of China, legal liability shall be pursued in accordance with the law". However, these provisions remain overly broad. Further specific implementing rules are

required to clarify how to identify unlawful conduct.

C. Conflicts of Multi-party Rules

The conflict of multiple rules refers to situations where differing legal provisions and technical standards across states or regions prevent enterprises from simultaneously meeting all data compliance requirements during cross-border operations. This fundamentally stems from the tension between state sovereignty and market globalization, which can increase enterprises' risk of non-compliance and compliance costs, thereby impacting data security and industrial development.

1. Cumulative Obligations Across Multiple Jurisdictions

This conflict manifests as the accumulation of obligations across multiple states. This phenomenon stems from the fragmented nature of the international data governance system. Different states or regions, guided by their own political, economic, and cultural considerations, have established distinct frameworks. These frameworks create intersecting constraints during cross-border data flows, often hindering a single business entity from simultaneously complying with multiple requirements when conducting data export activities.⁵

2. Challenges in Mutual Recognition of Regulatory Standards

This conflict manifests as difficulties in mutual recognition of regulatory standards. Against the backdrop of rapid global digital economic development, significant regional disparities exist in the formulation of technical standards — such as communication protocols and product certifications — which lack uniformity and compatibility, thereby hindering mutual recognition. This forces multinational enterprises to bear cumulative technical compliance costs.

Take data encryption algorithms as an example. China has vigorously promoted its domestically developed National Cryptographic Algorithm System, of which the SM series is a core part, including SM2 (asymmetric), SM3 (hash), and SM4 (symmetric) algorithms.⁶ Designed with domestic

⁵ Anupam Chander and Uyên P. Lê, *Data Nationalism*, *Emory Law Journal*, Vol. 64, No. 3, 2003, p. 677.

⁶ National Institute of Commercial Cryptography Standards, *Overview of China's Commercial Cryptographic Algorithm Standards*, <https://www.niccs.org.cn/niccs/index.html> (Last Visited on July 12, 2026).

information security requirements in mind, these algorithms are widely used in critical sectors such as finance and government affairs. However, in international markets, most states and regions have long adopted globally recognized cryptographic algorithms such as Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) algorithm, an asymmetric encryption algorithm, which are regarded as essential benchmarks for data security compliance. This fragmentation in cryptographic standards means Chinese enterprises seeking to serve both domestic and international users are often required to develop two separate encryption systems, significantly increasing technical development costs.

More alarmingly, this fragmentation may trigger severe technical and operational risks. When overseas user data transits through Chinese servers, discrepancies in encryption algorithms and key management mechanisms may lead to format incompatibilities, decryption failures, or even transmission interruptions. Such technical failures not only degrade user experience but also heighten data leakage risks through abnormal data retention or repeated format conversions during transit. Moreover, the difficulties in mutual recognition of cryptographic technical standards can generate hidden trade barriers. Some states refuse to acknowledge foreign technical standards under the guise of “security reviews” or “technical compliance”, thereby effectively shielding domestic industries and restricting foreign competitors. This practice not only hinders global technological exchange and cooperation but also subjects enterprises to heightened uncertainty in cross-border data transfers.

V. PROTECTION PATHWAYS OF CHINA’S ENTERPRISE DATA EXPORT FROM THE PERSPECTIVE OF FOREIGN-RELATED RULE OF LAW

A. Enhancing the Domestic Legal and Regulatory Framework

This initiative will clarify vague concepts in current legislation, supplement provisions lacking in some crucial areas, and refine the scope of regulatory measures and their targets. Consequently, it can more accurately and efficiently contain security risks associated with enterprise data export at the source,

effectively countering legal sanctions and “long-arm jurisdiction” threats from other states.

1. Refining Data Classification and Cross-border Security Assessment

Regarding classification standards, the existing system relies solely on the post-breach harm as the basis for categorization. To ensure comprehensiveness, the standards of identifying “important data” should be appropriately expanded. The new classification criteria should be based on the following three principles: The first is the data subject, with particular focus on groups such as minors and public officials. The second is the data type, prioritizing data concerning sectors such as critical infrastructure, national defense and sensitive personal information. The third is the quantifiable elements, including indicators such as geographic scope and crisis response speed that can be quantified to make the classification clearer.

After the classification standards are clarified, a stricter security assessment system for “important data” should be established. Firstly, it is necessary to enhance the evaluation of enterprises’ internal capacities, encompassing their technical capabilities, governance frameworks, and other relevant factors. Secondly, clear approval procedures should be established to minimize human intervention. Finally, it is necessary to establish a rigorous penalty regime for enterprises that conduct unauthorized data export, thereby deterring such violations.

2. Clarifying Parity Clauses for Extraterritorial Jurisdiction Laws

To counteract foreign “long-arm jurisdiction” rules, China should further refine Article 36 of the Data Security Law of the People’s Republic of China and Article 4 of the International Criminal Judicial Assistance Law of the People’s Republic of the China: for important data, full control should be retained domestically; for general data, law enforcement cooperation can be allowed, but only with prior approval. Additionally, Article 3 of the Anti-Foreign Sanctions Law of the People’s Republic of China can be invoked to add the CLOUD Act and other discriminatory laws to the list of countermeasures.

To exercise extraterritorial jurisdiction with respect to other countries, China should further refine Article 2 of the Data Security Law of the People’s

Republic of China to clarify the circumstances under which extraterritorial jurisdiction may be exercised. It should be clarified that when exercising extraterritorial jurisdiction, the principle of proportionality must be upheld, weighing the severity of harm caused by data processing activities, the degree of connection between the data processor and China, and the appropriateness of the law enforcement measures relative to the nature of the violation.

B. Strengthening Diversified International Legal Cooperation

This initiative will effectively promote the convergence of domestic and foreign laws, address the fragmentation of data governance rules among states, thereby mitigating legal conflict risks and reducing corporate compliance costs. It facilitates the flow of data elements while safeguarding data sovereignty, enabling China to enhance its voice and rule-making authority in the global data governance.

1. Promoting the Signing of Bilateral and Multilateral Data Flow Agreements

By negotiating and signing bilateral and multilateral data flow agreements, China can engage in data resource sharing with other states, and establish a smoother and more efficient international cooperation framework in the field of enterprise data export. In practice, China possesses cooperative foundations with partners in the Belt and Road, Asia-Pacific Economic Cooperation and BRICS (Brazil, Russia, India, China, South Africa), offering advantages in both the efficiency and depth of dialogue. Prioritizing cooperation with these partners could serve as a breakthrough point for China in concluding data flow agreements.

2. Extending Participation in Shaping International Data Governance Rules

As data sovereignty concerns national interests and global data regulations vary significantly, states are collectively working to build a new governance system. Amidst this trend, China should put forward new proposals, leveraging its strengths to build multilateral consensus and strive to secure rule-making authority. The divergence of interests among states, shaped by their respective development and security demands, has become the root cause of conflicts over sovereignty. To achieve the transition from “state competition” to “state

collaboration”, nations must establish mutual respect as the foundation and pursue win-win cooperation as the objective.

With the proposal of the Global Initiative on Data Security and the Global Cross-border Data Flow Cooperation Initiative, China can elevate the concept of “secure data flow” to “legitimate and controllable flow”.⁷ This approach focuses on the legitimacy of cross-border data flows, emphasizing both the reduction of cross-border transmission risks through technological and institutional means and the full realization of data value. It can balance the diverse interests of nations, offering a more inclusive solution to global data governance.

C. Enhancing Enterprises’ Self-directed Compliance Capabilities

This initiative would break through the traditional “public authority” data governance model, gradually shifting toward a “multi-center” governance approach. By stimulating the intrinsic motivation of enterprises, it enhances the comprehensiveness and accuracy of data cross-border data security assessment and supervision. This enables enterprises to proactively identify and prevent risks from an operational perspective.

1. Establishing Internal Corporate Compliance Frameworks

Given significant variations in data types, sensitivity levels and cross-border requirements across different industries, without tailored compliance guidelines, corporate data export may fall into a one-size-fits-all management mode. Consequently, establishing internal compliance frameworks is essential. It should define fundamental principles, clarify key concepts, delineate responsibilities, and specify obligations to provide targeted guidance. For instance, a high-speed train company implemented its internal “Data Security Management Measures”, categorizing data into five tiers from highest to lowest sensitivity: Core Data, Important Data, Internally Sensitive Data, Internally General Data and Externally Public Data, thereby effectively achieving refined governance over such activities.

⁷ Xu Wanxiu and Zuo Xiaodong, China’s Approach to Cross-border Data Flow Governance in the Context of Global Competition, *Strategic Study of CAE*, Vol. 27, No. 1, 2025, pp. 111–121.

2. Establishing Cross-border Compliance Departments

In light of increasingly stringent oversight of cross-border data flows, investigations into corporate data by foreign judicial and law enforcement bodies have become routine. Therefore, establishing dedicated cross-border compliance departments is imperative. Such departments should operate across three stages: pre-event, during-event, and post-event. During routine operations, such departments must gather real-time regulatory developments in target states to formulate contingency plans. When facing extraterritorial investigations, such departments serve as the sole point of contact with foreign regulators, preventing operational departments from directly responding and thereby mitigating compliance risks. Post-investigation reviews should be conducted to assess compliance costs incurred during the resolution process and update their understanding of the latest regulatory trends in that state.

D. Advancing Pilot Innovations in the “Data Free Trade Zone”

1. Aligning with International High-standard Rules for Cross-border Data Flows

Firstly, entities should progressively implement the data export rules under RCEP. Alignment should encompass dispute resolution mechanisms, consensus among member states, and bilateral or multilateral free trade agreements. Secondly, entities should actively align with the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the Digital Economy Partnership Agreement (DEPA), including data security and personal information protection clauses that can strengthen management across all stages of data collection, processing, storage, and circulation, as well as exceptions that can minimize restrictions on enterprises' data export, thereby fostering a favorable business environment.

2. Exploring a “Whitelist” System for Enterprises' Data Export

To make this pilot workable, authorities should distinguish low-risk transfers from activities involving important or sensitive data and adopt clear review and exit standards while preserving necessary security controls. Currently, China's data export security assessment process requires separate reviews for each activity, which not only increases the workload of government departments but

also imposes high compliance costs on enterprises. The “whitelist” system aims to designate states or regions meeting data protection standards as destinations for free data flow, which is modeled after the EU’s adequacy decision, significantly enhancing the efficiency of data export.⁸ The establishment of a “whitelist” should consider the following factors: Firstly, whether the receiving state has robust data protection laws. Secondly, whether there are clear channels for redress in case of risks. Finally, whether the principle of reciprocity can be upheld, and China can take countermeasures if a state engages in unfair treatment. Furthermore, the competent authorities should establish a regular assessment system to continuously monitor and evaluate the data governance practices of states or regions already on the list. Entities that no longer meet the prescribed standards should be promptly removed from the “whitelist”.

VI. CONCLUSION

With the advent of the Fourth Industrial Revolution, human society is entering the Digital Age, bringing new data-related challenges to states worldwide. This study reveals that Chinese enterprises face multi-dimensional risks in cross-border data transfers, encompassing both horizontal dimensions — such as national security, industrial security and personal information security — and vertical sources, including political, technological and legal factors. Concurrently, Chinese enterprises face foreign-related legal challenges, including conflicts stemming from unilateral assertions, jurisdictional overreach, and divergent regulatory regimes. These challenges impede the internationalization of Chinese enterprises and the efficiency of cross-border data flows, underscoring the imperative to balance development and security.

Looking ahead, amid the continuous advancement of technology and the ongoing evolution of international law, China’s cross-border data transfers will face both new challenges and opportunities. On the one hand, emerging technologies such as AI, blockchain and quantum computing are advancing at an unprecedented pace; on the other hand, the formulation of international data governance rules will exert far-reaching impacts. Consequently, China

⁸ Kong Lingjie, Data Protection and Transborder Data Flow in the European and Global Context, *European Journal of International Law*, Vol. 21, No. 2, 2010, pp. 441–468.

must adopt a proactive stance to navigate this complex and evolving landscape, specifically by: continually refining relevant legislation and policies; advancing technological research and talent cultivation; bolstering corporate compliance capabilities; and fostering a more open, equitable and rational international data governance order. In essence, data security and national security are complementary, constituting prerequisites for mutual development and progress. Effectively addressing cross-border data transfer issues is therefore indispensable for China to enhance its overall security capabilities.