International Journal of Education and Humanities
ISSN: 2770-6702 | Vol. 24, No. 1, 2026

Building a Coordinated Regulatory Mechanism for Cross-Border Data Flows under the Holistic Approach to National Security

Linqi Li*, Chenyu Guo

School of Law, Henan Normal University, Xinxiang 453007, China

Abstract: While cross-border data flows generate enormous development opportunities, they also pose unprecedented challenges to national security. Although China has initially established a legal framework for regulating cross-border data flows, its coordinated regulatory mechanism still suffers from an imperfect legal system, ineffective coordination, and incomplete supporting mechanisms for pre-, in-process, and post-event regulation. These deficiencies undermine the effectiveness of national security safeguards and the sustainable development of the digital economy.Guided by the Holistic Approach to National Security, a sound legal framework for cross-border data flow regulation should be built by improving the multi-level legal system, establishing a dynamic adjustment mechanism, and enhancing the synergy between domestic and international regulatory rules. A multi-stakeholder coordinated regulatory mechanism should be established by clarifying the necessity of a unified regulatory authority and setting it up, creating a tiered collaborative supervision system that includes local authorities, industry regulators, industry associations, and third-party service providers, and strengthening a social oversight network with anonymous protection and reward mechanisms. Pre-event regulation should be reinforced through a combination of measures, including the formulation of industry-differentiated standards and the adoption of negative lists. In-process regulation should be enhanced by strengthening technical support and promoting technology application, so as to empower oversight through technology. Post-event regulation should be advanced by optimizing the effect evaluation mechanism, strengthening the risk handling mechanism, and reinforcing the accountability mechanism for violations, thereby establishing a whole-chain regulatory mechanism for cross-border data flows.

Keywords: Coordinated Regulatory Mechanism, Holistic Approach to National, Security Cross-Border Data Flows.

1. Introduction

With the acceleration of economic globalization, the demand for cross-border data flows is growing ever stronger, making it essential to put in place adequate safeguards in areas such as legal and regulatory frameworks, accountability systems, and security risk prevention.[1]In the digital era, data has become a vital factor of production-as important as land, labor, capital, and technology-and serves as a principal means of driving social development and enhancing national competitiveness. Cross-border data flows are one of the defining features of the digital economy age, and both their scale and frequency are growing exponentially. While such flows bring enormous opportunities, they also pose unprecedented threats to national security.In recent years, China has made considerable progress in developing its legal framework for cross-border data flows. In the area of cyberspace governance, the enactment of major laws and regulations such as the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law has provided basic norms for cross-border data flows and established corresponding security review mechanisms. Nevertheless, China's coordinated regulatory mechanism for cross-border data flows still suffers from an imperfect regulatory legal system, ineffective coordinated supervision, and incomplete supporting mechanisms for pre-, in-process, and post-event regulation. These deficiencies constrain the systematic safeguarding of national security and the sustainable development of the digital economy.As the fundamental guideline for national security work in the new era, the Holistic Approach to National Security is highly consistent with the value objectives of coordinated cross-border data flow regulation. Guided by the Holistic Approach to National Security, this paper seeks to improve the coordinated regulatory mechanism for cross-border data flows by building a sound legal framework for data flow regulation, establishing a multi-stakeholder coordinated supervision mechanism, and strengthening the whole-chain regulation of cross-border data flows, so as to safeguard national security, promote the development of the digital economy, and advance the modernization of the national governance system and governance capacity.

2. Establishing a Sound Legal Framework for the Regulation of Cross-Border Data Flows

At present, China's legal regulatory system for cross-border data flows still has many problems, which affect the comprehensive safeguarding of national security and the long-term development of the digital economy.

First, the legal system for cross-border data flows lacks operability. Existing legislation is highly principle-based but lacks detailed rules. The security review system under the Data Security Law has not yet been translated into specific rules, and the security assessment for outbound data transfers relies heavily on departmental interpretations. Under the Cybersecurity Law, the boundaries of responsibilities between critical information infrastructure and network operators are unclear, and it is difficult to identify controllers and processors in scenarios such as cloud services, thereby affecting compliance effectiveness.

Second, the extraterritorial application of the legal system for cross-border data flows is limited. In contrast to the "long-arm jurisdiction" trend in foreign legislation, the Cybersecurity Law adopts the principle of territoriality, while the extraterritorial jurisdiction of the Data Security Law and the Personal Information Protection Law is limited and their rules are general. This makes it difficult to effectively counter excessive jurisdiction by other countries, and there is also a lack of clear procedures and remedy mechanisms for blocking unilateral data requests by foreign law enforcement agencies.

Third, data localization measures for cross-border data flows give rise to trade compliance challenges. Mandatory local storage may violate commitments under the General Agreement on Trade in Services (GATS), increasing two-way compliance barriers for enterprises. Domestic regulation leans towards data security and local storage, creating tension with the orderly flow and regulatory balance advocated by agreements such as the Regional Comprehensive Economic Partnership (RCEP), which affects the discourse power in global data governance and the development of digital trade.

2.1. Improving the Multi-Level Legal System for Cross-Border Data Flow Regulation

Overall, China's legal system for regulating cross-border data flows has taken initial shape, filling gaps in data-related regulatory legislation. However, some key issues remain and need to be addressed in a targeted manner.

First, the legislation on cross-border data flow regulation contains too many framework provisions and needs to be more practically targeted. For example, both the Cybersecurity Law and the Personal Information Protection Law require that outbound transfers of personal data undergo a security assessment by the cyberspace administration. Yet, the legislation on cross-border data flow regulation is generally characterized by considerable vagueness, making specific implementation rather difficult. Moreover, the Data Security Law provides for the establishment of a data security review system, but this has not yet been translated into specific rules. The construction of this system faces three difficulties: the boundaries of the reviewing authorities' powers and responsibilities remain unclear, a mechanism for classifying risk levels is absent, and no objection or remedy procedures have been established. As some scholars have critically pointed out, the institutional design appears comprehensive, but in reality it lacks a clear directional stance in data legislation, and the standards for controlling the "strictness or leniency" of cross-border data flows remain ambiguous.[2]

Second, expand the extraterritorial application of laws governing cross-border data flows. From a comparative law perspective, the GDPR imposes jurisdiction over the processing of its citizens' personal data outside the EU. In contrast, the Cybersecurity Law applies only within China's territory, governing activities such as the construction, operation, maintenance, and use of networks within China, as well as the supervision and management of cybersecurity. This self-limiting territorial jurisdiction curtails the law's extraterritorial application. The Data Security Law brings within its regulatory scope acts conducted outside China that harm national security, public interests, or the lawful rights and interests of citizens, while the Personal Information Protection Law regulates certain processing of personal information outside China through a limited enumeration. Nevertheless, the scope of application of these three laws remains relatively limited. Therefore, China could draw on the relevant provisions of the GDPR to broaden its scope of application and reserve a defensive "long-arm jurisdiction" weapon for itself. The Data Security Law stipulates that organizations and individuals within China may not provide data to foreign judicial or law enforcement authorities without approval, but this provision is rather general and of limited utility. Some scholars suggest that China could compile a legal appendix concerning national long-arm jurisdiction, so as to specifically deny the effectiveness of different types of long-arm jurisdiction in a targeted manner.[3]In addition, the specific application procedures for foreign law enforcement agencies seeking to obtain data from China, the approval process and time limits of the designated authorities, and the legal liability for violating the approval obligation should be further clarified.

Third, address the GATS compliance issues arising from data localization measures. The core requirement of data localization measures is that personal data collected and generated through domestic operations must be stored within the country. However, GATS does not restrict the geographical location of cross-border service providers, and therefore data localization measures are very likely to affect the liberalization of cross-border data service trade.[4] Moreover, China made specific commitments under the GATS with no restrictions on "data processing services,"[5] Adopting mandatory data localization measures is equivalent to imposing quantitative or type restrictions on service providers, and is highly likely to violate the specific commitments undertaken by China under the GATS. Therefore, China should actively participate in the formulation of global data governance rules. The improvement of cross-border data flow regulatory rules requires comprehensive consideration. While China's own stance on data governance is certainly important, we must not overlook the need to work with other countries in the international community to shape mutually recognized rules.[6]On the one hand, we should actively integrate into the multilateral data governance frameworks dominated by the US and Europe. For example, China could attempt to participate in the CBPR system, so as to stimulate the vitality of domestic data flows, bring cross-border data transfers into compliance with its rules, and thereby facilitate digital economic cooperation more smoothly. On the other hand, China can make full use of the Belt and Road Initiative platform to strengthen digital economic cooperation with partner countries, drive the development of their digital industries, and simultaneously expand the global footprint of its own digital industry.

2.2. Establishing a Dynamic Adjustment Mechanism for Cross-Border Data Flow Regulation

The legal system consists of two major components: static construction and dynamic operation.[7]However, there are growing tensions among data sovereignty, privacy protection, and national security. The traditional static regulatory system for cross-border data flows cannot adequately adapt to the various problems arising from technological updates, changing industry demands, and international policy clashes. Therefore, it is necessary to establish a dynamic adjustment mechanism for cross-border data flows, achieving regulatory flexibility through legislative amendments, improvements to industry standards, and policy coordination, thereby

enhancing the legal system for cross-border data flow regulation.

2.2.1. Revising Laws in Line with Technological Developments

The regulatory mechanism for cross-border data flows must keep pace with technological updates; otherwise, legal lag will lead to regulatory failure or stifle innovation. Rapid technological advances have transformed the ways data is stored, processed, and transmitted, while also generating new risks.

First, the decentralized nature of blockchain technology means that data storage and transmission no longer rely on a geographically located node, challenging the traditional principle of jurisdiction based on data localization. Article 3 of the EU's General Data Protection Regulation (GDPR) asserts "long-arm jurisdiction," meaning that EU law applies as long as the data processing concerns EU residents, regardless of where the server is located.[8]However, data in blockchain networks is distributed across various nodes, thereby giving rise to legal conflicts.

Second, the large-scale deployment of artificial intelligence has intensified divergences over data anonymization standards. Traditional anonymization techniques may fail when confronted with the correlation analysis capabilities of AI; a single dataset may be anonymized, yet the integration of multiple datasets can re-identify individuals. The Court of Justice of the European Union explicitly stated in the Schrems II ruling that the technical capabilities of the data-receiving country-such as mass surveillance technologies-should serve as a criterion for assessing the lawfulness of cross-border data transfers.[9] Therefore, the EU amended its Data Governance Act in 2022, requiring companies to adopt dynamic anonymization techniques and undergo regular third-party technical audits.

Third, technical standards can serve as an "operational bridge" for law enforcement. The Privacy Information Management System standard issued by the International Organization for Standardization (ISO) provides detailed specifications for technical control measures regarding cross-border data transfers and has been referenced by the laws of many countries as proof of compliance. Section 1798.185 of the California Consumer Privacy Act (CCPA) stipulates that the state Attorney General may formulate technical standards to specify matters such as data encryption strength and retention periods for access control logs. For disruptive technologies such as quantum computing, legislation needs to pre-establish "technology trigger clauses." For instance, Article 17 of the EU's Digital Markets Act requires large platforms to submit a risk impact assessment before using new technologies. If a new technology may compromise data security, the regulatory authority can suspend its use. This is the so-called "precautionary legislation" model, which reduces the risks arising from legal lag by means of technology early warning.

2.2.2. Adjusting Industry Rules in Line with Industry Conditions

The complexity of regulating cross-border data flows stems from the marked differences in data attributes, usage scenarios, and risk levels across industries. In establishing its regulatory system for cross-border data flows, China formulates different rules tailored to the characteristics of various industries, aiming to safeguard national security and individual privacy while facilitating the development of the digital economy and international trade.

First, the high sensitivity of financial data requires a balance between security and speed in cross-border flows. China's Financial Data Security Classification Guide categorizes data into five levels and stipulates that data above Level 4 shall not, in principle, be transferred abroad. Yet scenarios such as cross-border payments and anti-money laundering demand a high degree of real-time data interaction. Accordingly, the Pilot Scheme for Cross-Border Data Flows in the China (Beijing) Pilot Free Trade Zone grants pilot institutions the right to transmit necessary transaction data abroad after completing a risk assessment.

Second, the cross-border flow of medical data involves issues such as bioethics, patient privacy, and biosafety. China's Regulations on the Administration of Human Genetic Resources require that human genetic information be transferred abroad only after approval by the Ministry of Science and Technology. The Health and Medical Data Security Guide (GB/T 39725-2020) further mandates that anonymization must meet a standard under which individuals cannot be re-identified. To meet the special needs of cross-border medical cooperation, the Hainan Boao Lecheng International Medical Tourism Pilot Zone implements a "privileged data flow" policy.[10]With patient informed consent, medical institutions may encrypt electronic medical records and imaging data and transmit them to overseas partner institutions for diagnosis, while the original data remains stored on a domestic regulatory platform. This creates a state where the data is usable but not visible-meeting the demands of cross-border collaboration for rare disease treatment while achieving the "data available but not visible" effect through Secure Multi-Party Computation (MPC).

2.3. Enhancing the Coordination between Domestic and International Regulatory Rules on Cross-border Data Flows

Currently, most laws on data regulation are domestic in nature, operating only within the sovereign jurisdiction of a single state, and they are difficult to apply when cross-border issues and international disputes arise.[11]At present, China's stance on cross-border data flows is relatively conservative, as reflected in its legislation by the ambiguous definition of important data and the broad scope of regulatory targets. In particular, where personal information involves one million or more individuals, outbound transfer security assessments and data localization storage are required.[12]In fact, given China's current stage of data development, although the level of data protection in certain regions may not match that of large cross-border enterprises, they already possess a degree of data processing capacity and protection mechanisms, backed by strong technical support. It is therefore necessary to start with the existing rules on localized data storage for cross-border data flows, clarifying the purposes for which flows are restricted, and specifying the types of cross-border data that are subject to restrictions based on the protection of national security, public interest, and similar concerns. For cross-border data flows that do not affect these interests, restrictions should be reduced, and regulation may be achieved through industry self-discipline. Adopting certain data localization measures is absolutely necessary, but on this basis, there is also a need to "scale back" these localization measures, striving to ensure the free flow of data under the guidance of the Holistic Approach to National Security, thereby achieving coordination with the RCEP agreement's regulation of cross-border data flows.

With regard to cross-border data transfers, compared with other agreements, the RCEP adds that each contracting party may regulate such data when necessary, and that a party, when measures are necessary to protect its essential security interests, may independently determine whether data is allowed to cross its borders.[13]To a certain extent, this accommodates the interests of developing countries and aligns with China's own stance on cross-border data flows. Therefore, relaxing localization restrictions represents a feasible attempt for China to better integrate into international trends.

3. Establishing a Multi-Stakeholder Coordinated Regulatory Mechanism for Cross-Border Data Flows

At present, the operational effectiveness of the regulatory system for cross-border data flows is deeply constrained by its organizational structure and the allocation of powers and responsibilities. While the government-led regulatory model can safeguard the bottom line of national security, it suffers from insufficient participation by market mechanisms and social forces, making it difficult to forge synergy through coordination among multiple stakeholders.

First, there is a lack of a unified regulatory authority for cross-border data flows. At the regulatory level, the decentralized regulatory model currently adopted in China has led to regulatory conflicts and inefficiency.[14]At present, the regulation of cross-border data flows involves multiple departments, including cyberspace administration, industry and information technology, commerce, and public security. This "multi-agency regulation" model is prone to causing confusion of powers and responsibilities, with misplaced oversight and regulatory gaps coexisting. Due to the absence of a unified coordinating body at the national level, each department tends to formulate policies based on its own functions, and insufficient coordination leads to regulatory vacuums or policy conflicts, thereby undermining the effectiveness of policy implementation and the certainty of corporate compliance.

Second, there is a lack of tiered and coordinated regulation. The self-regulatory functions of industry associations and third-party services have yet to be effectively activated. As data has permeated every aspect of people's lives, no industry can function without it. Bottom-up self-regulation is just as important as top-down government oversight. The regulation of cross-border data flows is highly technical and specialized, requiring regulators to possess the capability for formal review of technologies such as cloud transmission and blockchain encryption.[15],as well as the capability for substantive review of data content. Coupled with the rapid iteration of digital technologies, relying entirely on government regulation alone can lead to problems such as insufficient technical reserves for regulation and the improper allocation of regulatory personnel, thereby creating barriers in both technical cognition and regulatory enforcement. In China, the implementing entities of cross-border data governance policies are relatively singular, with limited participation from third-party institutions.[16],making it difficult to provide timely and equal compliance assistance and technical support to enterprises in different regions.

Third, the social oversight network for cross-border data flows is underdeveloped. The inadequacy of public participation channels renders the social oversight network largely nominal. Remedy mechanisms for data subjects, such as the right to know and the right to object in cross-border data flow scenarios, have not been effectively implemented, and the public opinion supervisory function of the media and social organizations has not been fully brought into play.

The key to regulating cross-border data flows lies in the coordinated operation of all stakeholders. To this end, we can construct a "gear model," in which the government, enterprises, industry associations, technical institutions, relevant organizations, and the public each perform their respective functions and jointly promote the secure and efficient flow of data across borders. In this gear model, the government serves as the core driving force; enterprises, associations, and technical institutions act as the key transmission gears; and relevant organizations and the public function as lubricants. All stakeholders coordinate with one another, share information in real time, and work together to ensure that cross-border data flows are secure, orderly, and efficient, thereby advancing the healthy development of the digital economy.

3.1. Establishing a Unified Regulatory Authority for Cross-Border Data Flows

The core concern of cross-border data flows is national security risk. Therefore, entrusting the Cybersecurity Review Office with the regulatory responsibilities for cross-border data flows is consistent with its functional positioning and offers the following advantages. First, it facilitates strengthened coordination and helps forge regulatory synergy, thereby avoiding overlapping and duplicative data regulation across different industries and sectors. Second, it is conducive to establishing a "single external window" and enhancing international exchanges and cooperation in data security governance. Furthermore, under the unified regulatory authority, various industries may still exercise industry-specific regulation based on their respective characteristics and specific circumstances, while the unified national-level regulatory authority should possess more robust enforcement authority.

3.2. Building Tiered and Coordinated Regulation for Cross-Border Data Flows

At present, China has initially established a regulatory legal framework for cross-border data flows and is further exploring mechanisms to facilitate outbound data flows. However, the issue of coordination in regulatory practice still requires attention.[17]Because data involved in cross-border flows concerns issues such as national security, privacy protection, and intellectual property protection, it is difficult for any single entity to handle the problems arising from such flows. Establishing a tiered and coordinated regulatory system for cross-border data flows can enable data to be supervised at four levels: local authorities, competent industry departments, industry associations, and third-party service providers.

3.2.1. Local Level: Pilot Legislation and Coordinated Regulation

When building a security system for cross-border data flows, local legislative bodies should fully exercise their leading role as legislators and formulate a systematic regulatory framework tailored to the strategic positioning and objectives of free trade port development. By unleashing local legislative autonomy and advancing the implementation of

these rules, they can achieve efficient synergy between the intended reform objectives and management effectiveness.[18] At the local level, it is necessary to establish a local regulatory body for cross-border data flows, responsible for the day-to-day supervision of local cross-border data flows. This regulatory body should possess cross-departmental coordination functions, forming a joint local regulatory force with departments such as cyberspace administration, industry and information technology, commerce, and public security. Regular regulatory meetings should be held to jointly address the various challenges encountered in the process of cross-border data flows, so as to prevent overlapping regulation and regulatory gaps.

3.2.2. Industry Regulatory Authority Level: Licensing and Compliance Guidance

Competent industry departments should, in line with their scope of duties, clarify their regulatory responsibilities for cross-border data flows. An industry market access system should be established to conduct qualification reviews and issue licenses for enterprises engaged in cross-border data flows. Higher market access thresholds should be imposed on sectors such as finance, telecommunications, and healthcare-industries that involve national security, public interests, and citizens' fundamental rights-based on data sensitivity and the development needs of each industry. Enterprises in these sectors must demonstrate strong data protection awareness and robust compliance capabilities. At the same time, competent industry departments should formulate sector-specific standards for cross-border data flows, and promote the alignment of legal rules with internal industry standards, covering areas such as data classification and grading, security level protection, and privacy protection. They should also issue compliance guidance manuals that provide specific compliance guidelines and best practices for enterprises conducting cross-border data flows. Through these standards and guidance, enterprises can be guided to conduct cross-border data flows in accordance with industry best practices, thereby reducing compliance costs and improving regulatory efficiency.

3.2.3. Industry Association Level: Self-Regulatory Norms and Dispute Mediation

Industry associations in the modern sense originated during China's transition from a planned economy to a socialist market economy.[19]Industry associations are self-regulatory organizations. They should guide their member units to conduct operations in accordance with the relevant data outbound regulations by formulating self-regulatory conventions. Industry associations are encouraged to take the lead in developing group standards and publishing industry compliance best practices, thereby promoting the sharing of compliance costs among enterprises and the joint development of compliance solutions.[20]Industry associations should regularly organize training and exchange activities to enhance their member units' awareness of data processing and compliance, and to promote communication among enterprises. They may also assist relevant departments in conducting industry monitoring and evaluation, thereby promptly identifying problems that arise in the development of the industry.

3.2.4. Third-Party Service Provider Level: Professional Consultation and Regulatory Support

The regulation of cross-border data flows is highly technical and specialized. Regulators are expected to possess the capacity for formal review of technologies such as cloud transmission and blockchain encryption, as well as the ability to conduct substantive review of data content. At present, however, regulation faces rapid digital technology innovation, insufficient technical regulatory capacity, and inadequate allocation of regulatory personnel, creating two major barriers: the understanding of regulatory technologies and regulatory enforcement. Drawing on the practical experience of industry self-regulation in the United States, China can leverage third-party professional institutions to review “binding agreements,” participate in standard-setting, and establish continuous monitoring mechanisms, thereby enhancing the compliance and security of cross-border data flows. By advancing the development of China’s cross-border data security technologies, the country can address current practical challenges such as regulators’ insufficient technical comprehension and the shortage of specialized professionals.[21] Third-party service providers can offer enterprises professional compliance consultation on cross-border data flows. They can assist enterprises in interpreting national and local laws, regulations, and policy documents concerning cross-border data flows, and, taking into account the actual circumstances of the enterprise, provide tailored compliance solutions for cross-border data flows. They can help enterprises carry out compliance assessments for cross-border data flows, identify compliance risk points, and propose personalized remediation suggestions. They can also conduct cross-border data flow auditing and certification. Furthermore, third-party service providers can assist regulatory authorities in implementing cross-border data flow supervision-for example, by providing professional training and policy guidance for the regulatory work of authorities, and by supporting the enhancement of regulatory authorities' capacity for cross-border data flow supervision.

3.3. Strengthening the Social Oversight Network for Cross-Border Data Flows

Establishing a social oversight network for cross-border data flows is an important measure for building a multi-stakeholder coordinated oversight mechanism, protecting personal privacy, safeguarding the legitimate interests of enterprises, and promoting the development of the digital economy. As can be seen from Articles 8, 9, 11, and 14 of the Cybersecurity Law, China’s current regulatory trend is to supplement administrative regulation with social oversight, such as industry self-regulation and reporting to relevant authorities by individuals and social organizations.[22] Therefore, the social oversight network can be improved from the perspective of oversight methods.

3.3.1. Anonymity Protection Mechanism for the Social Oversight Network of Cross-Border Data Flows

First, it is essential to improve the anonymity protection mechanism. This refers to a series of measures and methods adopted in the process of social oversight of cross-border data flows to protect the privacy of supervisors and relevant personnel, so that their sensitive information such as their identities is not disclosed. Anonymization has a special legislative function: it can promote the reasonable use of data and enhance the productivity and utilization efficiency of data elements, on the premise of regulating data processing activities and protecting the rights and interests of data subjects.[23]By establishing an anonymity protection mechanism, the concerns of oversight actors can be addressed, enabling them to exercise their oversight rights confidently

and without fear of risk. All personnel who have access to whistleblowing information must sign confidentiality agreements and are strictly prohibited from disclosing whistleblower information to any third party. In the event of an information leak, accountability shall be pursued immediately. Relevant staff who leak whistleblower information shall be subject to administrative penalties and financial penalties, and where the act constitutes a crime, criminal liability shall be pursued. This ensures that the confidentiality system is strictly enforced, so that whistleblowers need not worry.

3.3.2. Reward Mechanism for the Social Oversight Network of Cross-Border Data Flows

"Motivation is the tendency of people to act toward a specific goal, that is, stimulating their subjective initiative, generating intrinsic motivation within them, and driving them toward the desired goal."[24]Therefore, in the realm of reporting cross-border data violations, in order to transform the general public from "bystanders" into "participants," it is necessary to establish a multi-tiered incentive mechanism that combines material and non-material rewards, genuinely converting external inducements into sustained intrinsic motivation. From the perspective of material rewards, different levels should be determined based on three main factors-the value of the reported information, the degree of impact on the case investigation, and the amount of data loss recovered-so as to demonstrate the importance attached to and the protection afforded to high-value reports.

As for non-material rewards, they should go beyond the mere conferral of honors and place emphasis on social recognition as the principal means of spiritual motivation. For whistleblowers who meet the relevant requirements, in addition to granting certificates of honor and conferring titles such as "Data Security Guardian" or "Advanced Individual in Cross-Border Data Oversight," official platforms may be used to commend whistleblowers in anonymous or pseudonymous form, and the relevant honors may be incorporated into social credit evaluations, assessments of courageous acts, and relevant industry appraisals. Through such profound spiritual recognition, whistleblowers can develop a sense of pride, belonging, and accomplishment in protecting public data security, thereby transforming external rewards into an intrinsic motivation to proactively assume responsibility and actively engage in oversight.

4. Building a Whole-Chain Regulatory Mechanism for Cross-Border Data Flows

China's regulation of cross-border data flows has long prioritized pre-event measures over in-process and post-event oversight. Although the three pre-event review pathways-security assessments, standard contracts, and protection certifications-have been largely established, they remain, like the supporting mechanisms for continuous in-process monitoring and post-event accountability, far from complete. This front-loaded regulatory structure leaves the post-exit stages-such as storage, use, and onward transfers-without sustained follow-up supervision. Regulatory intensity rapidly diminishes once the outbound transfer review is completed, making it impossible to form a complete management system that encompasses pre-exit risk assessment, in-transfer flow monitoring, and post-exit violation handling. Moreover, the absence of substantive regulatory means remains a technical bottleneck that hinders the seamless integration of the regulatory chain. Both China's current outbound data review procedures and the mainstream regulatory arrangements in the international community "rely primarily on procedural reviews in the form of examining supporting documentation, with very few substantive measures involving functional checks or technical testing."[25]Risks arising from scenarios such as big data analytics and secondary processing by artificial intelligence cannot be verified through a predominantly procedural review approach when it comes to substantive aspects-such as whether data has been used beyond its authorized scope, whether security incidents have occurred, or whether data has been intercepted by third parties. This results in the most critical link of whole-chain regulation facing the conundrum of being "unable to see, unable to regulate, and unable to detect."

To this end, guided by the Holistic Approach to National Security, it is necessary to strengthen pre-event regulation through a combination of measures, including formulating industry-differentiated standards for cross-border data flows and establishing negative lists for cross-border data flows; enhance in-process regulation by empowering it with technology through stronger technical support and intensified technology application for cross-border data flows; and advance post-event regulation by optimizing the effect evaluation mechanism, strengthening the risk handling mechanism, and reinforcing the accountability mechanism for violations. In doing so, a whole-chain regulatory mechanism for cross-border data flows will be built, so as to safeguard China's national security and promote the healthy development of the digital economy.

4.1. Strengthening Pre-Event Regulation of Cross-Border Data Flows Through a Combination of Measures

To ensure the secure cross-border flow of data under the Holistic Approach to National Security, it is essential to implement pre-event regulation through a combination of measures so as to strengthen the whole-chain regulation of cross-border data flows. Such pre-event regulation can be carried out by formulating industry-differentiated standards for cross-border data flows and establishing negative lists for cross-border data flows.

4.1.1. Formulating Industry-Differentiated Standards for Cross-Border Data Flows

Setting different standards for cross-border data flows across industries is key to safeguarding data security and promoting lawful and compliant cross-border data flows. Data in different industries have their own distinct characteristics. Business data in the financial sector includes a large amount of customer account information and transaction data, involving personal privacy, financial security, and national economic security; when problems arise in cross-border flows, systemic financial risks can easily be triggered. Business data in the healthcare sector includes a large volume of patient medical records, genetic data, and other information. On the one hand, cross-border flows are necessary to meet the needs of medical treatment, scientific research, and cross-national medical assistance; on the other hand, they must guard against the ethical and legal risks arising from breaches of patient privacy.

Therefore, uniform standards for cross-border data flows cannot meet the requirements of cross-border data processing

in various industries. Establishing industry-differentiated standards can address the specific cross-border data processing needs of each industry, making the regulation of cross-border data flows more targeted and effective. This ensures that cross-border data flows and security protection avoid a "one-size-fits-all" regulatory approach that could either hinder industry development or create regulatory gaps leading to cross-border data risks.

4.1.2. Establishing a Negative List for Cross-Border Data Flows

When aligning with international economic and trade rules, some scholars recommend clarifying a "non-conforming measures" list-essentially a negative list-to make the security assessment mechanism more operable.[26]The negative list, also referred to as the “prohibition list,” is a foreign investment access management model that stands in contrast to the positive list. It primarily denotes a list of industries or goods in which a country restricts or prohibits foreign capital entry or imposes limits on foreign shareholding ratios. It adheres to the rule-of-law concept that “everything which is not prohibited is allowed,” and follows the interpretive logic of “entry unless explicitly restricted.”[27]**The negative list system, as a form of list-based governance, originated abroad and was initially solely a measure for regulating a country's outward foreign direct investment. The Third Plenary Session of the 18th CPC Central Committee proposed that "all types of market entities may equally enter areas not on the list in accordance with the law," thereby extending the negative list system from its original scope of regulating foreign investment markets to the market access of both domestic and foreign capital.

Although some regions have already explored the use of negative lists in practice, deficiencies still remain. While the data on the list has been classified, tiered management still needs improvement. A true negative list should strictly follow the legal logic of "everything that is not prohibited is allowed," and strive to enhance the rule of law and transparency in the regulation of outbound financial data. Therefore, on the basis of comprehensively considering the risk weightings of data flow liberalization and data security objectives, the negative list should be subdivided into a list of data prohibited from being transferred abroad and a list of data restricted from being transferred abroad, with corresponding regulatory measures for cross-border data flows adopted for each type. Data that implicates data security objectives-where the interests at stake significantly outweigh the objectives of data flow liberalization-even if there is a necessity for its export, should be regarded as core data and placed on the prohibited list.

4.2. Strengthening In-Process Regulation of Cross-Border Data Flows Through Technology Empowerment

In-process regulation, as the intermediate stage of the whole-chain regulatory mechanism for cross-border data flows, plays a vital role in strengthening the oversight of cross-border data flows. Technical prevention and control can be leveraged to support such regulation—for instance, by employing blockchain technology and artificial intelligence in in-process supervision.

4.2.1. Increasing Technical Support for Cross-Border Data Flows

Blockchain technology is a revolutionary scientific and technological achievement in the current digital era, and it is playing an increasingly important role in the digital governance ecosystem.[28]Blockchain technology is an entirely new digital trust infrastructure. It protects user data privacy through a decentralized and tamper-proof database, where users retain full ownership and control of their data. Users generate private keys to control transaction accounts, rather than linking personal identity information to account addresses, and publish public account addresses using public key encryption, thereby safeguarding privacy while allowing anyone to access specific transaction records. The entire network forms a tightly woven web in which information is extremely difficult to tamper with, giving blockchain exceptionally high data stability and reliability.[29]With blockchain technology, users can not only easily participate in any transaction activity on the network, but also every detail of each transaction is disconnected from specific real-world individuals-this is inherent to the nature and characteristics of the blockchain network. The blockchain network breaks the complete monopoly of centralized data controllers over data, grants users genuine rights to data privacy protection, enables users to control their own data, and makes transactions on the network more transparent and trustworthy.

4.2.2. Strengthening the Application of Technology in Cross-Border Data Flows

The cross-border data flow monitoring platform should be real-time in nature, providing comprehensive monitoring of cross-border data flows. It should conduct real-time monitoring of factors such as the direction, volume, and speed of data flows, promptly detecting data transmission anomalies-for instance, a sudden spike in data traffic or flows directed to unusual overseas servers. The platform should issue real-time alerts upon such detections and promptly follow up with analysis and handling. Real-time monitoring can effectively prevent data from being maliciously tampered with, stolen, or abused during cross-border transmission.

The platform should be equipped with robust data encryption algorithms, enabling end-to-end encryption for cross-border data throughout the entire transmission process. These encryption algorithms should be highly secure and resistant to cracking-for example, by adopting international standards such as the AES encryption algorithm-to prevent data from being intercepted and decrypted during cross-border transmission. For sensitive data fields, the platform needs to have an automatic masking function that can mask sensitive fields and replace them with hidden values without affecting usability, thereby ensuring the protection of personal privacy and trade secrets during cross-border data transmission.

The cross-border data flow monitoring platform should also possess strong risk early-warning capabilities. By analyzing historical and real-time data and employing machine learning algorithms and data mining techniques, the platform can provide real-time early warnings of risks associated with cross-border data flows.

4.3. Improving Mechanisms to Advance Post-Event Regulation of Cross-Border Data Flows

Under China's current regulatory rules, post-outbound supervision of data is relatively weak. Data processors are subject to fewer constraints once the data is transferred abroad,

and the emergency response mechanism for handling risk incidents remains unclear.[30]In fact, strengthening post-outbound supervision of data not only benefits information security, but also eases the strain on pre-event regulation, thereby facilitating the secure cross-border flow of data.

4.3.1. Optimizing the Effect Evaluation Mechanism

The evaluation and assessment mechanism for the implementation effect of post-event supervision of cross-border data flows refers to the use of scientific evaluation indicators and methods to evaluate the post-event supervision of cross-border data inflows and outflows. It aims to objectively, comprehensively, scientifically, and truthfully determine whether the post-event supervision has achieved the expected regulatory objectives, thereby providing support for the formulation and revision of regulatory policies.

Establishing an effect evaluation system can, on the one hand, enable the competent authorities to understand the achievements made in regulatory work, identify the problems and deficiencies therein, and accordingly adjust the direction and means of supervision, making regulatory work more targeted and effective. On the other hand, it can provide enterprises and individuals with clear regulatory standards, prompting them to act in compliance with the rules governing cross-border data flows and cultivating their awareness of data security and compliance. Moreover, the effect evaluation system can provide the public with open and transparent regulatory information, thereby enhancing society's trust in and identification with the regulatory framework.

4.3.2. Strengthening the Risk Handling Mechanism

Big data, artificial intelligence, and other technological means can be used to monitor risk factors in cross-border data flows in real time-that is, by using network traffic monitoring software to detect anomalies in data transmission, such as excessively fast speeds or unusually long durations, so as to promptly identify hidden dangers like data breaches and cyberattacks. Risk early warning indicators should be established, with the indicators and their thresholds determined based on historical data and risk factors. For example, a warning would be triggered if the number of data breach incidents exceeds a certain threshold or if the error rate of cross-border data transmission surpasses a specified value. These risk early warning indicators should cover aspects such as data security, privacy protection, and compliance, enabling comprehensive monitoring of data risks. Furthermore, early warning information should be disseminated. When a risk early warning indicator is activated, the regulatory authorities, enterprises, and data subjects should be notified immediately, with details including the scope of impact and response measures.

At the same time, contingency plans for different types of cross-border data flow risks should be formulated to better handle risk disposal. The plans should include emergency response procedures, division of responsibilities, resource allocation, and other elements. The capability for rapid response and swift handling is also essential: once a risk event occurs, the plan should be activated immediately and disposal carried out. Moreover, active communication and coordination among regulatory authorities, market entities, data subjects, and other parties should be strengthened during emergency response. All parties should be kept promptly informed of the progress and handling of the risk event, thereby safeguarding their right to know.

4.3.3. Strengthening the Violation Accountability Mechanism

Unapproved cross-border transfers, data leaks caused by failure to adopt security safeguards, and breaches of privacy protection requirements all constitute violations. Penalty standards should be set based on the nature, circumstances, and severity of the violation. Overseas recipients that violate the rules may also be placed on a blacklist. According to China's Cybersecurity Law, Data Security Law, Criminal Law, and other laws, the customary penalties for domestic data processors' violations in outbound data activities include rectification orders, fines, revocation of business licenses, suspension of relevant business, and criminal liability. However, regulatory measures targeting overseas data recipients remain relatively scarce. To effectively combat and deter violations by overseas recipients, they should be barred from receiving domestically generated data for a specified period and their commercial activities within China should be restricted. At the same time, a dynamic compliance assessment should be conducted. Overseas data recipients that have accepted and completed the rectification measures required by China's regulatory authorities may be re-admitted. However, attention should be paid to whether they have previously experienced security incidents or still pose security risks, as this better alerts regulatory authorities to prudently evaluate subsequent data transfers to them and enhances security certification.

5. Conclusion

As a new factor of production, data's borderless flow and its tension with sovereign borders have been continuously reshaping the landscape of international competition. How to strike a dynamic balance between openness and security has become a pressing challenge for all nations. Guided by the Holistic Approach to National Security, China has established a coordinated regulatory mechanism for cross-border data flows. This represents both an inevitable response to the risks of the digital age and a proactive attempt to advance the transformation of the global digital governance system.

The Holistic Approach to National Security provides, at a strategic level, a value reference and a clear direction for regulatory efforts. Under the globalization of the digital economy, the duality of security and development in data flows has transcended traditional security boundaries, evolving into a complex challenge that spans political, economic, technological, and cultural dimensions. China has put forward the Holistic Approach to National Security, structuring its basic framework around five major elements and five pairs of relationships, and has integrated data security into the broader national security system. It emphasizes both the extension of cyberspace sovereignty through data sovereignty and the supportive role of market-based allocation of data factors for economic security. This has fostered an integrated solution that embodies both strategic resolve and governance flexibility-one that not only safeguards the fundamental interests of national security but also contributes Chinese wisdom to the sustainable development of the global digital economy.

The establishment of a coordinated regulatory mechanism for cross-border data flows is, in essence, a significant enhancement of national governance capacity in the digital era. It is both a practical embodiment of the Holistic Approach to National Security and China's response to global digital governance. At a time when technological innovation and rule

reconstruction proceed hand in hand, the success of this mechanism depends not only on the rationality of its institutional design, but also on whether the governing entities can maintain strategic composure amid ongoing interactions and negotiations. Only in this way can a security barrier be erected on the foundation of openness and innovation, thereby achieving the protection of data sovereignty, the flourishing of the digital economy, and the building of a community with a shared future for mankind.

Acknowledgments

This work was financially supported by the Post-Funded Project of the National Social Science Fund of China(Grant No. 25FFXB079).

References

[1] Zhang, P., & Qiu, Z. (2022). *Five essays on data elements: Information ownership, value, security and transactions*. Peking University Press.

[2] Hong, Y. (2021). The US-Europe strategic stance on data competition and China's response: From the dual perspectives of domestic legislation and economic and trade agreement negotiations. *Chinese Review of International Law*, 6, 69–81.

[3] Dong, J. (2021). Security governance of cross-border data flows. *Science & Technology Review*, 39(21), 9–17.

[4] Peng, Y. (2018). A study on trade regulation issues of data localization measures. *Global Law Review*, 40(2), 178–192.

[5] People's Republic of China. (2017). *Schedule of Specific Commitments on Trade in Services of the People's Republic of China: B. Computer and Related Services*. http://www.gov.cn/gongbao/content/2017/content_5168131.htm

[6] Feng, J. (2021). Governance of cross-border data should emphasize holistic considerations. *China Information Security*, 5, 75–77.

[7] Li, J. (2025). Review and optimization path of enterprises' cross-border data flow system under the holistic view of national security. *Hebei Academic Journal*, 45(3), 181–189.

[8] European Commission. (2018). *General Data Protection Regulation (GDPR)*. EUR-Lex.

[9] Court of Justice of the European Union. (2020). Data Protection Commissioner v. Facebook Ireland and Maximillian Schrems (Case C-311/18). Curia.

[10] Luo, P., Ma, X., & Chen, J. (2023). Promoting cross-border data circulation and transactions to build Hainan International Data Port. *Investment & Cooperation*, 12, 49–51.

[11] Xu, Y., Yang, L., & Lv, W. (2024). "Freedom" and "Sovereignty": Dynamic game of cross-border data flow governance models—From the perspective of global digital trade rules. *Administrative Tribune*, 31(6), 157–167.

[12] Xiong, G., & Zhang, S. (2023). Improvement of China's data export security management system from the perspective of holistic national security. *Journal of Harbin Institute of Technology (Social Sciences Edition)*, 25(5), 32–40.

[13] Mei, A., & Chen, Z. (2023). Institutional construction of China's data security supervision from the perspective of holistic national security. *E-Government*, 11, 104–115.

[14] Fang, J., & Li, B. (2025). Realistic challenges and path optimization of China's legal system for data export security. *Journal of Hangzhou Dianzi University (Social Sciences Edition)*, 21(3), 51–59.

[15] Song, D., & Wu, D. (2024). Research on the optimization of the regulatory system for cross-border flow of personal data under the new security pattern. *Information Studies: Theory & Application*, 47(3), 54–61.

[16] Wu, J., Dong, K., & Ma, T. (2025). Analysis and optimization path of China's cross-border data flow governance policy: From the synergistic perspective of "executive subjects - policy tools - policy objectives". *Journal of Modern Information*, 45(8), 109–120.

[17] Chen, J. (2023). Observation and suggestions on the current status of China's cross-border data flow supervision. *China Information Security*, 10, 58–61.

[18] Chen, L., & Liu, Y. (2021). Research on the legal regulation of cross-border data flows in Hainan Free Trade Port. *Journal of Customs and Trade Research*, 42(3), 1–14.

[19] Hui, Y. (2024). Research on legal issues of local industry associations and suggestions for regulatory legislation. *Hebei Enterprise*, 1, 146–148.

[20] Yan, B., & Wang, Y. (2026). Cross-border data flow regulation and corporate supply chain transfer. *Economic Research Journal*, 61(1), 143–166.

[21] Song, D., & Wu, D. (2024). Research on the optimization of the regulatory system for cross-border flow of personal data under the new security pattern. *Information Studies: Theory & Application*, 47(3), 54–61.

[22] Li, A., & Zhang, J. (2017). Data security and supervision. In Internet Finance Law Research Institute, China University of Political Science and Law (Ed.), *Summit on Big Data Rule of Law in the New Era - Big Data, New Growth Drivers, New Momentum, New Order Proceedings* (pp. 37–61).

[23] Lin, B. (2024). Dilemmas and improvements of generalized legislation on anonymization of personal information. *Administrative Law Review*, 6, 29–46.

[24] Li, Y., & Chen, Y. (2015). On the reward mechanism for plaintiff's winning in environmental civil public interest litigation. *Western Law Review*, 1, 1–8.

[25] Luo, W. (2021). Procedural and substantive supervision of cross-border data flows based on life cycle. *Journal of China University of Political Science and Law*, 5, 142–154.

[26] Liu, Y., & Liang, Q. (2025). Limits and responses of exception clauses for cross-border data flows under DEPA. *Journal of Shanghai University of International Business and Economics*, 32(4), 98–111.

[27] Yu, Y. (2026). Development of China's negative list and its application in the field of cross-border data flow: Taking the practice of Beijing-Tianjin Pilot Free Trade Zone as an example. *China Business & Trade*, 35(7), 56–59.

[28] Zhao, W. (2024). *Research on legal issues of cross-border data flows: National governance, corporate compliance and technological innovation*. China University of Political Science and Law Press.

[29] Ma, L. (2020). On the regulatory path of cross-border data flows under the background of blockchain and China's response. *Foreign Trade*, 5, 35–39.

[30] Zhang, M. (2024). Compliance dilemma and regulatory response of data export by China's securities companies. *Tianfu New Idea*, 2, 120–129.