ISSN: 2688-8645

A Study on the Risks and Market Access Regulations for AI-Driven Cross-Border Sharing of Financial Data under the Digital Trade Framework

Meiting Zhan, Qianying Wu, Ziyi Liu, Qingyuan Liu and Ye Ju *

Faculty of Law, College of Applied Arts and Science, Beijing, China

* Corresponding Author: Ye Ju (Email: juye@buu.edu.cn)

Abstract

AI technology is reshaping the paradigm of cross-border financial data flows within the digital trade framework, shifting from static transmission to dynamic collaboration and giving rise to threefold risks: data breaches, algorithmic abuse, and sovereignty conflicts. Traditional regulatory logic centered on territorial jurisdiction and post-incident accountability is becoming obsolete. Fragmented international rules lead to regulatory arbitrage and inefficient dispute resolution. A transformative pathway emerges, grounded in three theoretical pillars: sovereignty constraints, collaborative governance, and risk prevention. This approach replaces territorial sovereignty with algorithmic sovereignty, builds a multi-stakeholder collaborative governance network, and implements real-time circuit breaker-style risk prevention. The access system design centers on three core mechanisms: a dynamic data classification list anchored by the AI lifecycle, overcoming limitations of fixed attribute categorization; differentiated entity qualification reviews based on responsibility binding, clarifying the boundaries of rights and responsibilities for financial institutions, technology platforms, and overseas recipients; and a data purpose binding system using technical hardening, achieving "usable but invisible" financial data and automatic compliance. The implementation strategy involves: internally advancing regulatory technology empowerment and collaborative governance platform development; externally adopting a three-step approach—ASEAN pilot programs, Belt and Road expansion, and multilateral rule integration—to embed China's dynamic data classification into the global financial governance framework.

Keywords

Digital Trade; AI-Driven; Cross-Border Financial Data Sharing; Risk Prevention; Access System.

1. Problem Statement

Digital trade is reshaping the way cross-border factors are allocated. Data has shifted from being an accessory to transactions to a dominant production factor, and cross-border supply of financial services increasingly relies on cross-jurisdictional coordination of financial data. AI is gradually evolving into an infrastructure and decision-making engine as a foundational technology stack and an integrated platform, rapidly integrating scattered, multi-source, and heterogeneous data into a closed loop from models to decision-making flows and then to feedback, significantly enhancing the efficiency and accuracy of financial payments, credit granting, compliance, and risk control.

The current domestic and international legal systems, mostly established on static risk prediction models, have formed a structural contradiction with the dynamic data flow paradigm driven by AI. Therefore, the core task of regulating AI-driven cross-border sharing of financial

ISSN: 2688-8645

data is to drive the legal system to transform from static defense to dynamic response. This article attempts to explore from the institutional level how to construct a cross-border data trade rule system that is both risk-controllable and highly collaborative, in order to respond to the dual demands of security and openness in cross-border financial data flows in the era of digital trade.

2. Theoretical Evolution and Regulatory Legitimacy of Cross-Border Financial Data Sharing

2.1. The Evolution of AI-Driven Cross-Border Financial Data Sharing and the Transformation of Its Regulatory Models

For AI-driven Cross-border Sharing of financial data digital trade rules, as the international framework for regulating core issues such as data cross-border flow and the treatment of digital products, provide a preliminary institutional context for the globalization collaboration of financial data. AI-driven cross-border sharing of financial data refers to the process of collecting, analyzing, transmitting, and collaboratively using financial data from different jurisdictions in the context of digital trade, through the utilization of AI technology, and achieving systematic mechanisms for functions such as financial risk assessment, credit pricing, and demand forecasting through a continuously evolving shared value model. This mechanism is deeply integrated into the cross-border transaction processes of goods and financial services, enabling collaborative sharing of financial data and assetization, and ultimately transforming into a dynamic and intelligent value generation system. Compared to the document-based data flow in traditional financial trade, AI-driven cross-border sharing of financial data has undergone paradigm shifts in the dimensions of financial data, technical architecture, risk forms, and regulatory logic (see Table 1). The cross-border sharing system of financial data has gradually evolved into algorithmic collaboration, and it is urgently necessary to restructure the regulatory logic in theory to support the reconfiguration of the core regulatory framework.

Table 1. Comparison between Traditional Financial Trade and AI-driven Cross-border Sharing of Financial Datal

Comparison Aspect	Traditional Financial Trade Data	AI-Driven Cross-Border sharing of Financial Data	Core Leap Points
Financial Data	Paper-based documents, structured data	Multimodal unstructured data	Data shifts from static to dynamic, digital and real-time
Technical Architecture	Relies on centralized systems, empirical rules	Relies on privacy computing, blockchain, large models, machine learning and other technologies	Shifts from experience-driven to technologically intelligent and automated operation
Risk Profile	The structure of power and liability risks is clear	AI restructures the power and liability risk structure	Risks are more complex and concealed; governance frameworks require systematic foresight
Regulatory Logic	Clear rules, cleart audit trails	Rapid model iteration, difficult regulatory and auditing is difficult	Regulatory challenges increase, need to shift towards technology-driven approaches

ISSN: 2688-8645

2.2. Theoretical Underpinnings of AI-Driven Cross-Border Financial Data Sharing within the Digital Trade Framework

2.2.1. Constraining Sovereignty: Reconfiguring Jurisdictional Boundaries from Territoriality to Algorithmic Sovereignty

Data sovereignty serves as the logical starting point for AI-driven cross-border financial data sharing. However, its data localization requirements fundamentally conflict with the open flow emphasized by digital trade rules. In AI scenarios, intangible data transcends geographical boundaries, subjecting national sovereignty to unprecedented challenges [1]. Traditional sovereignty frameworks are inadequate for AI contexts, making the transition from “territorial jurisdiction” to “algorithmic sovereignty” an imperative.

To effectively resolve this fundamental conflict, a dynamic data classification system must be established to stratify sovereignty. Within AI scenarios, a multidimensional classification system should be established based on data generation logic, with risk grading according to harm impact levels[2]. Diverse technical measures should be employed to protect and govern financial data. Shifting from static data classification to a dynamic grading system, data sovereignty theory not only defines the scope of data subject to national sovereignty concerns within the digital trade framework, ensuring differentiated exercise of sovereignty, but also establishes power boundaries for subsequent multi-subjects’ engagement.

2.2.2. Collaborative Governance: The Dynamic Reconfiguration of Rights and Responsibilities Among Multiple Actors

The global nature of digital trade necessitates building multi-subjects governance networks within sovereign sphere, with collaborative governance theory providing an organizational blueprint. Key participants include national governments, international organizations, and other differentiated entities. As collaborative governance progresses, challenges emerge: disorder governance divisions of labor, disconnects between governance and actual needs, and inefficient governance processes[3]. Therefore, it is necessary to reshape the form of collaborative governance by fully leveraging AI to build an integrated collaborative governance platform encompassing communication, information disclosure, and decision support[4]. Based on the distinct roles of diverse subjects, establish responsibility-binding, differentiated access review standards to achieve dynamic reshaping of authority and responsibility. This provides a structural foundation for reviewing subject qualifications. Within the digital trade framework, collaborative governance theory offers a platform for international cooperation in national regulation, facilitating the efficient cross-border flow of financial data.

2.2.3. Risk Prevention: The Shift in Regulatory Logic from Ex-Post Remedy to Real-Time Circuit Breakers

After defining authority boundaries and stakeholder structures, theoretical frameworks must ultimately guide action. The risk prevention principle provides a methodological approach. Modern digital trade rules recognize nations' sovereign right to implement precautionary measures for public policy objectives, but increasingly advocate for AI-driven, dynamic, end-to-end risk prevention.

Risk prevention in AI scenarios emphasizes ex ante review mechanisms and timely response mechanisms. Ex ante review means that enterprises voluntarily apply for certification, organize their own risk assessments, and predict risks through results to determine whether to apply for review, with enterprise self-review as the principle[5]. A multi-layered liability system shifts legal responsibility from punishment to prevention through compliance improvement pressure, thereby curbing potential risks at their source. The key to timely response mechanisms lies in strictly binding AI's cross-border data usage with clear compliance boundaries, dynamically collecting risk information, and automatically triggering corresponding alert levels through the system. This enables intelligent identification and early warning of abnormal data

ISSN: 2688-8645

flows. Applying the precautionary principle provides a methodological framework for balancing security and development objectives in digital trade.

Thus, achieving a paradigm shift in cross-border financial data sharing driven by AI requires a theoretical fulcrum formed by the underlying reconstruction of sovereignty, collaborative mechanisms, and risk prevention. These three elements form a progressive system within AI scenarios, evolving from boundaries to structures to methodologies. Based on this, a corresponding mapping relationship emerges from theory to institutional formation (see Table 2). Abstract legal principles should be translated into operational institutional mechanisms to establish a governance system for AI-driven cross-border financial data sharing.

Table 2. Theoretical-Institutional Mapping Table

Theoretical Foundation	Institutional Mapping Pathway
Sovereign Constraints	Dynamic Data Classification System, Enabling Precise and Dynamic Exercise of Sovereignty
Collaborative governance	Framework for Entity Qualification Review, Shaping a Diverse and Collaborative Dynamic Governance Network
Risk Prevention	Data Usage Binding Mechanism Under Behavioral Regulation: Establishing End-to-End Monitoring and Real-Time Circuit Breaker Risk Control

3. Mapping the Risks and Challenges of AI-Driven Cross-Border Financial Data Sharing within the Digital Trade Framework

3.1. The Risk Landscape of AI-Driven Cross-Border Financial Data Sharing within the Digital Trade Framework

Within the digital trade landscape, the deep application of AI technology and cross-border regulatory barriers form a risk spectrum. The inherent vulnerabilities of AI technology serve as the source of risk, amplified through cross-border business chains to ultimately impact national financial data sovereignty. This manifests as a tripartite transmission mechanism encompassing technology, regulation, and sovereignty.

3.1.1. Compounded Risks of Financial Data Breaches: AI-Driven Processes and Cross-Border Barriers

Within the digital trade ecosystem, AI technology is reshaping traditional financial business models while simultaneously giving rise to multifaceted security challenges. AI models possess inherent structural vulnerabilities in security. Financial institutions increasingly rely on third-party AI service providers to aggregate highly centralised data into data asset pools. As a critical link in digital trade supply chains, any security breach within these systems could trigger cascading risk propagation. This would exacerbate systemic fragility within the financial sector, creating cross-border risk diffusion effects that pose dual threats to both personal financial privacy protection and the operational security of financial institutions[6]. Concurrently, cross-border data flows encounter multiple legal and policy barriers, amplifying systemic risks in global financial operations[7]. Governments worldwide implement data localisation measures mandating the domestic storage of sensitive financial data, creating tension with the inherent need for efficient digital trade circulation. This compels multinational financial institutions to adopt decentralised data storage architectures, trapping data security within a compliance-versus-security dilemma. Even when local storage requirements are met, cross-border data transfers remain subject to complex approval and assessment mechanisms. Multinational financial institutions must simultaneously comply with multiple heterogeneous legal systems across participating digital trade nations, while attackers may exploit jurisdictional arbitrage to evade cross-border accountability[8]

ISSN: 2688-8645

The interplay between AI technology and cross-border data regulation constitutes a nonlinear risk amplification mechanism, rendering the root causes of data breaches difficult to pinpoint. On the one hand, traditional data anonymisation and de-identification techniques become markedly less effective against AI's powerful associative reasoning and reconstruction capabilities. Attackers can achieve re-identification through cross-dataset correlation analysis, leading to risks where compliance appears formal yet substantive violations persist. Conversely, the distributed and cross-border nature of the technology supply chains underpinning global digital trade means vulnerabilities in any single component can rapidly propagate and amplify risks throughout the chain (see Fig.1). Furthermore, cross-border regulatory barriers severely impede vulnerability remediation and coordinated responses.

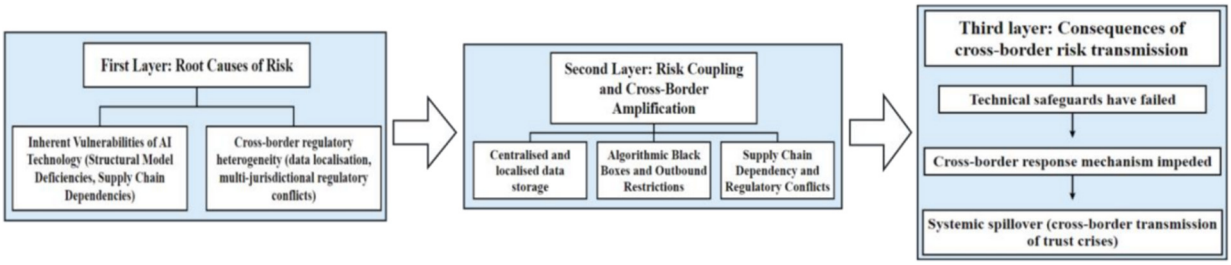

Fig 1. Data Breach Risk Transmission Flowchart Under Dual Influences of AI-Driven Factors and Cross-Border Regulation

3.1.2. Financial Data Misuse Risks Catalyzed by AI Algorithmic Attributes and Regulatory Divergence

Table 3. Comparison of Financial Regulatory Models Across Major Global Economies Driven by Artificial Intelligence

Regulatory dimension	European Union	United States	China
Core Philosophy	Power above all, pursuing risk prevention	Mobility first, innovation foremost, accountability through post-event review	Synergy between Sovereignty and Development
Regulatory Paradigm	Strictly Prudential Approach: Unified Legislation and Comprehensive Supervision	Flexible and adaptable, decentralised and sector-specific regulation	State-led, top-down approach, with equal emphasis on development and regulation
Primary regulatory mechanism	Risk classification and tiering with penetrative supervision	Reliance on institutional oversight and judicial precedent	Implementation of data cross-border security assessments[11], algorithmic registration systems and regulatory sandbox approaches
Severity of penalties	Hefty fines are the most effective deterrent	Substantial settlements and class action compensation	Administrative penalties and criminal liability form a combined approach

In the digital transformation of finance driven by digital trade, AI algorithms harbour systemic risks of abuse[9]. Firstly, the predictive accuracy of high-performance AI models relies on the volume, dimensionality, and timeliness of training data, compelling financial institutions to push beyond data collection boundaries in competitive environments. Secondly, AI algorithms can infer users' undisclosed sensitive attributes from superficially compliant data, giving rise to indirect discrimination and unfair pricing. Their black-box nature not only obscures individual decision-making injustices and amplifies systemic market risks, but also serves as a pretext for enterprises to circumvent scrutiny, undermining accountability mechanisms and causing regulatory lag. Thirdly, AI-powered generative agents can automate

ISSN: 2688-8645

market abuse, challenging traditional financial governance models reliant on human oversight and ex post accountability [10].

Major global economies exhibit divergent institutional traditions, risk prevention priorities, and developmental objectives, giving rise to differentiated financial regulatory frameworks (see Table 3). The inherent heterogeneity of these systems is deeply intertwined with the intrinsic characteristics of artificial intelligence. This interplay not only profoundly impacts the compliance costs and efficiency of cross-border financial activities but also reshapes the power structures and risk transmission dynamics within global financial governance.

3.1.3. The Risk of Sovereignty Conflicts over Cross-Border Financial Data: Between the Borderless Nature of AI and the Bounded Nature of Sovereignty

The boundless nature of AI technology is systematically reshaping the paradigms of global financial data flows and risk structures within digital trade. On one hand, the inherent cross-border nature of financial data flows and the multinational deployment capabilities of AI models create institutional conflicts with national data localisation policies. On the other hand, the black-box characteristics of algorithms and cross-border capital fluctuations triggered by high-frequency trading expose the profound lag and real-time regulatory challenges inherent in traditional territorial regulatory frameworks.

Traditional financial data sovereignty emphasised a nation's supreme control over the generation, storage, processing, and transmission of domestic financial data. However, within the digital trade context, computing power has become an essential prerequisite for unlocking data value and enabling financial data to participate as a production factor in global trade, directly impacting financial innovation efficacy and national competitiveness. Furthermore, geopolitical conflicts in the digital trade sphere have shifted security risks down the computing power supply chain, compelling the extension of sovereign boundaries to hardware and foundational software layers. The form of sovereignty is transitioning from static control over data to dynamic control over data processing capabilities—that is, an outward expansion into the realm of computing power sovereignty. This trend is evident in China's international practices, such as its emphasis on the security and controllability of critical financial information infrastructure. Nevertheless, it faces formidable challenges, including high barriers to independent innovation and the potential for US technological nationalism[12] to create computing power silos and efficiency losses within the digital trade landscape.

3.2. Regulatory Challenges in Governing AI-Driven Cross-Border Financial Data Sharing under the Digital Trade Framework

3.2.1. At the Domestic Level: The Inadequacy of Static Classification and Formalistic Review in Addressing Dynamic Risks

Regarding data classification standards, the Data Security Law employs a static logic that categorizes data based on inherent attributes and predefined risk levels, binding protection intensity to data classification tiers. In AI scenarios, the integration and analysis of multiple low-sensitivity datasets, coupled with evolving cross-border financial data flows, can generate new high-sensitivity information and dynamic risks. Static classification fails to provide differentiated regulatory guidance for such scenarios, hindering the sustainable development of cross-border financial data sharing. This fundamentally conflicts with the principles of freedom and efficiency advocated by digital trade rules.

Furthermore, access reviews primarily rely on formal examinations, lacking dynamic oversight of risks after data exits the country. Article 7 of the Measures for the Security Assessment of Data Outbound Transfer details the materials required for declaring data outbound transfers. Although Article 9 stipulates that “on-site verification of the declarant may be organized to prevent data security risks”, seemingly implementing “substantive review”, this

provision appears more like a means for regulators to enhance the effectiveness of formal review by retaining this authority. Therefore, it remains fundamentally centered on formal review. The significant disconnect between current reviews and substantive risks constitutes a substantial barrier to the free flow of data, failing to meet the inherent requirements of digital trade for the efficient allocation of data as a key factor.

3.2.2. At the International Level: Deficiencies in Soft Law Efficacy and Conflicts in Rules Reciprocity

The issue with the international regulatory framework lies in the prevalence of declarations of principle over operational obligations, resulting in insufficient binding force for international rules. This prevents effective handling of real-time issues arising from cross-border financial data flows driven by AI. The application of international provisions relies heavily on subjective interpretations by individual nations. Regulatory bodies, as governmental agencies, may be influenced by external factors such as international relations, leading to biased oversight and the imposition of restrictive measures that fail to align with actual risks[13]. According to the WTO's Understanding on Rules and Procedures Governing the Settlement of Disputes, under clear rules and smooth processes, a case may take two to three years or even longer to progress from consultations to final enforcement. Even with the CPTPP's enhanced dispute resolution efficiency, the process still requires several months or more. This fails to provide timely compensation for compliant parties nor impose prompt sanctions on violators.

Regarding dispute resolution mechanisms, there is a lack of effective mutual recognition and convergence mechanisms. For instance, while the CPTPP prohibits data localization, the RCEP permits member states to restrict data flows under the justification of “legitimate public policy”[14]. This has increased uncertainty in the cross-border flow of financial data and raised compliance costs for businesses. Furthermore, developed and developing economies generally hold divergent views on digital trade rules, with digital trade governance exhibiting regional and bloc-based characteristics[15]. For instance, major trading nations such as the United States, China, and the European Union exhibit significant divergences in their data governance paradigms, creating a new digital divide[16].

4. Designing a Market Access Regime for Cross-Border Financial Data Sharing within the Digital Trade Framework

4.1. A Risk-Anchored, Dynamic Grading System for Market Access to Financial Data

4.1.1. Formulating a Dynamic Grading List for Financial Data in the Context of AI Applications

Data classification, categorization, and identification serve as foundational tasks for implementing technical controls and commercial operations, and are also central to the governance of cross-border data flows[17]. Globally, more than 135 countries have enacted data protection laws, most of which include rules governing the cross-border transfer of financial data. However, the existing regulatory framework is largely shaped by European and American systems[18]. China’s current static four-tier classification system, based on inherent data attributes, adopts a “one-size-fits-all” approach, which suffers from delayed adjustments and a regulatory focus that remains limited to controlling data export.In contrast, the application of AI systems often involves the intertwining of diverse data types, making traditional static classification inadequate for matching actual risks. There is an urgent need to shift the review mechanism from static categorization to dynamic identification. The dynamic tiered list for AI scenarios classifies data based on three dimensions: data attributes, application scenarios, and processing activities. This enables more real-time and proactive adjustments, extending

ISSN: 2688-8645

regulatory coverage to risks across the entire AI lifecycle. The list establishes an integrated digital regulatory mechanism of "perception –assessment –execution, "which not only effectively addresses flow-related risks but also enhances the efficiency of data movement(see Fig.2).

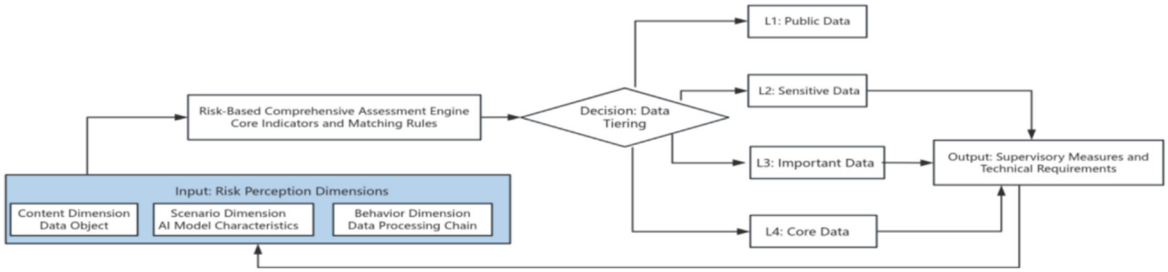

Fig 2. AI-Driven Dynamic Tiered List for Cross-Border Financial Data

4.1.2. Entity Qualification Review under the Principle of Accountability Linkage

To align data tiering with the mobility risks associated with AI models, it is necessary to establish a dynamic adjustment mechanism capable of continuously perceiving the operational environment in which data are situated, the relevant processing activities, and the resulting technological consequences. This mechanism comprises two core components. First, an annual assessment conducts a systematic review across three dimensions within the AI lifecycle: the evolution of model use cases, model performance and bias, and the maturity of the cross-border regulatory and technical environment. On this basis, the corresponding data risk levels are recalibrated. Second, a trigger-based mechanism functions as an emergency response system. It automatically escalates risk classifications in the event of AI security incidents, data misuse, or abrupt changes in the legal environment. Conversely, where technological advances lead to a measurable reduction in risk coefficients, a downgrade assessment may be initiated accordingly (see Fig.3).

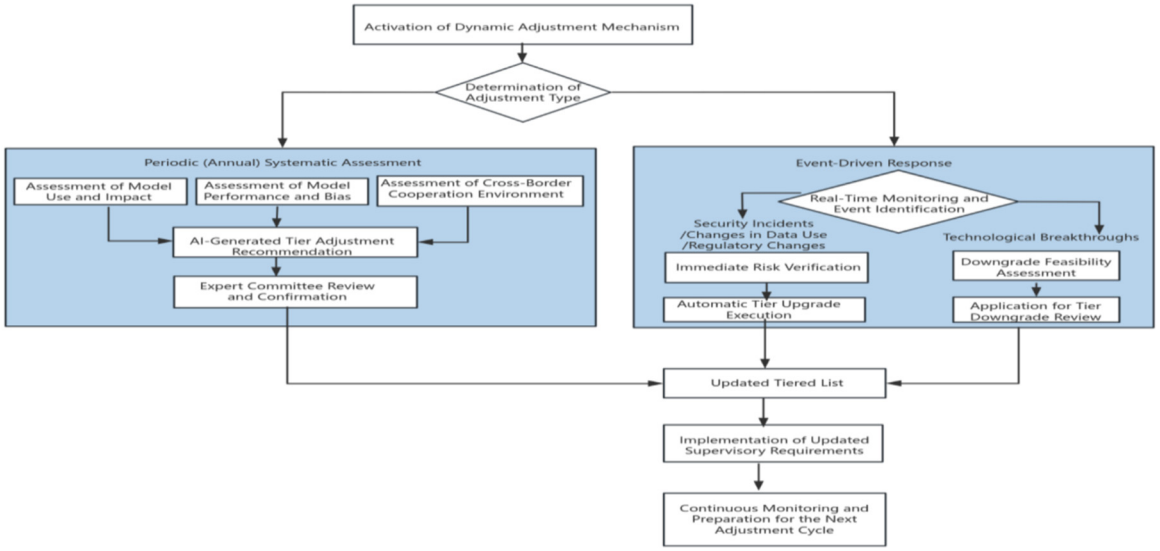

Fig 3. Dual-Track Dynamic Adjustment Mechanism for Cross-Border Financial Data

4.2. Subject Qualification Review under the Principle of Responsibility Binding

4.2.1. Prioritizing Holistic Data Governance Capability in Cross-Border Financial Institutions

The review of cross-border data transfers by financial institutions should center on their overall data governance capabilities and capacity for systemic risk prevention. In practice, such reviews should assess three principal dimensions. First, institutions should demonstrate a governance framework that covers the entire data lifecycle, including data classification and

ISSN: 2688-8645

tiering in AI application scenarios, the deployment of encryption technologies, and employee security training. Second, evaluators should examine the approval and accountability mechanisms governing the cross-border transfer of high-risk data, as well as the institution's record of legal compliance. Third, the business legitimacy of data exports should be assessed, with particular attention to the necessity of data transfers in specific use cases, such as AI-enabled cross-border payments and automated investment advisory services.

4.2.2. Requiring Technology Platforms to Ensure Security and Neutrality in Technical Architecture

As critical hubs in the cross-border flow of financial data, technology platforms should be subject to reviews that focus on technical security and algorithmic compliance. In collaborative arrangements, platforms are required to clearly delineate responsibility boundaries in order to prevent excessive data collection or improper use. By deploying technologies such as federated learning and differential privacy, platforms can operationalize the principle of "compliance by design", thereby strengthening data protection while simultaneously promoting financial innovation. In addition, platforms should establish regulatory interface mechanisms to support real-time monitoring and cross-border auditing.

4.2.3. Requiring Overseas Data Recipients to Ensure Commensurate Data Protection

The review of overseas data recipients should focus on whether they are capable of providing security safeguards that are substantially equivalent to China's level of financial data protection within their respective domestic legal environments. Three dimensions merit particular attention. First, the compatibility of the recipient jurisdiction's legal framework with China's regulatory requirements should be assessed. Second, the adequacy of technical safeguards and internal management measures should be evaluated to ensure that data are used strictly in accodance with the agreed purposes. Third, overseas recipients should commit to accepting necessary forms of cross-border regulatory cooperation and to establishing effective mechanisms for regulatory coordination.

4.3. Use Limitation and Compliance Boundaries under a Behavioral Regulation Approach

4.3.1. Defining Lawfulness within Specific AI Application Scenarios

In AI application scenarios, the legal boundaries governing the cross-border flow of financial data should be incorporated as embedded clauses into data export licenses and access documentation, thereby establishing legally binding constraints. The permitted scope of use must be strictly confined to scenarios directly related to financial security and stability, such as cross-border payments, anti-money laundering supervision, intelligent exchange rate forecasting, and the optimization of international settlements. Furthermore, explicit prohibitive provisions must be established to rigorously define the purpose and scope of data usage, strictly prohibiting any deviation of data application from its core intended objectives.

4.3.2. Strengthening Data Security through Technical Hardening

Security should be strengthened through technical measures, with tiered protections implemented according to the risk level of the data. For low- and medium-risk data, standardized logging and digital watermarking techniques are employed to ensure full traceability and accountability in the event of leaks. For important data, privacy-preserving computation technologies, such as federated learning, are mandatorily applied to guarantee that data remain "usable but not visible". For core data, smart contracts are deployed to enforce automatic compliance controls, with real-time suspension of access upon detection of unauthorized use. By establishing a progressive technological framework—from traceability and leak attribution, to usability without visibility, and finally to automated enforcement—an intelligent security barrier can be constructed that aligns with the corresponding risk levels.

ISSN: 2688-8645

5. Institutional Safeguards and Pathways for Enhancing the Implementation of the Cross-Border Financial Data Access Regime within the Digital Trade Framework

5.1. At the International Level: Embedding Chinese Standards within the Global Financial Governance Architecture

5.1.1. Promoting the Harmonization of Dynamic Grading Standards through an ASEAN Pilot Program

China could prioritize pilot initiatives with advanced ASEAN members such as Singapore and Malaysia, leveraging the ASEAN Digital Masterplan 2025 and DEFA negotiations to promote compatibility of data tiering standards. In emerging markets such as Indonesia and Vietnam, China could use technical assistance programs to disseminate its dynamic data tiering standards for AI applications and share best practices in data governance. Simultaneously, a China–ASEAN Financial Data Regulatory Sandbox could be established, allowing certified institutions to conduct cross-border data transfers within predefined limits based on tiered classifications. This approach would facilitate the coordinated development of regional financial security and digital trade.

5.1.2. Disseminating the Data Dynamic Adjustment Regulatory Framework through the Belt and Road Initiative

Building on the ASEAN pilot programs, China could extend these initiatives to Belt and Road partner countries and form a standards alliance. By establishing a cooperative mechanism for cross-border financial data governance, member states could achieve mutual recognition of low-mobility data whitelists under AI application scenarios. In contexts such as cross-border supply chain finance and infrastructure investment and financing, China's standards could be actively applied through federated learning nodes to conduct joint AI modeling, ensuring that key Chinese business data remain "usable but not visible" while supporting multinational risk management. This approach would promote the harmonization of standards among Belt and Road countries and contribute to building a digital community of shared destiny.

5.1.3. Integrating Multilateral Rules into China's Dynamic Data Governance Mechanism

Within multilateral frameworks such as RCEP and CPTPP, China should actively promote the adoption of dynamic data tiering standards as a regional consensus. Specifically, in the context of RCEP upgrade negotiations, China could advocate for the incorporation of dynamic tiering standards and dynamic adjustment mechanisms into the e-commerce chapter, elevating these approaches from a national proposal to an Asia-Pacific standard and promoting them to countries with underdeveloped data governance systems. Facing the more stringent regulatory requirements of the CPTPP, a dual-track strategy could be adopted. On one hand, China can demonstrate its privacy-preserving computing practices in cross-border insurtech and intelligent investment advisory services, thereby showing that strict regulation and high-level openness can coexist. On the other hand, China can invoke financial prudential exceptions to safeguard control over core data, while advocating for the establishment of cross-border data flow emergency mechanisms. These mechanisms would explicitly prohibit discriminatory practices based on cross-border data processing. By incorporating provisions for substantially equivalent data protection in bilateral and multilateral agreements, China can contribute its expertise to global digital governance.

ISSN: 2688-8645

5.2. At the Domestic Level: Driving the Implementation of Dynamic Data Access Rules

5.2.1. Institutional Guarantees: Legal Frameworks for Facilitating Efficient Cross-Border Data Flows

Legal frameworks should move away from a "one-size-fits-all" management approach and instead construct differentiated access pathways based on the risk levels associated with AI application scenarios. At the same time, a flexible institutional evolution mechanism should be established, with legislation providing interface provisions that authorize regulatory authorities to adjust requirements in response to technological developments. Additionally, a regulatory sandbox system should be instituted to provide compliant experimentation space for innovative financial services. The design of legal norms must balance stability with adaptability, leaving sufficient room for the responsible opening of financial data, thereby achieving an integrated approach that combines high-level openness with robust risk management.

5.2.2. Technical Empowerment: Regulatory Technology for Comprehensive Prevention and Control of Flow-Related Risks

At the technological level, the development and application of regulatory technology (RegTech) should be actively promoted to achieve intelligent financial risk prevention and control. A national-level platform for cross-border financial data supervision should be established, enabling real-time monitoring and automated interception of high-risk activities such as letters of credit and settlement processes through smart contracts. In scenarios such as cross-border fraud prevention and exchange rate forecasting, the mandatory use of federated learning should ensure that data remain "usable but not visible". By combining intelligent risk control with privacy-preserving computation, a robust regulatory baseline can be maintained that prevents unauthorized data export, providing essential technical support for financial openness.

5.2.3. Collaborative Governance: Building a Community for Cross-Border Financial Data Governance

At the collaborative governance level, efforts should focus on establishing a cross-border financial data governance community, prioritizing the signing of regulatory cooperation agreements with financial hubs such as Hong Kong and Singapore to achieve mutual recognition of data tiering standards and joint supervision. Encrypted channels can be used to conduct joint inspections of wealth management and other financial activities, while specialized arbitration tribunals should be established to handle cross-border data disputes. By relying on mutual recognition of rules, coordinated supervision, and dispute resolution mechanisms, an internationalized governance system for cross-border finance can be constructed.

6. Conclusion

AI-driven cross-border sharing of financial data is reshaping global financial infrastructure, representing a fundamental transformation in the paradigm off actor mobility within the digital trade era. The conflict between static rule-based frameworks and dynamic governance has intensified. Establishing an integrated governance framework centred on "dynamic tiering, responsibility binding, and purpose locking" essentially embeds the characteristics of AI technology within legal regulation. A deeper institutional innovation lies in the paradigm shift from sovereign cession to algorithmic sovereignty. Moving forward, cross-border financial data governance must overcome multiple frontier challenges: technologically, confronting new risks such as quantum computing's impact on cryptographic systems and reverse attacks on federated learning models; institutionally, balancing the market-based allocation of data factors with prudent financial regulation; and internationally, prioritising the establishment of cross-

border regulatory sandboxes and rapid dispute resolution mechanisms amid divergent digital sovereignty perspectives. A global perspective is essential, leveraging multilateral platforms such as ASEAN and the Belt and Road Initiative to establish new paradigms for cross-border financial data sharing and access that both safeguard financial security and foster digital trade development.

References

[1] Xu Yumei, Yang Liu, Lü Wei. “Freedom” and “Sovereignty”: The Dynamic Game of Cross-Border Data Flow Governance Models—A Perspective from Global Digital Trade Rules [J]. Administrative Forum, 2024, 31(06): 161.

[2] Zhang Jing, Zhu Chengfeng. Governance Challenges and Improvement Pathways for Cross-Border Financial Data Flow [J]. Journal of Financial Development Research, 2025(06): 83-84.

[3] Zheng Linhao, Xu Yingfang, Ren Yuzhuo. Establishing a National Data Security Governance System: Theory, Challenges and Countermeasures [J]. Price Theory and Practice, 2023, (9): 55.

[4] Guo Hailing, Liu Zhongshan, Wei Jinjin. Research on the Practical Dilemmas and Resolution Pathways of Collaborative Governance for Cross-Border Data Flow in China [J]. Modern Intelligence, 2024, 44(09): 151.

[5] Cao Pantian, Yuan Ruijing. Preventive Governance of Data Security Risks in Overseas Listings by Enterprises [J]. Hebei Academic Journal, 2023, 43(03): 209.

[6] Huang Jingwen, Tao Shigui: Financial Technology in the Digital Intelligence Era: Risks and Regulation[J]. Lanzhou Academic Journal, (2023) No.6, p.39.

[7] Jiang Liwen, Jiang Huan. Legal Challenges and Countermeasures for Cross-Border Securities Regulation in Data Security [J]. Southern Finance, 2021, (11): 84-85.

[8] Liu Yan, Ran Congjing: International Strategies for Cross-Border Supervision of Financial Data and China's Approach[J]. Financial Review, Vol 15 (2023) No.4, p.117.

[9] Di Xingsi. Fairness Advancement in AI Governance within the Financial Sector: An Approach Combining Algorithm Explainability and Collaborative Regulation [J]. Nanjing Social Sciences, 2025, (07): 86.

[10] Yang Dong, Cheng Xiangwen. Research on Consumer-Centred Open Banking Data Sharing Mechanisms [J]. Journal of Financial Regulation Research, 2019, (10): 103-104.

[11] Xu Duoqi, Dong Jiajie. Financial Enterprise Compliance Governance in China's Cross-Border Data Flow [J]. Journal of Social Sciences, Jilin University, 2024, 64(03): 45-46.

[12] Cheng Zhibo. The Essential Implications and Manifestations of Contemporary Western Technological Nationalism [J]. Studies in Science of Science, 2024, 42(03): 489.

[13] Zheng Shufeng. The Dilemmas and Responses of Cross-Border Data Rules from a Digital Economy Perspective [J]. International Trade, 2022(05):66.

[14] Cai Jiahao, Bai Chun. The International Trade Rules System in the Digital Economy: Governance Dilemmas and Evolutionary Pathways [J]. Economic System Reform, 2025(03):72.

[15] Ma Tao, Liu Bingyuan. Cross-border Data Flow, Data Element Monetisation and Global Digital Trade Governance [J]. International Economic Review, 2024(02):156.

[16] Yik-Chan Chin, Jingwu Zhao. Governing Cross-Border Data Flows: International Trade Agreements and Their Limits[J]. Laws,2022,11(4):3.

[17] Baesens B, Bapna R, Marsden J R, Vanthienen J, Zhao J L. 2016. Transformational Issues of Big Data and Analytics in Networked Business[J]. MIS Quarterly,40(4):808.

[18] Graham Greenleaf, 2019.Asia's Data Privacy Dilemmas 2014-2019: National Divergences, Cross-Border Gri-dlock[EB/OL].(2019-08-01) [2025-11-12]. http:// www. ssrn. com/ link/ UNSW-LEG. Html.