世界互联网大会 World Internet Conference

北京郵電大學 Beijing University of Posts and Telecommunications

互联网治理与法律研究中心 INSTITUTE OF INTERNET GOVERNANCE AND LAW

Outcomes of World Internet Conference
Think Tank Cooperation Program

Research Report on Cross-Border Data Flow Mechanism in the Asia-Pacific Region

Institute of Internet Governance and Law
at Beijing University of Posts and Telecommunications

APRIL 2026

世界互联网大会
World Internet Conference

北京郵電大學
Beijing University of Posts and Telecommunications

互联网治理与法律研究中心
INSTITUTE OF INTERNET GOVERNANCE AND LAW

Report Writing Group

Chair

Xie Yongjiang	Professor and Director of Institute of Internet Governance and Law at BUPT

Members

Xu Yunhong	Adjunct Researcher of Institute of Internet Governance and Law at BUPT
Pan Jing	Associate Professor of School of Humanities of BUPT
Huang Xuechen	Adjunct Researcher of Institute of Internet Governance and Law at BUPT
Huang Yawen	Research Assistant of Institute of Internet Governance and Law at BUPT
Guan Chunfeng	Research Assistant of Institute of Internet Governance and Law at BUPT
Wang Zhepeng	Research Assistant of Institute of Internet Governance and Law at BUPT
Xiang Yuyao	Research Assistant of Institute of Internet Governance and Law at BUPT
Kang Yuning	Research Assistant of Institute of Internet Governance and Law at BUPT

Contents

Summary

This report focuses on the cross-border data flow mechanism in the Asia-Pacific region, and systematically analyzes its necessity, feasibility, existing obstacles and optimization paths.

As the core driving force of the development of the global digital economy, cross-border data flow plays a key role in promoting trade growth, technological innovation and global governance. The Asia-Pacific region accounts for more than 60% of the world's GDP and have high digital trade activity in the region. Cooperation on cross-border data flows is necessary for multiple reasons, including economic and trade development, rule coordination and technological innovation, security and trust assurance, and regional strategic considerations.Similar market demands across Asia-Pacific countries and regions provide a feasible foundation for cooperation.

Through comparative research, it is found that Asia-Pacific countries show diverse characteristics in legal regulation, governance models, regulatory systems and data sovereignty strategies, forming differentiated paths such as self-discipline-led, mutual recognition of rules, and security priority. At present, cross-border data flow faces three core obstacles: lack of unified international rules and the insufficient effectiveness of existing guiding rules; the definition of privacy protection and the strictness of the institutional environment are different, and the foundation of trust is weak; industry data flow standards need to be refined urgently, and there is a gap in the supervision of non-sensitive commercial data and special industry data.

This report recommends building a coordination mechanism from three aspects: first, promote the harmonization of cross-border data laws and regulations, and unify the language of protection standards and rules; second, strengthen cross-border data supervision cooperation, improve regional cooperation and the construction of data exchanges and clearing centers; third, lead the innovation of systems and mechanisms, and balance data flow and security, technological development and sovereignty maintenance.

I. The significance of cross-border data flow in the Asia-Pacific region

1. The significance of cross-border data flow

Cross-border data flow refers to the process of transmitting, storing, and processing data between different countries or regions. Enterprises conducting cross-border business, scientific research institutions conducting international cooperation, and cloud service providers providing services to global users cannot be separated from the scope of cross-border data flow, and cross-border data flow has become a key force in promoting the process of global integration. In the business field, cross-border data flow enables enterprises to integrate global resources, enhance market competitiveness, and promote the prosperity and development of international trade. In the field of scientific research, cross-border data flow breaks geographical restrictions, promotes the sharing and integration of global scientific research resources, and accelerates the pace of scientific and technological innovation.

Cross-border data flow is of great significance. First, alleviate the pressure of data localization. Under the data localization model, enterprises often need to invest a lot of resources to establish data centers in various places to meet requirements. Cross-border data flow can break down these barriers and promote knowledge dissemination and technical cooperation on a global scale. Enterprises and research institutions in different countries and regions can more easily access, analyze and utilize data resources from around the world, accelerate the research and development process of new products and services, and enhance the innovation and competitiveness of the entire industry. Second, promote global economic growth. According to the TeleGeography database, as of September 2025, the scale of global cross-border data flow reached 1835 Tbps, an increase of 24% over the annual scale of 2024 (1479Tbps)[1]. Third, promote the realization of global governance. Cross-border data flow break through the limitations of traditional territorial sovereignty and play an important role in combating international cybercrime, addressing global climate change, and cooperative development of genetic information, and possess instrumental value for realizing the concept of a community with a shared future for mankind.

However, while cross-border data flow brings many conveniences, it also raises a series of problems that cannot be ignored. The first is data security issues, such as hacker attacks and cyber espionage in data flow, which can easily lead to the leakage of trade secrets, personal privacy, and sensitive state information. Secondly, there are significant differences in privacy protection standards and laws and regulations between different countries and regions, and enterprises are prone to compliance difficulties when transmitting data across borders. In addition, the subject, scope, and intensity of data supervision vary from country to country, resulting in many gaps and loopholes in the supervision of cross-border data.

[1]China Academy of Information and Communications Technology (CAICT):Global Digital Governance Blue Book (2025),p. 1.

2. The necessity of cross-border data flow cooperation in the Asia-Pacific region

The Asia-Pacific region, encompassing some of the world's most dynamic economies, including China and ASEAN, underscores the growing necessity for cooperation in cross-border data flow.This necessity is not only reflected in bridging institutional differences, but also in the comprehensive needs of promoting regional economic development, promoting the exchange of rules, promoting technological progress, ensuring security and trust, and enhancing regional global influence.

A. Economic and trade development needs

The rapid expansion of cross-border e-commerce, fintech and digital services directly depends on the free flow of data. If data cannot be transmitted freely and securely across borders, this growth trend will be severely restricted. Therefore, the practical needs of economic and trade development have become an important driving force for strengthening cross-border data flow cooperation in the Asia-Pacific region.Due to the highly complementary industrial chain relationships among economies in the Asia-Pacific region, a close digital trade network has been formed.Without unified rules, enterprises will face high compliance costs and weaken the advantages of regional cooperation.

B. The dual drive of rule collaboration and technological innovation

Cross-border data flow is not only an economic need, but also the result of the dual role of rules and technology. The Asia-Pacific region has various institutional arrangements for cross-border data flow, such as APEC's Internet and Digital Economy Roadmap, the Cross-Border Privacy Rules (CBPR) and the Cross-Border Privacy Enforcement Arrangement (CPEA), the Global CBPR Forum, the Trusted Data Free Flow (DFFT), and the ASEAN Digital Economy Framework Agreement (DEFA). These rules are showing a trend of alignment and mutual recognition. In summary, rule coordination provides an "institutional template" and "minimum consensus" for cross-border data flow, while technological innovations such as privacy enhancement technologies, cross-border data transmission security technologies, and end-to-end data traceability technologies transform this coordination from a principle-based approach into an operational capability. Together, these two aspects are driving substantial progress in Asia-Pacific cooperation on cross-border data flows.

C. Security and trust assurance and regional strategic considerations

In the process of promoting cooperation in cross-border data flow, security and trust guarantees have always been key issues. For the Asia-Pacific region, without a coordinated trust and security framework, digital cooperation between economies will gradually be separated by their respective regulatory barriers, and the connectivity of regional internal markets will be seriously weakened. More importantly, the global digital

governance landscape is facing the challenge of rule fragmentation and institutional competition, and major economies such as America and the European Union (EU) are strengthening the spillover effect of their own rules. If the Asia-Pacific region cannot reach a minimum consensus and coordination mechanism at the regional level, transnational companies will be forced to shuttle between multiple systems, which will not only increase the complexity and cost of compliance, but also weaken the institutional competitiveness of the region as a whole. In this context, non-binding and inclusive mechanisms in the Asia-Pacific region have become a strategic advantage, enabling soft coordination and capacity building beyond high political sensitivity, and providing a framework for security and trust for regional economies.

3. Basis of cross-border data flow cooperation in the Asia-Pacific region

The similar market demand for cross-border data flows among economies in the Asia-Pacific region has become an intrinsic driving force for cooperation. First, balance the need for data security and openness. Asia-Pacific economies generally face the dual pressures of data security and economic development, and should seek a balance between data security and openness. Second, the need for transaction trust. At present, the regulation of cross-border data flow in various economies is characterized by fragmentation and decentralization, and unified rules for cross-border data flow have not yet been formed, which is difficult to meet the growing transaction trust requirements between economies. Finally, the need for digital transformation. Cross-border data flow can bring together global data resources, provide enterprises and scientific research institutions with a broader perspective and richer materials, thereby stimulating innovative thinking. Cross-border data flow innovates and expands the form and depth of traditional trade in goods and services, develops new trade formats, and effectively promotes the transformation and innovation of the global industrial chain.

II. Comparative study on the cross-border data flow mechanism in the Asia-Pacific region

1. Legal regulation of cross-border data flow governance

The Asia-Pacific region has developed a diverse and systematic approach to the legal regulation of cross-border data flows, including the “adequacy” model, the “localization” mechanism that emphasizes data sovereignty, and numerous regional institutional innovations that adopt mixed legal systems and adapt flexibly.

America has shown significant phased evolution and institutional diversity, and its regulatory model has changed from highly market-oriented to national security-led, and the shift to "security review mechanism" for cross-border domestic data regulation in America has become increasingly obvious.

Japan's Personal Information Protection Law has the characteristics of the data governance model of America and Europe, and its unique compromise design makes Japan's Personal Information Protection

Law both systematic and operational.

Although Republic of Korea also adopts integrated legislation, its highly centralized and consistent institutional structure makes the application of law more direct and the law enforcement efficiency higher.

As one of the earliest countries in the world to establish a legal system for cross-border data flow, Australia has built a cross-border data governance framework covering three core categories: government data, personal health data and personal privacy data, providing a clear path for the compliance management of cross-border data.

There are also differences in the level of legal regulation among ASEAN economies. The Singapore government has built a relatively mature legal regulatory framework for cross-border data through a series of regulations. Malaysia is still on a relatively cautious and gradual development path in the construction of the legal system for cross-border data flow. Thailand has continuously improved its governance system for cross-border personal data flow in recent years. Indonesia has learned from the EU, Japan and Republic of Korea to establish government licensing and compliance mechanisms for cross-border data flow. Countries such as the Philippines and Vietnam have adopted the mixed law path and set up data privacy committees or cybersecurity bureaus to participate in cross-border supervision. On the whole, ASEAN countries have gradually shown a number of common trends and typical paths, generally adopting the regulatory model of "prohibition as a principle and exception as a condition", and some countries have begun to take the initiative to connect with international mechanisms.

Canada and Mexico, as members of the North American Free Trade Area (USMCA), both allow cross-border data flow in their domestic laws. Canada stipulates that equivalent protection must be ensured for data export, but does not impose mandatory localization obligations. Mexico establishes data subjects' rights and processors' obligations to support international cooperation and participate in the Organization for Economic Co-operation and Development (OECD) and APEC multilateral data governance mechanisms.

In recent years, China has gradually built a relatively systematic legal framework, covering laws and policy documents such as the Cybersecurity Law, the Personal Information Protection Law, the Data Security Law, the Regulations on Promoting and Regulating Cross-border Data Flow, the Measures for Security Assessment of Data Export, the Measures for Authentication of Personal Information Export, and the Measures for Standard Contracts for Personal Information Export. Based on the importance of the data, China has constructed a classified and graded system of rules for cross-border data flow that combines leniency and strictness.

In addition, America, Japan, South Korea, Australia, New Zealand and other countries have reached an "adequacy assessment" with the European Union on personal data protection, allowing free cross-border flow.

In summary, the legal regulation of cross-border data flow in the Asia-Pacific region presents a diverse and dynamically evolving development path.Some economies are dominated by the "principle of sufficiency", some

economies emphasize data sovereignty and localized control, and a large number of economies adopt a mixed legal model.

2. Governance model for cross-border data flow in major Asia-Pacific economies

The control measures and governance models of Asia-Pacific economies on cross-border data flow show a broad spectrum from laissez-faire to strong regulation. Focusing on the strategic deployment of "free flow of data across borders", America adopts a de-regionalization and de-localization model to strengthen institutional power output, vigorously promotes free-flow data policies through dominance, and strictly controls the export of specific types of data. China's data export management follows the principle of overall security first, and actively promotes the orderly and free flow of data in accordance with the law while effectively protecting data sovereignty and security. Japan adopts a governance model that combines "mutual recognition + corporate responsibility", emphasizing international cooperation and institutional compatibility. Republic of Korea embodies the governance idea of "strengthening compliance obligations and gradual opening-up", and the flow of personal data overseas needs to be informed and guaranteed that the recipient has sufficient protection capabilities, and requires enterprises to assume higher information protection and cross-border risk control obligations [2]. Australia and Singapore are embodied in a governance structure of "broad regulation and compliance guarantees", striking a dynamic balance between the free flow of data and the protection of privacy rights. Among ASEAN economies, Thailand, Indonesia, and Malaysia are increasingly regulating cross-border data flow. It is worth noting that Russia, India, and Vietnam all attach great importance to localized data storage.

Overall, Asia-Pacific economies can be roughly divided into six categories in terms of control measures and governance models: first, "self-disciplined", such as America and New Zealand, emphasizing corporate self-discipline and contractual mechanisms; second, "mutual recognition of rules", such as Japan, Republic of Korea, and Canada, promoting system compatibility through international rule docking and standard contracts; third, "security priority", such as China, Russia, and Vietnam, emphasizing national security priority and localized control; fourth, "hybrid collaboration", such as Singapore and Australia, taking into account regulatory frameworks and market dynamics; fifth, "transitional", such as Thailand, the Philippines, and Malaysia, with systems gradually evolving to multiple responsibility mechanisms; Sixth, the "initial type", such as Papua New Guinea, has no independent regulators.

[2] See Mohammad Nurul Rahman: Exploring Digital Trade Provisions in Regional Trade Agreements (2022), PMC, https://pmc.ncbi.nlm.nih.gov/articles/PMC9357432/.

Table 1: Types of control measures and governance models for cross-border data flow in some Asia-Pacific countries

Economy	Control measures	Main compliance paths	Localization	Types of governance models	Regulators	recognition mechanism
America	Contractual mechanism/ national security control	Self-discipline/ Third-party agreements	No	Self-disciplined	Federal Trade Commission (FTC)	EU adequacy/CBPR /USMCA
China	Security assessment	Safety assessment/ SCC/ Certification	Yes	Security priority	Cyberspace Administration of China (CAC)	No
Japan	Equivalent protection	SCC/BCRs/ Mutual recognition	No	Mutual recognition of rules	Personal Information Protection Commission (PPC)	EU adequacy/CBPR
Republic of Korea	Whitelist mechanism	SCC/ Certification	No	Mutual recognition of rules	Personal Information Protection Commission(PIPC).	EU adequacy/CBPR
Singapore	Equivalent protection	SCC/BCRs/ Certification	No	Hybrid collaboration	Personal Data Protection Commission (PDPC)	EU adequacy/CBPR
Australia	Reasonable obligations	SCC/BCRs/ Certification	No	Hybrid collaboration	Office of the Australian Information Commissioner (OAIC)	CBPR/CPRR
Canada	Reasonable guarantees	SCC/BCRs/ Certification	No	Mutual recognition of rules	Office of the Privacy Commissioner of Canada (OPC)	EU adequacy/CBPR/ USMCA
Malaysia	Full protection	SCC/BCRs/ Certification/ Whitlist	No	Transitional	Personal Data Protection Department (PDPD)	It is proposed to join CBPR.
Thailand	Full guarantee	SCC/BCRs/ Certification/ Whitlist	No	Transitional	Ministry of Digital Economy and Society (MDES)	ASEAN
Indonesia	Government license	SCC/BCRs/ Certification/ Whitlist	Yes	Security priority	Directorate General for Informatics Application Ministry of Communication and Information Technology (DGIA MCIT)	It is proposed to join CBPR.

Russia	Localization	Whitelist/ license	Yes	Security priority	Federal Service for Supervision of Communications, Information Technology and Mass Media (Roskomnadzor)	No
Vietnam	Localization+approval	Licensing mechanism	Yes	Security priority	Ministry of Public Security (MPS)	No
Mexico	Equivalent protection	SCC/BCRs/ Mutual recognition	no	mutual recognition of rules	National Institute for Transparency, Access to Information and Personal Data Protection (INAI)	USMCA/RIPD
Philippines	Equivalent protection	SCC/BCRs/ Certification	No	Transitional	National Privacy Commission (NPC)	CBPR
New Zealand	Equivalent protection	SCC/BCRs/ Certification	No	Self-disciplined	New Zealand Privacy Commissioner's Office (OPC)	EU adequacy/CPRR
Brunei	Equivalent protection	Assessment/SCC /MCC	Yes	Initial type	Authority for Infocommunications Technology Industry (AITI)	It is proposed to join CBPR.
Papua New Guinea	The legal system was just established.	To be built	No	Initial type	No independent regulator	No
Peru	Contract guarantee	SCC/BCRs/ Mutual recognition	No	Transitional	Autoridad Nacional de Protecci ó n de Datos Personales (ANPD)	RIPD
Chile	Contract guarantee	SCC/BCRs/ Mutual recognition	No	Transitional	Personal Data Protection Authority (under construction)	RIPD

3. Regulatory system and enforcement mechanism for cross-border data flow in major Asia-Pacific economies

Asia-Pacific economies show significant differences in the construction of regulatory systems, mainly in the organizational structure of regulatory agencies, the allocation of regulatory authority, the application of regulatory technical means, the inclusion mechanism of industry entities, and the dynamic adaptability of system implementation.

The cross-border data regulatory system in America reflects the typical characteristics of "decentralized supervision + industry autonomy", and the government encourages a governance ecosystem featuring the

trinity of industry, regulators, and standardization bodies. China's regulatory system for cross-border data flow emphasizes the institutional arrangement of "centralized supervision + multi-level coordination", and the regulatory framework is implemented based on a three-tier collaborative network of central, local and industry authorities. Japan's cross-border data supervision system is characterized by "independent supervision + international docking", and the Personal Information Protection Commission has set "adequacy determines system" [3]. Singapore's regulatory system reflects the compound structure of " light-touch regulation + technology empowerment + capability guidance".The Personal Data Protection Commission has established a "transparency registration system" [4] . Its model of guided regulation plus digital supervision balances efficiency and risk control. Republic of Korea's cross-border data supervision system highlights the characteristics of "centralized coordination + sub-domain management" and has the characteristics of "cross-agency collaborative supervision". Australia's cross-border data regulatory system is built on the "Information Commissioner + resilience framework".

Table 2: Comparison of regulatory systems for cross-border data flow governance in some Asia-Pacific countries

Economy	Core regulators	independent or not	Coverage of regulatory functions	Cross-border regulatory mechanisms	Technical means support
America	Federal Trade Commission (FTC)	No	Decentralization (industry decentralization)	Self-Regulatory Framework + Certification	Compliance model + industry standards
China	Cyberspace Administration of China (CAC)	No	Centralized + multi-level collaboration	Evaluation + Filing + Sandbox	Real-time audit platform, label recognition
Japan	Personal Information Protection Commission (PPC)	Yes	Unified supervision across the country	Adequacy + mutual recognition system	Registration system
Singapore	Personal Data Protection Commission (PDPC)	Yes	Unified supervision across the country	Toolbox + capacity building	Risk scoring algorithm
Republic of Korea	Personal Information Protection Commission (PIPC)	Yes	Sub-field + collaboration	Licensing + registration platform	Privacy-preserving technology platform
Australia	Office of the Australian Information Commissioner (OAIC)	Yes	Unified coordination and supervision	Reasonable Obligations + the Privacy Impact Assessment	Evaluation Center + AI Review

[3]See Personal Information Protection Commission, Japan: Guidelines on the Act on the Protection of Personal Information (APPI) (2022), https://www.ppc.go.jp/en/legal/.
[4]See Personal Data Protection Commission, Singapore: Advisory Guidelines on Key Concepts in the PDPA (2021), https://www.pdpc.gov.sg.

4. Comparison of the strategic deployment characteristics of data sovereignty in major Asia-Pacific countries

The issue of data sovereignty is the core issue of national strategic security, technological competition and global governance, and Asia-Pacific countries have shown significant diversification characteristics in the strategic deployment of data sovereignty. Cross-border data flow greatly challenge the applicability of the principle of "territorial law", so countries have tried to build a new governance order and establish the practical logic of sovereignty over their digital territories.

From the perspective of the strategic deployment of major Asia-Pacific countries, different countries and regions have adopted differentiated data sovereignty paths according to their own security concerns, industrial structure, technological autonomy and international strategic position.

Table 3:Comparison of data sovereignty strategic deployment characteristics of major Asia-Pacific countries

Economy	Strategic core goal	focus on sovereign boundaries	International expression language	Core documents
China	Equal emphasis on data security and data resource utilization	Dual-track approach to national security and data element circulation	Cyber sovereignty	Data Security Law of the People's Republic of China ,Outline of the National Informatization Development Strategy
America	Strengthening the capacity for global data acquisition	Extension of cross-border law enforcement power	Global data universal jurisdiction	CLOUD Act, National Cybersecurity Strategy
Japan	Data flow with trust promote free trade	Trust mechanism and technical specifications	DFFT	Digital Society Construction Strategy
Singapore	Digital connectivity and regulatory coordination	Multilateral trust and compliance mechanisms	DFFT+Trust Framework	Digital Economy Blueprint 2025
Australia	Data localization and national digital sovereignty	Priority of state control	Digital Sovereignty	Data and Digital Government Strategy
Canada	Protect citizens' privacy and self-regulation	Priority of privacy sovereignty	Data Protection Sovereignty	Digital Charter ,Privacy and Other Legislation Amendment Act
Republic of Korea	Strengthen the foundation of domestic data governance	Balance between security and industry	Digital Sovereignty	Digital New Deal 2.0
Mexico	Data autonomy and local economic protection	Strengthening of regional data sovereignty	Sovereign Data Strategy	National Digital Development Plan for 2022-2026

In terms of institutional construction path, the deployment of data sovereignty by various countries presents four main types: First, the integrated model of "legal system, administrative system, and industrial policy" represented by China； second, the path of "technical standards-market-oriented-extraterritorial application" represented by America; the third is the "international collaboration-governance leadership" model represented by Japan and Singapore; Fourth, the " privacy priority -state control" path represented by Canada and Australia.

Various countries have also shown significant divergence in their strategic layout of international data sovereignty.Japan, Singapore and others advocate multilateral mechanisms based on the "DFFT", focusing on strengthening cross-border cooperation agreements, data circulation arrangements, and trusted certification mechanisms.China, Russia, ASEAN and other economies prioritize data sovereignty and regional coordination, and call for the establishment of multilateral trust-building mechanisms.In addition, medium-sized economies such as Australia and Canada seek a balance between multilateral and bilateral approaches. While safeguarding their own sovereign space, they actively participate in the formulation of regional rules.

In terms of specific policy tools, the strategic deployment of data sovereignty places greater emphasis on technicality, enforceability, and dynamic adaptability.This is mainly reflected in the integrated application of data outbound filing and approval systems, national-level data certification systems, enterprise compliance governance platforms, and regulatory systems linked with national security and anti-monopoly laws.

From the perspective of fundamental strategic logic and governance philosophy, various countries generally present four types of paradigms in the strategic deployment of data sovereignty. The first is the " state sovereignty priority" type, represented by China and Russia, emphasizing national security and public interests; the second is the " personal data-centered" type, represented by Canada and Republic of Korea, emphasizing that civil rights are the core foundation of data sovereignty; the third is the "ecologically oriented co-governance" type, represented by Japan and Singapore, emphasizing the participation of multiple subjects and collaborative governance; Fourth, the " market-driven and security-balanced " type, represented by America, forms a hybrid path. Overall, the data sovereignty strategies of Asia-Pacific countries reflect diverse path choices and governance thinking. Countries are accelerating the improvement of their legislative systems, regulatory frameworks, and international cooperation mechanisms. In the future, the data sovereignty of Asia-Pacific countries will continue to undergo a complex process of transition from confrontation and competition to institutional coordination.

III. Major obstacles to cross-border data flow in the Asia-Pacific region

Compared to traditional goods and services, data, due to its intangible and high-speed nature, presents greater challenges in terms of governance complexity, sovereignty sensitivity, and technological uncertainty during cross-border flow. Despite the Asia-Pacific region’ s continued efforts to promote the establishment of cross-border data flow mechanisms, there are significant differences among countries in terms of institutional

design, regulatory priorities, and privacy standards. In the absence of mandatory and unified rules, data flow is constrained by factors such as legal heterogeneity, security barriers, and increased compliance costs.

1. The urgent need to establish unified international rules for cross-border data flow

The international community has not yet formed a unified system for the legal regulation of cross-border data flow, and countries generally face the dilemma of balancing data sovereignty, free cross-border flow, and data security. APEC has long been committed to promoting digital governance cooperation in the Asia-Pacific region, with the CBPR serving as a significant attempt at a regional data governance mechanism and considered a core component of digital rule-making. However, the CBPR lacks mandatory constraints, members have varying willingness to adopt it, and the institutional interface design is unclear, resulting in the failure to form a unified rule system that is comprehensive and effectively enforced. This has led to a large number of institutional "breakpoints" and policy "grey areas" in the practice of cross-border data flow [5].

A. Limited effectiveness of existing guidelines

Currently, APEC primarily relies on the CBPR as its basic institutional framework. However, the overall participation of member economies in the CBPR system is clearly insufficient. Since the mechanism's inception in 2013, only nine economies—America, Mexico, Japan, Canada, Singapore, Republic of Korea, Australia, Chinese Taipei, and the Philippines—have joined, with no new members added since 2021. This situation reflects significant differences within APEC regarding the adaptability and acceptance of the CBPR system. Behind this difference lies a deep-seated institutional asymmetry among member economies, resulting in extremely limited consensus building and rule diffusion effects.

The exit mechanism also reflects a loose system. While the low-threshold, unilaterally withdrawable exit mechanism reflects APEC's "non-binding cooperation" philosophy, it weakens the stability and authority of the rules. From a legal perspective, the CBPR is a "non-mandatory governance tool," its operation relying on the willingness and mutual trust of participants, rather than the uniform application and enforcement of hard law. This means that while the CBPR promotes regional data flow standardization in principle, it struggles to build a stable and unified regional data governance architecture due to differences in implementation, lack of accountability, and loose exit mechanisms.

[5] See Shi Jiaying: Latest Developments in APEC Digital Economy Cooperation and China's Participation Strategy, Northeast Asia Economic Research, Vol. 8, No. 5, 2024.

Table 4: Comparison of APEC and EU Cross-Border Flow Mechanisms

Dimension	APEC-CBPR	GDPR
Legal binding force	There is no coercion, members join voluntarily.	It has legal force and applies to all members.
Compliance objects	Enterprises are the main players, with a lack of intergovernmental coordination.	Enterprise and national institutional evaluation in parallel.
Data type applicable	Traditional personal data	Covering personal, sensitive, biometric, and AI-generated data.
Compliance path	Third-party certification, standards vary	Automatic access control after the EU assesses the "adequacy" of third countries.
Member coverage	A small number of APEC members with low participation rates	The EU has adequacy decisions with about 17 countries/regions/international organizations.

B. Difficulty in balancing data protection and free cross-border data flow

Within the APEC framework, members exhibit highly diverse political systems, regulatory philosophies, and legal traditions. Achieving efficient and reliable cross-border data flow while ensuring privacy and national security has become a core challenge in institutional design. In practice, a dual dilemma emerges: deregulation may lead to data misuse and risks, while over-protection increases corporate compliance costs and inhibits innovation and cooperation.

Different economies employ divergent strategies regarding the strength of data protection and the facilitation of data flow. One approach emphasizes market-driven growth and prioritizes free flow, such as the US's corporate-led path, encouraging compliance through contracts and industry standards. However, privacy protection relies on corporate self-discipline, potentially leading to public distrust. Another approach emphasizes national sovereignty and data security, such as Vietnam's emphasis on storing important/core data domestically and requiring approval and retention of copies for data export. A third approach attempts to establish institutional bridges, promoting multilateral mechanisms centered on DFFT. However, "mutual trust" requires transparent institutional rules and policies, and in practice, mutual recognition mechanisms are imperfect. For example, although Republic of Korea and Japan are both CBPR members, companies still need to undergo dual compliance procedures.

The lack of an effective multilateral mediation mechanism for cross-border data disputes is a key weakness. APEC has not established a systematic and enforceable data arbitration platform, and disputes often rely on bilateral consultations or local judicial processes, which are inefficient and susceptible to political interference. The existing regulatory framework struggles to establish a dynamic balance between privacy protection and free flow

of data, exacerbating institutional fragmentation and intensifying competition and distrust among economies with different paths. Unilateral measures taken by various economies for security or protectionist reasons are creating a trend of "data barriers" replacing "data channels", weakening the possibility of multilateral mutual recognition mechanisms.

2. Privacy issues in cross-border data flow become more prominent

The prominence of privacy issues and differences in institutional environments have become key obstacles to cross-border data flow in the Asia-Pacific region. Significant differences in cultural perceptions of privacy, legal traditions, and governance models among different countries make it difficult to achieve standardization, mutual recognition, interoperability, and regulatory coordination in cross-border data flow.

A. Inconsistent scope of data privacy protection

The definition of "personal information" or "personal data" in privacy protection directly determines the scope and strength of legal application. The legal definitions adopted by different countries or regions vary significantly. This difference stems from different legal traditions and political cultures, and also reflects the different emphases that countries place on digital governance goals [6] . America employs a parallel system of industry-specific and state-level laws, prioritizing market efficiency and risk control. For example, while the California Consumer Privacy Act (CCPA) is close to the GDPR, its scope of application is limited. Japan's Personal Information Protection Law has recently aligned with EU standards, strengthening regulations on anonymized information. Singapore's the Personal Data Protection Act (PDPA) has a flexible definition, relying on "reasonable presumptions" from companies. Republic of Korea has strict definitions of personal data; its 2020 "Three Data Laws" refined classification standards, enhancing the precision of its laws [7]. China's Personal Information Protection Law and related regulations emphasize personal information protection, establishing categorized and tiered rules for the cross-border flow of personal information.

These legislative differences among countries directly impact the "identification threshold" and "protection obligations" for cross-border data flow. Companies face high institutional coordination costs due to inconsistent standards, severely hindering the development of the digital economy in the Asia-Pacific region.

B. The institutional environment for cross-border data flow varies among countries

Significant differences exist among countries regarding the legal basis, regulatory pathways, and enforcement mechanisms for cross-border data flow. Japan recognizes equivalent protection in some countries through a "whitelist system", requiring recipients to sign compliance obligations. Republic of Korea has received "adequacy certification" from the EU, requiring data subjects to agree to or recipients to provide a comparable level of protection. Singapore and Australia adopt a "moderate review + corporate responsibility" model, emphasizing ex-post accountability and voluntary certification. China, on the other hand, sets out pathways for different

[6] See Graham Greenleaf: Global Data Privacy Laws 2021: Despite COVID Delays, 145 Laws Show GDPR Dominance, Privacy Laws & Business International Report, no. 169 (2021), pp. 10-13.
[7] See In Hwan Park: Korea’ s Personal Information Protection Act and Sensitive Data Categories, Asia Data Policy Review, vol. 20, no. 2 (2021), pp. 45-62.

types and quantities of personal information, including security assessments, standard contracts, protection certifications, and free flow, reflecting a data sovereignty-first logic. Most Southeast Asian countries' personal information protection systems are in their early stages of development, with insufficient legal implementation, leaving businesses facing a dilemma of "laws existing but poorly enforced".

This institutional divergence not only affects the continuity of cross-border business operations but also restricts the construction of a unified regional digital market. The deep ties between data privacy and national security and sovereignty control make countries prone to a "protectionist resurgence" in policy-making.

3. The need for detailed regulations on cross-border data flow in industries

While a general legal framework for data flow has been gradually established in Asia-Pacific countries, standards for cross-border data flow in specific industries remain incomplete or inconsistent, necessitating regional-level refinement and coordination. Significant differences in industry needs mean that the lack of classification rules based on heterogeneity leads to poor regulatory adaptability, restricting free flow from low-risk industries while failing to effectively prevent spillover from high-risk industries.

A. Standards for cross-border flow of non-sensitive business data

Non-sensitive business data (such as product specifications, supply chain information, and logistics tracking) does not involve personal identification or core corporate secrets. However, most countries have not yet established clear classification and standardization paths. Some countries, citing national security sensitivities, apply a blanket approach to all types of data, imposing stringent compliance obligations, leading to an imbalance in data classification and inefficient regulation. Some developed economies, such as America, Canada, and Australia, have clearer classifications and fewer restrictions on non-sensitive data; however, many ASEAN countries, such as Vietnam, the Philippines, and Indonesia, include operational data in their localization requirements, necessitating local storage or approval even for data not involving privacy, thus increasing the burden on SMEs.

B. Standards for data Flow in special sectors such as finance and credit reporting

In the overall structure of cross-border data flow governance, the flow of data from special sectors such as finance and credit reporting has long been a regulatory focus. This data is highly sensitive and deeply intertwined with national economic security. Most countries adopt a "local priority, cautious export" strategy, resulting in generally conservative regulation. China implements dual regulation for financial data: combining general data laws with financial industry standards, requiring local storage, categorized and graded protection, and restricting export to specific security assessment scenarios. Some countries also adopt similar localization measures,

emphasizing substantive state control over cross-border data. For credit reporting data, Republic of Korea requires strict and refined management, requiring foreign e-commerce companies to have operations in at least five countries simultaneously before storing credit card information overseas, and dynamically monitoring this. America exhibits a dual approach: encouraging free flow but imposing access restrictions on specific foreign companies through national security reviews, creating a "one-way convergence under the guise of free flow". Countries like the Philippines and Malaysia require the use of local databases, with special permits required for export. Japan emphasizes data traceability.

Currently, there are no unified rules for the financial and credit reporting industries in the Asia-Pacific region. The differences in governance models among countries stem from different understandings of data sovereignty, risk tolerance, and stages of industrial development. Finding a balance between ensuring security and promoting interconnectivity will be a long-term challenge.

IV. Recommendations for establishing a coordination mechanism for cross-border data flow in the Asia-Pacific region

1. Coordinated development of cross-border data regulations

A. Unify data protection standards and balance data protection and free flow

Due to the different perceptions and regulatory priorities of data protection among countries in the Asia-Pacific region, it is recommended that APEC construct a unified regional data protection framework from the following three aspects:

First, establish a core principles framework. Based on the nine core principles of the APEC Privacy Framework (2015 edition), refine and expand upon them:(1) Data Minimization: requiring enterprises to collect only the minimum data necessary to achieve business objectives; (2) Purpose Limitation: emphasizing that data processing must have a clear and legitimate initial purpose, and subsequent use must not deviate from that purpose; (3) Transparency: requiring enterprises to inform users of the purpose of data and disclose the processing methods, scope, and possible cross-border flow; (4) Security: proposing specific compliance requirements in conjunction with emerging technology scenarios [8] .

Based on the sensitivity and risk level of data, it is recommended that data be divided into the following four categories: (1) National Security/Critical Infrastructure Data. In principle, it should be stored locally, with strict restrictions on cross-border flow, and can only be transmitted to fulfill international obligations or achieve specific cooperative purposes, and after assessment and approval at the national level. (2) Sensitive Personal Information/Highly Sensitive Industry Data. Implement "higher standards of protection requirements" [9] , requiring prior filing or regulatory approval for data subjects to obtain explicit authorization, and may require data

[8]See Liu Xiaochun：The Principles and Analysis of the GDPR(2019), "Security Insider" website.
[9]Data Security Technology Data Classification and Grading Rules (2024).

localization. (3) General personal information. Cross-border flow can be achieved through mechanisms such as certification, standard contracts, or consent. (4) Non-sensitive commercial data/de-identified statistical data. Establish a "simplified cross-border flow mechanism", allowing enterprises to freely flow data after fulfilling basic notification obligations, or clarifying the responsibilities of the recipient through contract terms to reduce compliance costs.

Second, establish a differentiated implementation mechanism. Implement differentiated standards according to development level: developed economies can take the lead in implementing the "high standard protection + simplified approval" model and provide technical assistance to developing economies; developing economies can set up a "transition period" and "simplified requirements", and build a data center security protection system through the "Digital Silk Road" technical assistance project. Third, improve the supporting guarantee system. A multi-level support mechanism can be constructed from the following four aspects:

(1)Develop standardized compliance tools. Formulate data export conditions according to industry, provide data sensitivity assessment examples and certification auxiliary toolkits, and provide free download channels for multilingual versions.

(2)Establish a cross-border regulatory cooperation mechanism. Build a data sharing system among regulatory agencies of various countries to exchange information such as corporate compliance audit reports and data breach incidents in real time; organize relevant countries to conduct joint investigations and punishments; and establish a "Data Cross-border Flow Dispute Mediation Committee".

(3) Promote technological innovation and application. Promote technologies such as federated learning and homomorphic encryption; utilize blockchain to achieve full traceability of cross-border data flow; and develop AI-driven data compliance monitoring tools to automatically identify high-risk behaviors in corporate data processing.

(4) Establish a dynamic adjustment mechanism. Regularly publish the "Asia-Pacific Data Cross-Border Flow Implementation Assessment Report" to analyze the effectiveness of standard implementation, technological risks, and market demand; establish a rule revision procedure of "proposal– expert review – public consultation – multilateral consultation", and promptly supplement protection requirements for emerging fields.

B. Standardize rule terminology and build a mutually compatible legislative and regulatory system

Ambiguity in rule terminology is one of the obstacles to cross-border data flow. Therefore, a "Guide to Cross-border Data Governance Terminology" could be compiled, and a regulatory mutual recognition mechanism could be established [10].

(1) It is recommended to standardize the definition of core terms.

[10]See Bradford, Anu, The Brussels Effect: How the European Union Rules the World (New York, 2020; online edn, Oxford Academic, 19 Dec. 2019), https://doi.org/10.1093/oso/9780190088583.001.0001, accessed 31 July 2025.

First, a functionalist definition approach should be adopted to accurately define high-frequency concepts and provide accompanying annotations to explain their extensions. The basic obligations of data processors should be clarified around fundamental aspects such as notification of personal information collection. At the same time, countries should be allowed to make supplementary provisions on the scope and protection measures of sensitive data, but these must be made transparent . Rules that meet the core standards should be mutually recognized through an "equivalence recognition" mechanism [11].

A tiered obligation system should be established at the level of substantive rules: the first level is the "hard law" bottom line that all economies must comply with, establishing minimum standards; the second level is the "soft law" space that allows countries to supplement provisions according to their national conditions, but transparency must be ensured through mandatory information disclosure.

Furthermore, a dynamic adaptation mechanism should be embedded to achieve a balance between rule convergence and legal cultural differences through three main paths: first, establish an "equivalence determination" procedure to mutually recognize foreign rules that meet core standards; second, set up periodic review clauses to keep rules, technologies, and international standards evolving in sync; and third, design a dispute resolution mechanism to resolve differences in rule interpretation through non-confrontational methods such as negotiation and mediation. Ultimately, a balance should be sought between standardization and flexibility to promote Pareto improvement in regional data governance.

(2) It is recommended to construct scenario-based guidelines for the application of terminology and provide judgment standards for easily confused scenarios.

Based on industry characteristics, differentiated compliance paths are recommended: Sensitive industries can adopt a sovereign data sharing architecture to achieve limited cross-border flow under the premise of localized storage; for industries with significant cross-border user flow, a dynamic authorization management system should be configured to adapt to the rules of different economies based on the user's real-time location. This framework should also include a risk warning mechanism to automatically generate a compliance roadmap for enterprises expanding into new markets.

(3) It is recommended to establish a dynamic update and domestic law conversion mechanism.

First, a terminology review committee should be established to iterate the core concept dictionary annually, incorporating emerging concepts into the system, and clarify their logical relationship with existing terms through annotations.

Second, operational standardized results should be formed to provide a reference for countries to revise their domestic laws. A legislative model covering key aspects such as security assessment and cross-border flow agreements can be developed, referencing the ASEAN Model Contract for Cross-Border Data Flow [12] , and a

[11]See Cai Peiru：A Study on the Right to Protection of Personal Data under EU Law—and Its Implications for the Construction of Personal Information Rights in China(2021), Jurist.
[12]See Yang Chunbaixue：ASEAN Releases Model Contract for Cross-border Data Flow (MCC)(2021), CAICT Internet Law Research Center.

corresponding enterprise compliance toolkit should be developed. (4) Constructing a Dynamic Management System for the "Regulatory Concordance List".

This system should include three functional modules: first, a conflict identification module, which regularly scans and marks clauses that conflict with the core principles; second, a conversion tool module, which automatically generates a difference analysis report; and third, an implementation monitoring module, which tracks the adoption of the list and publishes an annual compliance white paper. An emergency response channel should also be established to activate a temporary coordination mechanism within 72 hours in the event of a major regulatory conflict.

2. Coordination and cooperation in cross-border data supervision

Currently, data regulatory cooperation among Asia-Pacific region is primarily based on bilateral agreements, lacking a multilateral coordination mechanism, which leads to frequent regulatory conflicts[13].To improve this situation, it is recommended that APEC establish a Data Regulatory Cooperation Committee, composed of representatives from the data protection agencies of each member country, to coordinate cross-border enforcement actions. This mechanism could draw on the international cooperation framework of Article 50 of the EU's GDPR, but needs to be adapted to the diversity of the Asia-Pacific region [14].

Given that the politicization of data sovereignty has exacerbated the difficulty of cross-border data flows, regional "data clearing centers" could be established. These centers would be neutral data centers set up within specific countries or regions, allowing data to be stored locally while enabling cross-border analysis through privacy-preserving computing technologies. The compliance experience of Singapore's Trusted Data Sharing Framework (TDMF) could be drawn upon, combined with the blockchain technology of the Hong Kong Big Data Exchange (HKBDE)[15] , to ensure the traceability of data flows and meet the regulatory and auditing needs of all members.

A. Improve and promote regional cooperation in cross-border data regulation

Due to the significant divergence in data storage policies across the Asia-Pacific region, this policy diversity makes it difficult for enterprises to adopt a unified storage strategy.Therefore, companies should prioritize regional adaptation, accurately matching data classification and storage locations based on the policy characteristics of the target market. Furthermore, they should strictly adhere to the principle of "destination compliance verification" during cross-border flow. This involves three levels: pre-compliance review, agreement and technical safeguards, and dynamic management during and after the flow, ensuring that the entire data flow chain complies with the legal framework of the receiving parties.

To fundamentally alleviate regulatory conflicts, establish a dedicated agency to handle functions such as sharing regulatory dynamics, joint handling of cross-border incidents, and unified interpretation of rules. Based on this,

[13]See Anupam Chander & Uyên P. Lê, Data Nationalism, 64 Emory L. J. 677 (2015).
[14]See Christopher Kuner: A Global Regulatory Framework for Transborder Data Flows, in Transborder Data Flows and Data Privacy Law (Oxford, 2013; online edn, Oxford Academic, 26 Sept. 2013), https://doi.org/10.1093/acprof:oso/9780199674619.003.0008, accessed 2 Aug. 2025.
[15]See Xu Mingyue and An Xiaomi:Case Study on Singapore’ s Trusted Data Sharing Framework from the Perspective of Collaborative Theory, Intelligence Theory and Practice, Vol. 43, No. 10, 2020, pp. 177-182.

a regulatory mutual recognition mechanism should be established to mutually recognize regulatory measures that meet the standards. In practice, regional cooperation in cross-border data regulation needs to focus on the following seven factors:

(1) Refined Cross-Cultural Design [16]. There are both cultural and legal differences among countries regarding user data protection. This requires cross-border data mechanisms to go beyond a "technical compliance" perspective and understand the impact of regional culture on user decisions. Building a multilingual information platform is a key measure to promote cross-border data supervision communication. The platform should integrate information on data protection regulations and policies, utilizing translation technology and human proofreading to ensure the accuracy of information flow. Simultaneously, the platform interface and search function should be optimized, and interactive sections should be added to encourage experience sharing. Furthermore, localized design should be adopted to address language differences in different markets.

(2) Establishing cross-border data governance ethical guidelines. The guidelines should respect the cultural differences among countries, adhering to the principles of fairness, impartiality, and transparency, and regulating the entire data lifecycle: collection should be legal and necessary, storage must be secure, flow must confirm the recipient's protection capabilities, and use should guarantee the user's right to know. At the same time, an ethical review mechanism and a cross-border committee should be established to encourage voluntary compliance by enterprises. This provides ethical support for cross-border supervision, avoiding a "uniform authorization template" and fragmenting authorization scenarios based on cultural laws.

(3) Enhancing the professional competence of the data governance team. To effectively address the cross-cultural challenges in cross-border data supervision, systematic training must be provided to the data governance team. Training content should cover cultural background knowledge and strengthen cross-cultural communication skills. In addition, by analyzing typical cases, the team's sensitivity and ability to handle practical problems can be improved. Regular expert lectures, international exchanges, and field visits can be organized to ensure that teams accurately adapt to regulatory requirements under different cultural backgrounds.

(4) Strengthen international cooperation and forum mechanisms. Actively utilize international cooperation projects and professional forums to build bridges for communication and collaboration among countries. On the one hand, establish special cooperation projects to conduct joint research and standard setting, enhancing mutual trust among countries; on the other hand, hold high-level international forums to invite various parties to conduct in-depth discussions, promoting the exchange of ideas and sharing of experiences. In addition, enterprises can establish a "dynamic authorization management system", allowing users to modify the scope of authorization at any time according to their own needs.

(5) Establish a data regulatory coordination agency. This agency should have three core functions: coordinating the regulatory policies of countries; establishing unified enforcement standards; and promoting a regulatory mutual recognition mechanism. At the implementation level, beneficial international experience can be drawn

[16] See VID Capital: Breaking Through Data Compliance in Indonesia: Legal Analysis and Security Navigation for Chinese Enterprises Going Global, WeChat Official Account "VID Capital", March 24, 2025.

upon to establish a tiered and categorized regulatory system. For basic data protection principles, promote unified standards among countries; for special areas such as sensitive data, allow countries to formulate differentiated rules on the premise of meeting basic requirements.

(6) Construct a tiered response plan for cross-border data breaches. Event classification should be guided by actual impact, taking into account not only scope and severity but also the speed of spread and social impact. It is recommended to classify events into four levels: Level 1 is a general user data leak within a single country, causing no substantial loss; Level 2 is a sensitive data leak within a single country, posing a direct risk to the enterprise or user; Level 3 is a general data anomaly across 2-3 countries, with limited impact; Level 4 is a large-scale sensitive data leak across more than 3 countries, potentially triggering a regional regulatory crisis and a collapse of public trust. Differentiated response procedures should be matched to different levels.

(7) Building an intelligent security monitoring network. The Asia-Pacific regional security monitoring network should be technology-enabled, integrating existing intelligence resources to build a dynamic protection system covering the entire data lifecycle. In terms of technical architecture, a central monitoring platform should be deployed at the Asia-Pacific headquarters, using AI algorithms to establish a data flow baseline; edge computing terminals should be set up at each country node to perform real-time encryption verification of sensitive data, triggering local alerts and synchronizing with the central platform when anomalies occur. To improve the accuracy of risk identification, a cross-border threat intelligence sharing database needs to be established to aggregate high-incidence attack cases and virus characteristics from each country. This database should be used to identify regional risk sources through correlation analysis via a central platform, and warnings should be automatically pushed to affected areas. Simultaneously, data from the regulatory sandbox should be integrated to conduct specialized monitoring of innovative businesses.

B. Actively promote the construction of international data exchanges and data clearing centers

In the context of digital economic globalization, the scale of data flow in the Asia-Pacific region continues to expand, but it faces challenges such as ambiguous data ownership and differences in national standards, necessitating the construction of a standardized flow system. The core of this system is to achieve standardized transactions through regional data exchanges and ensure flow security through third-party data clearing centers, forming a full-chain governance mechanism of "transaction-processing-flow". Transactions require the formulation of unified rules, clarifying data ownership and pricing mechanisms, while introducing smart contract technology to automatically execute agreements on the scope and duration of data use.

Before cross-border data flow, it must be de-identified by an independent clearing center. This center can draw on the "data trust" model to anonymize sensitive information such as medical and financial data. The clearing center must be subject to joint supervision by various countries and work in conjunction with exchanges to guide enterprises in secondary processing of non-compliant data, ultimately issuing a "compliance certificate" containing processing information to shorten the approval cycle.

3. The formation of institutional and mechanism-led models to promote cross-border data flow

The Asia-Pacific region needs to start from both top-level institutional design and technological governance coordination to form a three-in-one model of "rules-technology-cooperation".

A. Institutional guidance balancing data flow and security

The institutional design for cross-border data flow needs to strike a balance between "free flow" and "secure controllability". This can be achieved by constructing a system that emphasizes both tiered and categorized management and compliance incentives and constraints, providing stable expectations for cross-border data flow.

Tiered and categorized management is the core of the institutional design. For highly sensitive data, a strict security assessment and approval mechanism should be established, implementing the principle of "domestic storage + authorized access". For general commercial data, a filing system should be adopted, allowing free flow to reduce enterprise costs.

Compliance incentive and constraint mechanisms are crucial for the implementation of the system. On the one hand, a "whitelist" system should provide policy preferences to incentivize enterprises to improve their compliance capabilities; on the other hand, penalties for violations should be strengthened. Simultaneously, the institutional design needs to proactively align with international rules and establish a dynamic adjustment mechanism to respond to changes in technology and the international situation.

For special scenarios such as cross-border e-commerce and telemedicine, rule innovation is necessary. For example, "data anonymization + blockchain evidence storage" can meet the regulatory requirements of cross-border e-commerce, or "end-to-end encryption + hierarchical access control" can ensure the secure flow of telemedicine data.

B. A governance mechanism that promotes technological development and sovereignty protection

Technological progress is the core driving force behind cross-border data flow, but it can also exacerbate data sovereignty conflicts. A collaborative mechanism of "technology empowerment + sovereignty protection" needs to be built: on the one hand, reducing security risks through privacy-enhancing technologies; on the other hand, maintaining digital sovereignty equality through multilateral cooperation platforms.

Privacy-enhancing technologies are key tools for achieving "data usable but not visible". Federated learning allows parties to jointly train AI models without transmitting raw data, such as sharing gradient parameters instead of patient records in cross-border medical research [17]; homomorphic encryption supports computation

[17] See Liu Yixuan, Chen Hong, Liu Yuhan, and Li Cuiping: Privacy Protection Technology in Federated Learning, Journal of Software, Vol. 33, No. 3, 2022, pp. 1057-1092.

on encrypted data, allowing companies to only obtain aggregated results without decrypting details. The widespread adoption of these technologies requires supporting standards and certifications, including issuing certificates for relevant technologies and clearly defining application parameters.Multilateral technology cooperation platforms are important carriers for maintaining digital sovereignty. APEC can build regional technology sharing platforms, open up open-source resources such as privacy computing toolkits, and avoid technological monopolies. At the same time, a risk assessment mechanism needs to be established to jointly evaluate emerging technologies, formulate application red lines, and prevent technological hegemony from eroding sovereignty.

Dynamic adaptation of technology governance rules is the guarantee for the sustainable operation of the mechanism. A closed loop of "technology monitoring - rule iteration" should be established, relying on research institutions to issue risk warnings and using "regulatory sandboxes" to test new rules in specific regions, ensuring that governance keeps pace with cutting-edge technologies.