frontiers | Frontiers in Marine Science

TYPE Policy and Practice Reviews
PUBLISHED 05 August 2025
DOI 10.3389/fmars.2025.1600050

OPEN ACCESS

EDITED BY
Yusheng Zhou,
Hong Kong Polytechnic University, Hong Kong SAR, China

REVIEWED BY
Hu Zhang,
East China University of Political Science and Law, China
Qiuwen Wang,
East China University of Political Science and Law, China

*CORRESPONDENCE
Liu Wang
willowwangliu@gmail.com

RECEIVED 25 March 2025
ACCEPTED 11 July 2025
PUBLISHED 05 August 2025

CITATION
Yu M and Wang L (2025) China's cross-border maritime data flow governance: progress, challenges, and prospects.
Front. Mar. Sci. 12:1600050.
doi: 10.3389/fmars.2025.1600050

China's cross-border maritime data flow governance: progress, challenges, and prospects

Minna Yu[1] and Liu Wang[2,3]*

[1]Law School, Ocean University of China, Qingdao, China, [2]Law School, Sun Yat-sen University, Guangzhou, China, [3]Southern Marine Science and Engineering Guangdong Laboratory (Zhuhai), Zhuhai, China

The rise of the big data strategy and the concept of new productive forces in China amplifies the significance of cross-border maritime data flow in driving the growth of the shipping economy. While China has made notable progress in facilitating and regulating cross-border maritime data flow through legislative and policy initiatives, the existing framework remains general and fragmented, falling short of addressing the specific and complex requirements of maritime data practices. Using normative and comparative analysis, this paper systematically examines the legal and policy landscape surrounding cross-border maritime data transfer in China, including laws, departmental regulations, and industry standards. It identifies two critical challenges: the conflict between promoting cross-border maritime data transfer and safeguarding national security interests, and the shortcomings in the maritime data classification and grading system. Finally, this paper proposes a multi-faceted approach to address these issues, emphasizing technological innovation, fostering international cooperation to establish unified technical standards, and advancing the legalization of the "national security" concept. It further advocates for building international consensus on defining "national security" within the context of maritime data governance, aiming to balance the facilitation of cross-border data flow with the protection of national security interests.

KEYWORDS

cross-border data flow, maritime data, Chinese practice, national security, data classification and grading, free trade zone

1 Introduction

1.1 Background

The governance of cross-border maritime data flow has become a critical issue in the digital era, driven by its profound implications for global trade, economic growth, and maritime security. Since 2019, the rapid development of smart shipping technologies has significantly increased the demand for seamless data exchange while raising regulatory and security

concerns. At the international level, the International Maritime Organization (IMO) has led efforts to harmonize maritime data governance. Key initiatives include the *Guidelines on Maritime Cyber Risk Management* (IMO (International Maritime Organization), 2022), the *Guidelines for harmonized communication and electronic exchange of operational data for port calls* (IMO (International Maritime Organization), 2023), and the mandatory implementation of "Maritime Single Window" (IMO (International Maritime Organization), 2024). The International Organization for Standardization (ISO) 5909 project, titled "business process and data exchange of distributed ledger technology (DLT)-based electronic bills of lading", has successfully passed the committee stage review (ISO). In addition, large economies such as the United Kingdom (UK) and the United States (U.S.) have advanced national initiatives. The UK highlights the dual objectives of unlocking the economic potential of data sharing and safeguarding critical infrastructure (Department for Science, Innovation & Technology, Department for Digital, Culture, Media & Sport, 2021), while the U.S. emphasizes on mitigating cybersecurity risks in its maritime data systems (U.S. Department of Transportation, 2024). These efforts reflect the growing international consensus on the importance of regulating cross-border maritime data flow and the diverse national strategies adopted to reconcile economic development with security requirements.

As a leading maritime nation, China has recognized the transformative potential of maritime technology for its shipping industry, which has been significantly reshaped by digital technologies such as blockchain, big data, and artificial intelligence (AI). These innovations have generated vast amounts of maritime data, leading to increased demand for cross-border data flow to optimize operations and foster international cooperation. However, China's advancements in maritime technology have also raised concerns from other countries, prompting strategic responses. For instance, to secure maritime data, protect U.S. commercial interests and weaken China's position in shaping data governance norms, the U.S.'s 118th Congress has passed the *Ocean Shipping Reform Implementation Act* of 2023 to ban the Pentagon from using any seaport in the world that relies on a Chinese logistics platform known as LOGINK[1] (USCC (U.S.-China Economic and Security Review Commission), 2022).

In sum, despite the international progress and China's active efforts, the governance of cross-border maritime data flow remains a complex and evolving issue. Existing regulatory frameworks are often fragmented and insufficient to address the specific challenges posed by the maritime sector, particularly in balancing the dual priorities of data facilitation and national security protection. These gaps underscore the need for a more comprehensive and tailored legal framework, both domestically and internationally, to ensure the secure and efficient governance of cross-border maritime data flow.

1.2 Literature review

Extensive research has examined the role of digital technologies in enhancing maritime operations, particularly focusing on the integration of navigation data to improve operational efficiency and maritime safety (Liu et al., 2023). Scholars have explored the potential of blockchain technology for secure data exchange (Carlan et al., 2020), the application of big data in maritime traffic analysis, and the use of artificial intelligence (AI) to optimize logistics and predictive analytics (Paladin et al., 2022). For instance, studies have analyzed how the integration of Automatic Identification System (AIS) data within big data frameworks can substantially enhance maritime research and decision-making (Ma et al., 2024). These technological advancements underscore the considerable potential to enhance cross-border maritime data flow, while simultaneously highlighting the pressing need for standardized data-sharing protocols to ensure interoperability across international jurisdictions (Sun et al., 2021). Although extensive research has been conducted on general cross-border data governance (Gregory Voss, 2020), and the emergence of the concept of data sovereignty has intensified discussions on the nexus between data governance and national security (Hong, 2023), studies specifically addressing maritime data governance remain limited.

To address these challenges, it is essential to turn attention to the national practices and regulatory approaches being adopted by key players in the field, with a particular focus on the regulatory approaches adopted by the U.S. and the European Union (EU). The EU and the U.S. have made substantial progress in developing comprehensive regulatory frameworks for cross-border data flow, but these frameworks remain fragmented when applied to the maritime sector. The EU's General Data Protection Regulation (GDPR) exemplifies a rights-based approach, emphasizing data privacy and protection (EU (European Union)), while the regulatory framework of U.S. encourages free data flow, relying on industry self-regulation and international agreements rather than a centralized, comprehensive data protection law (Xu et al., 2024). Notably, when it comes to maritime cybersecurity, the U.S. takes a cautious approach to defend its national security (United States Coast Guard Cyber Strategy, 2015).

Although these studies and regulatory frameworks address crucial aspects of cross-border data governance, significant gaps remain. First, the specific needs of maritime data flow, particularly in relation to security and interoperability across different jurisdictions, have yet to be fully addressed. This gap complicates the legal landscape for shipping companies and other stakeholders involved in global maritime trade, as they must navigate a patchwork of regulations that vary significantly across jurisdictions. Second, there is a lack of research specifically targeting the governance of maritime data flow. This gap is particularly evident in how to tailor regulatory frameworks to the unique challenges posed by maritime data flow, especially in jurisdictions like China. Third, the absence of detailed regulatory guidelines for maritime data flow leaves ample room for disagreement about how to reconcile a goal of efficient data exchange with goals of promoting cybersecurity and national

1 LOGINK refers to the National Transportation and Logistics Public Information Platform, which is an open, public and sharing logistics information exchange network in China.

security. Therefore, while the growing recognition of the importance of cross-border maritime data flow is evident, there is an urgent need for more focused research and regulatory development to address the unique challenges posed by this sector.

1.3 Methodology and structure

This article employs a qualitative research approach combinning literature review, comparative analysis and normative analysis, aiming to provide a comprehensive examination of China's regulatory framework governing cross-border maritime data flow. The literature review establishes the conceptual foundation, identifies existing research gaps, and positions this study within the current academic discourse. The comparative analysis assesses and contrasts China's regulatory approach with those of selected jurisdictions, notably the EU and the U.S., thereby providing valuable insights from differing governance models. Finally, the normative analysis evaluates China's existing regulatory framework against internationally recognized data governance standards and principles, including the EU's GDPR, relevant initiatives of the IMO, and applicable ISO standards on data interoperability and security. This approach allows for identifying the extent to which China aligns with international standards and highlights areas requiring further regulatory development.

Section 2 examines the evolution of regulatory regimes surrounding cross-border data flow, highlighting China's shifting stance in this area. Building on this foundation, this section identifies and evaluates the integrated approach adopted to regulate cross-border maritime data flow. Section 3 examines two critical challenges confronting China's governance of cross-border maritime data flow: the tension between facilitating cross-border data flow and safeguarding national security interests, and the complexities associated with maritime data classification and grading. Finally, Section 4 offers targeted recommendations to address these challenges, emphasizing both technological innovation and legal improvement to enhance the efficacy of China's cross-border maritime data governance.

2 China's cross-border maritime data flow regulation regime

2.1 Paradigm shift in China's position on cross-border data flow

As a global leader in digital technology and digital economy, China has undergone a significant transformation in its regulatory approach to cross-border data flow. This evolution can be divided into two distinct phases. The first phase, from 2014 to 2022, prioritized stringent restrictions on cross-border data flow, with an emphasis on safeguarding national security. The second phase, beginning in 2023, represents a paradigm shift towards promoting the secure and orderly flow of cross-border data, with an emphasis on balancing national security concerns with facilitation of data exchange (Table 1).

(1)The first phase:restrictive approach to cross-border data governance.

In the 2010s, profound shifts in global governance, driven by changes in international power dynamics, intensified both traditional and emerging challenges, such as regional conflicts, technological innovations, and climate change. These developments posed increasing threats to global and national security. In response, China introduced the concept of a "holistic approach to national security" in 2014, recognizing cybersecurity as a critical pillar within its broader security framework (State Council Information Office of the People's Republic of China, 2024). This approach was formally integrated into the 2015 *National Security Law*, which emphasized the need for a secure and controllable digital infrastructure to safeguard national sovereignty security and development interests in cyberspace.[2]

Building on this foundation, China introduced its national big data strategy in the *13th Five-Year Plan (2016-2020)*, marking it as a pivotal component of the country's long-term development (Central Compilation and Translation Press of PRC). This strategy sought to advance socio-economic development through improved digital infrastructure, better integration and sharing of digital resources, and the enhancement of data security. The strategy also underscored the importance of protecting national key data sources and strengthening pre-warning capacities, thereby aligning economic innovation with national security imperatives.

From 2017 to 2022, China made significant strides in regulating cross-border data flow by establishing a comprehensive legal framework. This included the *Cyber Security Law* (National People's Congress of PRC, 2016), *Data Security Law* (National People's Congress of PRC, 2021a), *Personal Information Protection Law* (National People's Congress of PRC, 2021b), and the *Measures for Security Assessment for Outbound Data Transfer* (State Council of PRC, 2022). Together, these laws and regulations prioritize the protection of national security while facilitating cross-border data flow. They emphasize the creation of an information security system to ensure the controllability of critical data in sensitive sectors, impose strict export controls on data with national security implications and mandate that data generated and collected by critical infrastructure is stored within China's territory.

(2)The second phase:shifting toward relaxation of cross-border data flow.

In recent years, China has faced severe economic challenges, driven by the US-China trade conflict and the COVID-19

2 Article 25 of the National Security Law provides that "The State constructs a network and information security protection system, it upgrades network and information security protection capabilities, strengthens the innovation, research, development and application of network and information technologies, it realizes the security and controllability of core network and information technologies, crucial infrastructure and information systems and data in important areas; it strengthens network management, it prevents, curbs and lawfully sanctions online attacks, online hacking, online theft of secrets, the dissemination of unlawful or harmful information and other such online unlawful and criminal acts, it safeguards national sovereignty security and development interests in cyberspace."

TABLE 1 Framework of China's regulatory system for cross-border data flow.

Phase	Character	Name of the legislations
Restrictive Approach (2014-2022): Emphasis on National Security and Data Protection	National Security Protection	National Security Law (2015)
		Cyber Security Law (2016)
	Data and Privacy Protection	Data Security Law (2021)
		Personal Information Protection Law (2021)
	Cross-border Data Flow Controls	Measures for Security Assessment for Outbound Data Transfer (2022)
Facilitative Approach (2023-Present): Promoting Secure Cross-border Data Flow	Promotion and Regulation of Data Flow	Regulations on Promoting and Regulating Cross-border Data Flow (2024)
	Digital Trade Development	Opinions on the Reform, Innovation and Development of Digital Trade (2024)

pandemic. In response, China has prioritized economic reform, with data emerging as a crucial component of the digital economy and being recognized as a new productive force (Guo and Li, 2025). By 2022, China's digital economy accounted for 41.5% of its GDP, and the country became the second-largest global producer of data (Qiushi, 2023). The large cross-border digital trade markets require China to relax conditions for cross-border data flow. At the same time, the international community has actively sought to establish global frameworks for digital governance. Bilateral and multilateral efforts, such as the United Nations' Global Digital Compact (United Nations, 2024), World Trade Organization's negotiations on e-commerce (WTO (World Trade Organization), 2024), the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) (Department of Foreign Affairs of Australia, a), the Digital Economy Partnership Agreement (DEPA) (Ministry of Trade and Industry of Singapore), and Regional Comprehensive Economic Partnership (RCEP) (Department of Foreign Affairs of Australia, b), reflect the global consensus on promoting cooperation in regulating cross-border data flow. In light of these developments, China has increasingly recognized that its restrictive data policies create uncertainty for enterprises, and potentially undermines its competitiveness in the global digital economy (Chen, 2024). Consequently, the Chinese government has begun to reconsider and ease restrictions on cross-border data flow.

On 28 September 2023, the Cyberspace Administration of China (CAC) released the *draft Provisions on Regulating and Promoting Transborder Data Flow for public consultation*. Subsequently finalized and published as the *Regulations on Promoting and Regulating the Cross-Border Data Flow* (hereinafter "*the Regulations 2024*") on 22 March 2024 (CAC (Cyberspace Administration of China), 2024), the official title notably emphasizes "promoting" over "regulating", reflecting a more open and facilitative approach toward cross-border data flow governance. *The Regulations 2024* introduced significant changes, including eased restrictions on outbound data transfer and reduced compliance burdens for data processors. On 17 August 2024, the General Office of the CPC Central Committee and the General Office of the State Council jointly issued *Opinions on the Reform, Innovation and Development of Digital Trade*, which reiterated that China will promote and regulate the cross-border data flow, and build platforms for the high-standard opening-up of digital trade.

To sum up, over the past decade, China's approach to cross-border data flow governance has been gradually shifting from a government-led, restrictive model to a more market-oriented, facilitative model. This evolving legal system serves as the foundational framework for regulating cross-border maritime data flow (Table 2).

2.2 China's integrated approach on cross-border maritime data flow governance

To address the unique challenges posed by cross-border maritime data flow—such as the need for international interoperability, sector-specific data security, and alignment with global standards—China has adopted an integrated governance model. This model operates across three interrelated levels: a top-down legal and regulatory framework, mid-level sectoral policies, and bottom-up experimental and enterprise-led practices. These three layers interact dynamically, supporting China's efforts to coordinate national security, digital innovation, and international cooperation in the maritime domain.

(1) Legal and Regulatory Framework: Top-Down Institutional Foundations.

As discussed in Section 2.1, China's overarching legal framework for data governance—including the *Cybersecurity Law*, *Data Security Law*, *Personal Information Protection Law*, and the 2024 *Regulations on Promoting and Regulating the Cross-Border Data Flow*—establishes binding requirements for all sectors, including maritime activities. These laws clarify the classification and protection of important and sensitive data, mandate security assessments for outbound transfers, and define the roles of key regulators such as the Cyberspace Administration of China (CAC). While sector-neutral in design, this framework provides the legal foundation for regulating the collection, processing, storage, and cross-border transfer of maritime data.

TABLE 2 Timeline of China's regulatory approach to cross-border data flow (2014-2024).

Year	Key regulatory measures and policy documents	Regulatory orientation
2014	Holistic Approach to National Security introduced	Restrictive (National Security)
2015	National Security Law	Restrictive (National Security)
2016	Cyber Security Law	Restrictive (Data Localization)
2016	National Big Data Strategy (13th Five-Year Plan, 2016-2020)	Restrictive (Data Security)
2021	Data Security Law	Restrictive (Data Security)
2021	Personal Information Protection Law	Restrictive (Privacy Protection)
2022	Measures for Security Assessment for Outbound Data Transfer	Restrictive (Data Export Control)
2023	Draft Provisions on Regulating and Promoting Cross-border Data Flow	Facilitative (Promoting Data Flow)
2024	Regulations on Promoting and Regulating Cross-border Data Flow (Final Version)	Facilitative (Open & Secure Data Flow)
2024	Opinions on the Reform, Innovation and Development of Digital Trade	Facilitative (Promoting Digital Trade)

(2) Policy Coordination: Sectoral Instruments for Maritime Data Governance.

To translate national data governance mandates into actionable strategies tailored to the maritime domain, Chinese ministries have issued sector-specific policy guidance. In May 2019, Ministry of Transport of PRC, together with the CAC and five other departments, jointly issued the *Guiding Opinions on the Development of Intelligent Shipping* (hereinafter "*Guiding Opinions on Intelligent Shipping*"). The document set a strategic goal for China to become a global innovation hub for intelligent shipping by 2025. It identifies the promotion of public maritime data sharing, the development of international maritime information communication systems, and the piloting of cross-border data exchange mechanisms as national priorities. It also introduces a phased "pilot–evaluation–expansion" approach to guide local implementation and iterative policy improvement (Ministry of Transport of PRC, 2019).

(3) Local and Corporate Practices: Bottom-Up Experimentation and Innovation.

Building upon these legal and policy foundations, coastal Free Trade Zones (FTZs) and major shipping enterprises have developed pilot initiatives that test regulatory flexibility, strengthen interoperability, and enhance compliance with international standards.

Local Pilot Projects. Free trade zones (FTZs) such as the Shanghai Pilot FTZ have introduced localized policy frameworks to facilitate maritime data governance. Shanghai has implemented a series of measures to enhance the transparency and efficiency of data exchange, most notably through the development of the China Shipping Database (Shanghai International Shipping Institute, 2024), which aims to serve the global shipping industry. Similarly, the Guangdong-Hong Kong-Macao Greater Bay Area has advanced regional maritime data integration by launching joint initiatives—such as the Guangdong-Macao Intelligent Maritime Management Cooperation Arrangement—that promote mutual recognition of data standards and harmonized governance mechanisms (Maritime Safety Administration of PRC, 2022). In Hainan, pilot programs have tested simplified approval procedures for outbound data transfers under strict security conditions, offering models for streamlined but secure data governance (Hainan Development and Reform Commission, 2024).

Enterprise-Led Innovation. Leading Chinese shipping enterprises also play a central role. For instance, COSCO Shipping Lines has actively participated in international standard-setting processes, including the ISO 5909 project for blockchain-based electronic bills of lading. COSCO has also developed proprietary digital logistics platforms that support real-time, secure data exchange across its global network. China Merchants Group has invested in port digitization and smart logistics infrastructure, demonstrating the private sector's capacity to drive both technological advancement and compliance with evolving regulatory expectations.

3 Article XXI of the General Agreement on Tariffs and Trade (GATT) entitled "Security Exceptions", which provides: Nothing in this Agreement shall be construed (a) to require any contracting party to furnish any information the disclosure of which it considers contrary to its essential security interests; or (b) to prevent any contracting party from taking any action which it considers necessary for the protection of its essential security interests (i) relating to fissionable materials or the materials from which they are derived; (ii) relating to the traffic in arms, ammunition and implements of war and to such traffic in other goods and materials as is carried on directly or indirectly for the purpose of supplying a military establishment; (iii) taken in time of war or other emergency in international relations; or (c) to prevent any contracting party from taking any action in pursuance of its obligations under the United Nations Charter for the maintenance of international peace and security.

4 The vagueness and ambiguity center on whether Article XXI is self-judging by states. To be more specific, whether the phrase "which it considers" renders the security exceptions purely self-judging, thereby precluding judicial resolution of disputes; and how to define "essential national interest", "other emergency in international relations", etc.

5 See Article 17.13, "security exceptions", of RCEP, the largest free trade agreement in the Asia-Pacific region; Article 29.2, "Security Exceptions", of CPTPP, the first international trade agreement to make clear provisions for cross-border data flow.

In summary, China's integrated approach to cross-border maritime data governance reflects a multi-level model that blends national regulation, policy coordination, and decentralized experimentation. This model enables a more adaptive and context-sensitive response to the legal, technical, and geopolitical complexities of maritime data flows, while supporting China's broader strategy of aligning domestic governance with high-standard global rules.

3 Legal challenges faced by China's cross-border maritime data flow governance

3.1 Conflicts in cross-border maritime data flow and national security protection

As cross-border maritime data flow grows in volume and strategic significance, tensions have emerged between the imperative to facilitate seamless data exchange and the equally pressing need to safeguard national security. This tension presents one of the core legal challenges in China's evolving regulatory approach to maritime data governance (Pinchis-Paulsen, 2020).

3.1.1 The root of conflict: expanding connotations of national security

In the digital era, the traditional concept of national security has broadened to encompass cybersecurity, data sovereignty, and information infrastructure protection. Maritime data—ranging from vessel tracking and port operations to underwater terrain and maritime logistics—carries both commercial value and potential military sensitivity. As such, states increasingly regard maritime data as a strategic asset requiring heightened regulatory scrutiny. This expanded understanding of national security, while justifiable, complicates the legal balance between data openness and security control.

3.1.2 Fragmentation in global governance: legal uncertainty and divergent practices

International trade law does provide a legal basis for states to restrict cross-border data transfers in the name of national security. Article XXI of the GATT 1947, [3] commonly known as the "security exception" clause, permits deviations from trade obligations where a state deems it necessary to protect its essential security interests. However, this clause remains controversial and vague, particularly regarding whether its invocation is entirely self-judging and how terms like "essential security interests" and "emergency in international relations" should be interpreted.[4]

Recent regional trade agreements have incorporated this clause into digital trade rules, but with divergent interpretations. [5] The US-led United States of America, the United Mexican States, and Canada (USMCA) and CPTPP adopted a more assertive approach, emphasizing the discretionary power of states in invoking and applying the security exception provisions; the RCEP takes a more cautious stance, which expanded the scope of "essential national interest" while limited the autonomy of states; and the Digital Economy Partnership Agreement (DEPA) adopts a more balanced position. This legal fragmentation increases regulatory uncertainty for enterprises and undermines the predictability of cross-border data governance.

3.1.3 China's dual challenges: institutional gaps and external constraints

Domestically, China's fundamental position is to promote and facilitate cross-border maritime data flow, provided that essential national interests are safeguarded. However, the current national legal system remains underdeveloped. Although the Data Security Law establishes the security assessment mechanism for outbound data transfer, it lacks comprehensive implementation guidelines and corresponding legal consequences, leaving the framework insufficient to reconcile national security with cross-border maritime data flow facilitation effectively.

Internationally, the ambiguous nature of the "national security" exception has enabled some countries to impose data localization requirements or restrict Chinese companies from participating in foreign maritime digital infrastructure, often on vague security grounds. These practices risk politicizing cross-border maritime data governance and fragmenting global maritime supply chains.

3.2 Complexities of maritime data classification and grading

The *Data Security Law* 2021 establishes a national system of categorized and hierarchical protection for data based on its significance to economic and social development. To support its implementation, the National Technical Committee (TC260) on Cybersecurity of Standardization Administration of China released the GB/T 43697-2024 "*Data Security Technology-Rules for Data Classification and Grading*" (hereinafter referred to as "*the Rules for Data Classification and Grading*") in March 2024, which came into effect on October 1, 2024. This standard provides guidelines for applying hierarchical data protection in practice.

According to *the Rules for Data Classification and Grading*, data must be first classified by industry sector[6] and then by business attribute[7]. Certain data categories, such as personal information,

6 Article 5.1 (a) of *the Rules for Data Classification and Grading* provides that "the industry sectors include industrial data, telecommunications data, financial data, energy data, transportation data, natural resources data, healthcare data, education data, scientific data, etc.".

7 Article 5.1 (a) of *the Rules for Data Classification and Grading* provides that "common business attributes include but are not limited to business domain, responsible department, descriptive targets, process targets, data subjects, content themes, data purposes, data processing, data sources."

8 Article 5.1 (c) of the Rules for Data Classification and Grading.

9 Article 6.6 of *the Rules for Data Classification and Grading* provides that, when there are discrepancies in the classification of the same data, the higher-grade classification must be applied.

should be identified and classified according to relevant regulations and standards.[8] Data grading is then conducted in order to identify the degree of harm to national security, economic operation, social order, public interests, organizational rights, and individual rights that data may pose if it is leaked, tampered with, destroyed, illegally acquired, illegally used, or illegally shared. Data is graded into three levels from high to low risk: core data, key data, and general data. However, applying this data classification and grading system within the maritime sector presents two significant challenges.

3.2.1 Implications of overlapping data classifications

Data in the maritime industry often spans multiple categories, complicating its classification and subsequent grading. For example, ship dynamic data, primarily technical, may intersect with personal data or national security data due to the nature of maritime operations. This overlap creates ambiguity in maritime data classification, especially in cases where customer data in maritime operations is both personal data and commercial data. Another example is maritime financial data. Under the *Financial Data Security-Guides of Data Security Classification* (JR/T 0197-2020), data generated by financial institutions in shipping and port operations should be classified as financial data. However, according to *the Rules for Data Classification and Grading*, maritime financial data should be categorized by both industry and business attributes, leading to potential dual classifications.

This dual classification can lead to inconsistent grading, where maritime financial data might receive a higher-than-necessary security level due to the "strictest standard" principle.[9] This principle, while designed to resolve classification conflicts by applying the most stringent standards, can inadvertently increase compliance costs and complicate international maritime operations by imposing overly strict data protection measures. In the context of maritime financial data, when data is classified under both "financial data" and "maritime-specific data", it could lead to the application of higher security levels than necessary. This could result in the need for additional security measures, such as encryption, access controls, and audit trails, which can add financial and administrative burdens to international shipping and trade operations. The need for stricter security can also create delays in cross-border maritime data flow, disrupting real-time operations, port logistics, and customs procedures, ultimately increasing costs and reducing efficiency.

3.2.2 International variations in data protection standards

Another key challenge is the lack of alignment between national data classification systems and international data protection regulations. As each country develops its own data protection rules based on its legal, economic, and security concerns, discrepancies emerge in how maritime data is categorized and graded. These differences create challenges for cross-border maritime data flow, as countries may require differing security assessments, potentially leading to delays or even the rejection of maritime data transfer requests.

For example, some countries, like China, prioritize national security and economic significance when categorizing and grading shipping data, while others, like the EU, emphasize personal data protection under the GDPR. In practical terms, Chinese shipping companies handling European shipments must navigate the complex interplay between China's data classification and grading system, which might classify personal information involved in shipping sector as "key data" due to its economic importance, and the EU's GDPR, which mandates high levels of protection for personal data in maritime operations. This discrepancy requires companies to reconcile China's data classification and grading system with the GDPR's stringent requirements for data minimization and purpose limitation. Such alignment is crucial, as failure to comply with GDPR can lead to significant legal and financial consequences. This situation underscores the complexities of applying national data classification and grading system in a globalized maritime sector where multiple, sometimes conflicting, regulatory frameworks govern the data flow. The lack of alignment between different data protection regimes poses a significant barrier to smooth cross-border data flow, emphasizing the need for greater harmonization and cooperation between nations to facilitate global data exchanges while respecting local laws.

In conclusion, the challenges arising from overlapping data classifications, inconsistent grading, and international discrepancies complicate the governance of cross-border maritime data flows. The absence of a unified approach to data classification and grading, both domestically and internationally, exacerbates governance difficulties. Addressing these issues requires a more harmonized approach to data classification standards and a flexible approach to grading those accounts for the unique characteristics of maritime data.

4 Prospects for China's cross-border maritime data flow governance

As China continues to refine its approach to the governance of cross-border maritime data flow, several key prospects are emerging that could influence the future direction of both domestic and international data governance frameworks. These developments align with China's broader objectives of advancing technological innovation, balancing national security considerations with facilitating cross-border maritime data flow, and fostering international cooperation in both the maritime sector and data governance.

4.1 Advancing technological innovation and international technical cooperation

One of the key prospects for China's cross-border maritime data flow governance lies in the emphasis on technological innovation and international technical cooperation. As the global maritime industry increasingly embraces digitalization, the ability to leverage advanced technologies will be crucial in enhancing

efficiency, security, and transparency in data management. China's maritime sector is positioning itself at the forefront of this transformation, with a growing focus on the development of blockchain, big data, artificial intelligence (AI), and the Internet of Things (IoT) to drive the digitalization of the maritime industry and to promote secure and seamless cross-border maritime data flow.

China is actively investing in innovative technologies to facilitate smooth and secure cross-border flow of maritime data. In particular, blockchain has become a key enabler for secure, transparent, and immutable transactions in maritime logistics. By leveraging blockchain's decentralized nature, China is contributing to digital platforms that streamline data exchange while mitigating risks such as fraud and data tampering. The Global Shipping Business Network (GSBN), jointly developed by COSCO Shipping Lines and other key international stakeholders in global trade and logistics, facilitates real-time, secure data sharing across international shipping lines, ports, and logistics hubs, showcasing China's leadership in both technological innovation and secure digital infrastructure. Moreover, big data technologies enable the real-time processing of vast amounts of data from sources like cargo movement, ship performance, and port operations. These insights lead to optimized shipping routes, predictive vessel maintenance, and improved supply chain efficiency. Through these advancements, China is driving operational improvements that not only benefit the global maritime industry but also ensure the secure and efficient management of cross-border maritime data flow.

International technical cooperation is essential to ensure that China's technological innovations align with global standards and best practices, preventing the creation of fragmented technological frameworks. By engaging with international organizations such as the IMO and the WTO, China can actively contribute to the development of global data governance standards, particularly in areas such as interoperability, cybersecurity, and data exchange protocols. China's involvement in international research projects and the establishment of global maritime data exchange protocols will help bridge technological gaps between countries, promoting uniform standards that facilitate seamless cross-border maritime data flows. This collaboration reduces the risk of "data silos" and enhances the efficiency of global maritime trade, positioning China as a key player in shaping international maritime data governance.

4.2 Improving the classification and grading system for maritime data

A critical step toward strengthening China's cross-border maritime data governance lies in developing a sector-specific classification and grading system for maritime data. While the Data Security Law establishes general principles for data classification—dividing data into general, important, and core categories—it lacks sector-specific implementation rules that reflect the unique technical, operational, and geopolitical sensitivities of maritime data. To address this gap, a tailored system should be developed based on the following dimensions:

First, a detailed classification of maritime data should be created through empirical research. This classification should account for distinct data categories such as navigational data, port operation data, vessel tracking data, cargo manifest data, personnel information onboard, marine meteorological data, and hydrographic survey data. Each category should be evaluated for its commercial utility, operational criticality, and national security sensitivity.

Second, grading criteria should be developed by referencing three key factors: scope of impact (e.g., single port vs. national system), degree of sensitivity (e.g., real-time vessel location vs. historical route patterns), and affected stakeholders (e.g., government, enterprise, foreign actor involvement). These criteria can draw from existing methodologies proposed in data security scholarship, while adapting them to maritime-specific risks and governance needs.

Third, clear procedural rules should be established for data reclassification and regulatory oversight. This includes delineating which entities have the authority to classify or reclassify data, under what circumstances data can be downgraded for export, and what conditions trigger the need for a security assessment or cross-border approval.

Finally, China should pilot this classification and grading system in key Free Trade Zones such as the Shanghai Lingang FTZ, which has already issued experimental guidelines for graded data management. Lessons learned from these pilot zones can inform national legislation and future WTO-aligned commitments.

This targeted regulatory mechanism will enable more precise alignment between national security protection and the facilitation of cross-border maritime data exchange, directly addressing the regulatory ambiguity identified in Section 3.1.

4.3 Legalizing the concept of "national security" and Building International Consensus

In light of the ambiguity and fragmentation discussed in Section 3.1, China's proactive effort to clarify and legalize the concept of "national security"—both in domestic law and within international regimes—will be pivotal for advancing its maritime data governance objectives and shaping global norms in this domain.

Domestically, China should promote legislative clarification by articulating the scope and content of "essential national interests" in the maritime sector through statutory interpretation, administrative rulemaking, or dedicated regulatory guidance. Clearer definitional boundaries—especially when tailored to cross-border maritime data—will help reduce interpretive uncertainty, enhance regulatory consistency, and improve the operability of the outbound data assessment mechanism established under the *Data Security Law*. Additionally, the development of sector-specific supporting instruments, such as maritime security guidelines, will ensure

more practical and targeted application of the national security concept.

Internationally, China can play a constructive role by supporting institutional efforts—such as WTO jurisprudence—that aim to establish clearer review standards for invoking national security exceptions. Insights from recent WTO panel decisions provide valuable normative guidance. First, the national security exception is not entirely self-judging: states invoking it must act in good faith and provide a plausible link between the measure taken and the stated security concern (WTO Panel Report, 2020). Second, the definition of "national security" is evolving, extending beyond traditional military threats to encompass cybersecurity and data protection. Third, actions taken under the guise of national security must meet a threshold of seriousness, such as threats comparable to war or other emergencies in international relations (WTO Panel Report, 2022). These principles align with China's holistic view of national security and are consistent with the values outlined in the *Global Security Initiative Concept Paper* issued by the Ministry of Foreign Affairs (Ministry of Foreign Affairs of PRC, 2024). Promoting these interpretations in regional digital trade agreements, such as CPTPP and DEPA, would enhance legal predictability and foster international consensus.

In practice, China's FTZs have taken the lead in exploring how to balance national security protection with data flow liberalization. In particular, the *Measures for the Classified and Hierarchical Management of Cross-border Flow of Data in Lingang New Area of China (Shanghai) Pilot Free Trade Zone (for Trial Implementation)* (hereinafter "*Measures in Lingang*"), issued in February 2024, represent a significant institutional innovation (Shanghai Pilot Free Trade Zone Lingang Special Area). These measures aim to align domestic regulations with high-standard international rules by creating a structured system for classifying and grading cross-border data, establishing approval thresholds for outbound transfer, and prioritizing sectors—such as shipping—with urgent data exchange needs. However, the detailed classification list for maritime data has yet to be published, suggesting that further technical refinement and policy testing are needed to implement this regime fully.

Looking ahead, China is well-positioned to take a leadership role in bridging domestic and international approaches to national security in data governance. By leveraging its experience in national security reviews and data classification, China can propose internationally recognizable criteria for assessing maritime data risks. Moreover, the lessons learned from FTZ pilot projects—such as the negative list mechanism and tiered approval procedures—can inform the development of transnational models that accommodate both security protection and economic openness.

In sum, legalizing the concept of national security—through both internal clarification and external consensus-building—will not only improve the credibility and transparency of China's regulatory approach but also contribute to a more stable and cooperative international environment for cross-border maritime data governance.

5 Conclusion

This paper has examined the evolving governance framework for cross-border maritime data flow in China, with particular attention to its legal, institutional, and strategic dimensions. Against the backdrop of increasing data-driven maritime operations and heightened national security concerns, China has adopted a multi-level governance approach that integrates top-down legislation, mid-level sectoral policy guidance, and bottom-up experimentation through local and enterprise-led initiatives.

Section 2 outlined how this integrated framework enables China to navigate the complexity of cross-border maritime data governance by balancing the promotion of digital innovation with the imperative of safeguarding national interests. Section 3 analyzed the legal tensions that arise from expanding interpretations of "national security" and the fragmentation of international digital trade regimes, identifying maritime data classification and security exceptions as two core regulatory challenges. In response, Section 4 provided targeted policy recommendations, including the development of a sector-specific data classification and grading system, the legalization and clarification of national security concepts, and the promotion of international consensus through WTO jurisprudence and regional agreements.

China's efforts, particularly through Free Trade Zone pilots and international standard-setting engagement, reveal a growing capacity to contribute to the construction of globally interoperable, security-aware data governance norms. However, significant challenges remain, especially in aligning domestic regulatory mechanisms with high-standard international rules and ensuring legal predictability for maritime actors engaged in transnational data exchange.

Looking ahead, China is well-positioned to play a more proactive role in shaping international frameworks governing cross-border data flows in the maritime domain. This will require continued legal innovation, enhanced regulatory transparency, and sustained participation in global digital trade negotiations. The lessons from China's approach offer valuable insights for other countries seeking to balance digital openness with sovereign control, and contribute to the broader discourse on the future of maritime data governance.

Author contributions

MY: Methodology, Writing – original draft, Writing – review & editing, Funding acquisition. LW: Resources, Formal analysis, Writing – review & editing, Conceptualization.

Funding

The author(s) declare that financial support was received for the research and/or publication of this article. This work was supported by China Postdoctoral Science Foundation (No. 2021M703027), and research project of Office of Foreign Affairs Committee of the CPC Shandong Provincial Committee (No. 22CKFJ19).

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Generative AI statement

The author(s) declare that no Generative AI was used in the creation of this manuscript.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

CAC (Cyberspace Administration of China) (2024).Provisions on regulating and promoting cross-border data flow. Available online at: https://www.cac.gov.cn/2024-03/22/c_1712776611775634.htm (Accessed February 16, 2025).

Carlan, V., Coppens, F., Sys, C., Vanelslander, T., and Van Gastel, G. (2020). Blockchain technology as key contributor to the integration of maritime supply chain? *Maritime Supply Chains*, 229–259. doi: 10.1016/B978-0-12-818421-9.00012-4

Central Compilation and Translation Press of PRC The13th five-year plan for the economic and social development of the people's republic of China (2016-2020). Available online at: https://en.ndrc.gov.cn/policies/202105/P020210527785800103339.pdf (Accessed February 16, 2025).

Chen, M. (2024). Developing China's Approaches to regulate cross-border data transfer: relaxation and integration. *Comput. Law Secur. Rev.* 54. doi: 10.1016/j.clsr.2024.105997

Department for Science, Innovation & Technology, Department for Digital, Culture, Media & Sport (2021).National Data Strategy Mission 1 Policy Framework: Unlocking the value of data across the economy. Available online at: https://www.gov.uk/government/publications/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy/national-data-strategy-mission-1-policy-framework-unlocking-the-value-of-data-across-the-economy (Accessed February 16, 2025).

Department of Foreign Affairs of Australia CPTPP text and associated documents. Available online at: https://www.dfat.gov.au/trade/agreements/in-force/cptpp/official-documents (Accessed February 16, 2025).

Department of Foreign Affairs of Australia RCEP text. Available online at: https://www.dfat.gov.au/trade/agreements/in-force/rcep/rcep-text (Accessed February 16, 2025).

EU (European Union) General data protection regulation. Available online at: https://gdpr-info.eu/ (Accessed February 16, 2025).

Gregory Voss, W. (2020). Cross-border Data flow, the GDPR, and data governance. *Washington Int. Law J.* 29, 485–532.

Guo, S., and Li, X. (2025). Cross-border data flow in China: Shifting from restriction to relaxation? *Comput. Law Secur. Rev.* 56. doi: 10.1016/j.clsr.2024.106079

Hainan Development and Reform Commission (2024).Hainan free trade port data outbound management list (Negative list). Available online at: http://plan.hainan.gov.cn/sfgw/0400/202502/df645fd9512144af9e2879a7e63392ac.shtml (Accessed June 16, 2025).

Hong, Y. (2023). The logical deconstruction and institutional construction of China's Data Security Legislation. *Law Sci. Magazine* 2, 38–53. doi: 10.16092/j.cnki.1001-618x.2023.02.001

IMO (International Maritime Organization) (2022).Guidelines on maritime cyber risk management. Available online at: https://wwwcdn.imo.org/localresources/en/OurWork/Security/Documents/MSC-FAL.1-Circ.3-Rev.2%20-%20Guidelines%20On%20Maritime%20Cyber%20Risk%20Management%20(Secretariat)%20(1).pdf (Accessed February 16, 2025).

IMO (International Maritime Organization) (2023).Guidelines for harmonized communication and electronic exchange of operational data for ports calls. Available online at: https://wwwcdn.imo.org/localresources/en/OurWork/Facilitation/FAL%20related%20nonmandatory%20documents/FAL.5-CIRC.52.pdf (Accessed February 16, 2025).

IMO (International Maritime Organization) (2024).Maritime single window. Available online at: https://www.imo.org/en/OurWork/Facilitation/Pages/MaritimeSingleWindow-default.aspx (Accessed February 16, 2025).

ISO ISO/DIS 5909. Available online at: https://www.iso.org/standard/84288.html (Accessed May 20, 2025).

Liu, Z., Zhang, B., Zhang, M., Wang, H., and Fu, X. (2023). A quantitive method for the analysis of ship collision risk using AIS data. *Ocean Eng.* 272, 113906. doi: 10.1016/j.oceaneng.2023.113906

Ma, Q., Tang, H., Liu, C., Zhang, M., Zhang, D., Liu, Z., et al. (2024). A big data analytics methods for the evaluation of maritime traffic safety using automatic identification system data. *Ocean Coast. Manage.* 251, 107077. doi: 10.1016/j.ocecoaman.2024.107077

Maritime Safety Administration of PRC (2022).Maritime Safety Administration of the Ministry of Transport and Marine and Water Bureau of Macao sign the Guangdong-Macao Intelligent Maritime Management Cooperation Arrangement. Available online at: https://www.msa.gov.cn/html/xxgk/hsyw/20220906/03E75970-DAF1-4F13-B522-ACF54F3BC3B4.html (Accessed February 16, 2025).

Ministry of Foreign Affairs of PRC (2024).The global security initiative concept paper. Available online at: https://www.fmprc.gov.cn/eng/zy/gb/202405/t20240531_11367484.html (Accessed February 16, 2025).

Ministry of Trade and Industry of Singapore Digital economy partnership agreement. Available online at: https://www.mti.gov.sg/Trade/Digital-Economy-Agreements/The-Digital-Economy-Partnership-Agreement (Accessed February 16, 2025).

Ministry of Transport of PRC (2019).Guiding opinions on the development of intelligent shipping. Available online at: https://www.gov.cn/zhengce/zhengceku/2019-11/19/5456289/files/d374652a8cb74c65ac3097506230e1e7.pdf (Accessed February 16, 2025).

National People's Congress of PRC (2016).Cyber security law of the people's republic of China.

National People's Congress of PRC (2021a).Data security law of the people's republic of China. Available online at: http://www.npc.gov.cn/c2/c30834/202106/t20210610_311888.html (Accessed February 16, 2025).

National People's Congress of PRC (2021b).Personal information protection law of the people's republic of China. Available online at: http://en.npc.gov.cn.cdurl.cn/2021-12/29/c_694559.htm (Accessed February 16, 2025).

Paladin, Z., Kapidani, N., Lukšić, ŽCheckt. a. e., Nicoletti, T., Moutzouris, M., and Blum, A. (2022). "A maritime big data framework integration in a common information sharing environment," in *Paper presented at the 2022 45th Jubilee International Convention on Information* (Communication and Electronic Technology), 1161–1166.

Pinchis-Paulsen, M. (2020). Trade multilateralism and U.S. National security: the making of the GATT security exceptions. *Michigan J. Int. Law* 41, 109–193. doi: 10.36642/mjil

Qiushi (2023).Digital economy empowers China's high-quality development. Available online at: http://en.qstheory.cn/2023-06/01/c_891471.htm (Accessed February 16, 2025).

Shanghai International Shipping Institute (2024).China Shipping Database offers service for global shipping industry. Available online at: http://sisi-smu.org/2024/0911/c8958a237266/page.htm (Accessed February 16, 2025).

Shanghai Pilot Free Trade Zone Lingang Special Area Measures for the classified and hierarchical management of cross-border flow of data in Lingang new area of China (Shanghai) pilot free trade zone (for trial implementation). Available online at: https://www.lingang.gov.cn/upload/1/dm/1708483614845.pdf (Accessed February 16, 2025).

State Council Information Office of the People's Republic of China (2024).Holistic pursuit of national security lays solid groundwork for China's rejuvenation cause.

Available online at: http://english.scio.gov.cn/in-depth/2024-04/16/content_117127859.htm (Accessed February 16, 2025).

State Council of PRC (2022).Measures for security assessment for outbound data transfer. Available online at: https://www.gov.cn/zhengce/zhengceku/2022-07/08/content_5699851.htm (Accessed February 16, 2025).

Sun, L., Zhang, H., and Fang, C. (2021). Data Security governance in the era of big data: status, challenges, and prospects. *Data Sci. Manage.* 2, 41–44. doi: 10.1016/j.dsm.2021.06.001

United Nations (2024).Global digital compact. Available online at: https://www.un.org/global-digital-compact/sites/default/files/2024-09/Global%20Digital%20Compact%20-%20English_0.pdf (Accessed February 16, 2025).

United States Coast Guard Cyber Strategy (2015). Available online at: https://www.dco.uscg.mil/Portals/10/Cyber/Docs/CG_Cyber_Strategy.pdf?ver=nejX4g9gQdBG29cX1HwFdA%3D%3D (Accessed February 16, 2025).

USCC (U.S.-China Economic and Security Review Commission) (2022).LOGINK: risks from China's promotion of a global logistics management platform. Available online at: https://www.uscc.gov/research/logink-risks-Chinas-promotion-global-logistics-management-platform (Accessed February 16, 2025).

U.S. Department of Transportation (2024).Office of maritime security. Available online at: https://www.maritime.dot.gov/ports/office-security/office-maritime-security (Accessed February 16, 2025).

WTO (World Trade Organization) (2024).Joint statement initiative on electronic commerce. Available online at: https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/INF/ECOM/87.pdf&Open=True (Accessed February 16, 2025).

WTO Panel Report (2020). Russia-traffic in transit, WT/DS512/R, 2019; WTO panel report, Saudi Arabia-measures concerning the protection of intellectual property rights, WT/DS567/R.

WTO Panel Report (2022). United states-origin marking requirement, WT/DS597/R.

Xu, W., Wang, S., and Zuo, X. (2024). Global data governance at a turning point? Rethinking China-U.S. cross-border data flow regulatory models. *Comput. Law Secur. Rev.* 55. doi: 10.1016/j.clsr.2024.106061