Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Governance of Cross-border Data Flow in China under the DEPA Framework: Challenges and Strategies

Yuanhong Shi

suise0101@163.com

China University of Political Science and Law

Jielun Lu

China University of Political Science and Law

Article

Keywords: DEPA, cross-border data flow, data governance, China countermeasures

Posted Date: September 9th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-10410487/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Abstract

Cross-border data flows is now a major problem that influences the political, economic, and social progress of nations all over the world. Due to the disparity in the level of development, regulatory strategies, and national interests of countries and regions, a globally integrated system of data regulation has not been developed. The Digital Economy Partnership Agreement (DEPA) in this context presents a novel method of data governance on a global scale. As the first global digital trade agreement, DEPA presents new and transparent regulations on the Cross-border data flows, which are based on the latest international standards and demands to provide the free movement of data across the borders. China is actively preparing to become a member of DEPA, but there is still a distance between its current regulatory framework of Cross-border data flows and the high-standard requirements of the agreement. China is still navigating complex regulatory issues in Cross-border data transfers, such as balancing data sovereignty issues, harmonizing domestic laws with those of DEPA, improving data review processes, and increasing regulatory and supervisory capacity. Thus, the application to join DEPA should be used as an opportunity to clarify the issues concerning the ownership and governance of data, enhance the successful alignment of the domestic data flow regulations with the DEPA rules, advance its data security management system, and actively create a more open, transparent, and efficient data governance system. This way, China will be able to make significant contributions to the global data governance development and share valuable insights and experience.

1. Introduction

In the current digital economy era, cross-border data flows have become a central issue in international trade and the advancement of digital economies. As the first international framework dedicated exclusively to the digital economy and digital trade, the Digital Economy Partnership Agreement (DEPA) introduces a novel approach to data governance and cross-border data regulation, distinguished by its forward-looking and flexible provisions. In November 2021, China formally submitted its application to accede to DEPA, signaling its intention to harness the opportunities arising from the rapid expansion of digital trade and the digital economy. With respect to cross-border data flow rules, DEPA exhibits several distinctive features that differentiate it from other digital economy and trade pacts. Its regulatory structure aligns more closely with the evolving needs of the digital economy and broadly resonates with China's aspirations to facilitate cross-border data movement and promote digital trade (Liu and Song 2023). In this context, China's bid to join DEPA presents a valuable chance to reassess and refine its current cross-border data governance system. Accordingly, this paper will examine relevant issues in cross-border data governance, while addressing the dual objectives of ensuring data security and fostering digital economic growth.

2. Current Status of International Governance of Cross-border data flows under the DEPA Framework

Against the backdrop of the WTO's multilateral rule-making on Cross-border data flows being stalled and failing to meet the development needs of digital trade, the United States (US) and the European Union (EU), as major participants in global digital trade, are attempting to elevate their respective regional legislative proposals for digital trade development into international standards(Qi 2025). Countries are engaged in intense competition over how to construct governance rules for Cross-border data flows. The launch of DEPA, however, provides a "new path" for bridging differences in digital governance rules, and also offers new opportunities for China's digital economic development and digital governance.

2.1 The Current Status of International Governance on Cross-border data Flow

At present, international governance of cross-border data flows remains fragmented, with multiple regulatory regimes operating side by side (Zhang and Gao 2025). The rapid growth of the digital economy has significantly accelerated both the scale and scope of such data flows. Due to their comparatively brief history of development and enormous size, the management of such flows is confronted with a variety of new challenges and more complicated regulatory landscapes. As a result, nations and areas that have had a long history of digital economic development have been better placed to develop effective governance structures, which have led to the disintegration of the global governance environment (Shi 2025). Moreover, the national priorities in terms of safeguarding the interests of the digital industry, the differences in regulatory goals and supervisory practices have resulted in the emergence of different governance frameworks, which have in turn become different regulatory systems (Xu et al. 2024). On the national and regional level, these strategies can be broadly divided into the following three models of Cross-border data flow regulation.

Firstly, the "American model" advocates the free flow of data. The US has long adhered to a free-trade approach that gives commercial gains priority over privacy protections (Chin and Zhao 2022). Existing U.S. laws and policies concerning cross-border data transfers are primarily designed to protect the commercial interests of digital-industry enterprises, thereby fostering the growth of the digital economy. While the regulatory landscape spans a broad range of industries and governmental bodies, enforcement standards vary considerably across different sectors and data categories, and no unified and extensive legislation has been developed so far. The US takes a two-pronged approach to ensure the competitive edge and international leadership of its multinational digital businesses. On the one hand, it puts strict restrictions on some types of data exported to foreign countries and on particular users of exported data. Conversely, it proactively facilitates the establishment of a more open, secure, reliable and liberalized digital trade environment, thus facilitating increased participation and benefits in international digital trade.

Second, the "European model" places greater emphasis on safeguarding privacy and personal information. The EU's current legal regime governing cross-border data transfers is primarily oriented toward the protection of individual entitlements and state security, with consumer welfare receiving particular attention. Centered around the General Data Protection Regulation (GDPR), the EU has

established a coherent institutional framework for managing transborder data flows, which enables the coordination and consolidation of supervisory measures. As noted by Voss (2022), scholarly discussion has largely concentrated on the intricate nature of this regime and the far-reaching implications of the GDPR as a landmark piece of EU data protection legislation. In response to the growing dominance of large foreign digital enterprises, the EU has been striving to nurture its own digital sectors and reinforce its digital autonomy. Through a robust regulatory apparatus, the EU seeks to ensure the integrity of data privacy and security while fostering the steady growth of its homegrown digital economy.

Thirdly, the “Chinese model” aims at a compromise between facilitating the data flows and protecting the security interests. In contrast to the governance models that the US and the EU have implemented, China prioritizes national security as the core of its regulatory framework and at the same time encourages the growth of digital trade and data flow (Jiang 2024). Its domestic regulatory system is a mix of laws, administrative regulations, and behavioral norms that support and supplement each other, creating a relatively complete system of governance. As the digital technological innovation rapidly develop, the competitiveness of China in the global digital environment has become more noticeable. To unify these benefits and to contribute to the further improvement of the high-quality development of domestic industries, China has enhanced its internal regulatory framework and actively encourages the internationalization of its standards. This strategy seeks to foster the expansion of digital economies, protect national security and increase the control over data sovereignty.

2.2. China promotes the process of joining DEPA

With the ongoing globalization of the digital economy, profound changes in the digital trade landscape have generated new demands for international governance. To counter these developments, Singapore, New Zealand and Chile have collectively come up with the DEPA which has gained a lot of interest among nations worldwide. South Korea officially became a member of DEPA in May 2024, with the US and other countries also showing interest in joining the agreement. In November 2021, China officially requested to become a member of DEPA (National Development and Reform Commission of the People’s Republic of China 2026). In August 2022, it formed a special working group to further its accession process, and to support negotiations with current members. After the initiation of the accession negotiations, China has been actively promoting the process and has been actively involved in the discussions with the parties of DEPA. At present, the negotiations have entered a critical stage. In April 2026, during the 10th Chief Negotiators Meeting of the DEPA Accession Working Group, which took place in Seoul, South Korea, China engaged in a thorough consultation with the DEPA members, such as Chile, New Zealand, Singapore, and South Korea, on the progress of the negotiations and the issues (China News Service 2026). Later, during the ministerial meeting between China and the members of the DEPA in May 2026, the parties further deliberated on the remaining issues in the negotiations. DEPA members welcomed the positive involvement of China and asked their respective negotiating teams to speed up the negotiation process and strive to ensure that the accession negotiations of China are completed in time.

Overall, China's accession to DEPA signals a shift toward a more proactive stance in shaping international rules in key areas such as cross-border data flows and digital commerce. This move carries significant weight in enhancing China's standing and influence within the global digital economy and trade architecture, while simultaneously contributing to the establishment of a more transparent, equitable, and inclusive international environment for digital trade.

3. Characteristics and Comparative Analysis of Cross-border Data Flow Governance under the DEPA Framework

To date, a comprehensive and globally unified governance regime for cross-border data transfers remains absent. Existing rules and norms in this domain are largely dispersed across a range of multilateral and bilateral free trade pacts. As the inaugural multilateral instrument devoted exclusively to digital trade, DEPA introduces innovative approaches to the regulation of transborder data movement and digital commerce. These features leave considerable policy space for China to arrange its legal and regulatory frameworks in emerging digital sectors.

3.1. Characteristics of Cross-border data Flow under the DEPA Framework

The world first multilateral trade agreement that is specifically focused on digital trade governance is the DEPA, which was signed on June 12, 2020. The agreement consists of 16 modules on different aspects of digital trade, with multiple links and stakeholders involved besides definitional provisions (Shi 2025). Modules 2, 4, and 8 are the most pertinent to the regulation of cross-border data transfers, and they respectively cover provisions related to online trade, data protection in data flows, and enabling technologies of the digital areas.

DEPA relies on the applicable provisions of the e-commerce chapter of the CPTPP and follows a modular design (Qi 2025). Regarding trade facilitation, the DEPA framework obliges members to promptly issue applicable laws and regulations on electronic payments and to conform to internationally accepted electronic payment standards, thus minimizing trade barriers as much as possible and creating a level playing field. In terms of data-related concerns, DEPA acknowledges the set standards of personal data protection and electronic cross-border data transfers through electronic means, which enables enterprises that comply with them to send data without any issues and guarantee the compliance with the relevant legal and regulatory standards. Simultaneously, members are supposed to maintain their current CPTPP obligations and open borders to the free movement of data. Regarding the emerging technologies, DEPA focuses on the fact that artificial intelligence must be transparent, fair, and explainable and must comply with human-centered values. It also promotes the harmonization of AI governance systems between the contracting parties on the international level, which fosters the responsible deployment and utilization of AI technologies across different jurisdictions.

3.2. Comparison of Cross-border data Flow Rules between DEPA, CPTPP and RCEP

(1) Comparison between DEPA and CPTPP. The Comprehensive and Progressive Agreement on Trans-Pacific Partnership (CPTPP) represents a high-standard free trade arrangement among eleven Asia-Pacific nations (Ma and Kang 2025).Provisions concerning digital commerce are predominantly contained in Chapter,which lays down rules on transborder data movement. Regarding obligations, the CPTPP endorses the principle of free movement of data, including personal information, but it allows restrictions in the name of valid public policy goals. These obligations are also limited by the timetables of non-conforming measures in other chapters. In addition, exceptions based on legitimate public policy objectives must satisfy a “non-discrimination and necessity” test to prevent their abuse.

DEPA has stricter and more detailed requirements on data flows than the CPTPP. With regard to data liberalization, DEPA provides fewer exceptions and adopts higher regulatory standards. It also goes further to limit the localization of data and provides that any restrictive measures must be reasonable, non-discriminatory and not disguised restrictions on trade. In this regard, DEPA provisions are more detailed, especially regarding the gathering and utilization of personal data. In general, DEPA provides a more rigid and comprehensive framework than the CPTPP that minimizes implicit barriers to digital trade.

(2) Comparison between DEPA and RCEP. The Regional Comprehensive Economic Partnership (RCEP) represents a free trade agreement involving all ten ASEAN member and five external partners, such as China, Japan, and South Korea(Shi 2023). Its provisions regarding transborder data movement are largely contained in Chap. 12, especially Articles 14 and 15. RCEP provides the free-flow principle for data and forbids data localization, but it does not forbid the contracting parties to take actions that are not in line with these principles to pursue legitimate public policy goals or safeguard vital security interests. Moreover, RCEP offers two-tier exception mechanism to these obligations. Its security exception is mostly left to the discretion of the implementing party to determine the necessity and scope, and has little scope to be reviewed or challenged by other parties.

DEPA has more stringent exception requirements and emphasizes more on data flow governance and interoperability than RCEP. It also introduces the Data Protection Trustmark (DPTM) framework to strengthen data protection and enhance mutual recognition mechanisms. Regarding technological innovation, DEPA embraces regulatory sandboxes and data-sharing systems to promote innovation and experimentation, but RCEP offers comparatively little explicit guidance and institutional support in this respect.

(3) China’s participation in the “new” digital trade rule DEPA. China officially applied to join the Singapore-led DEPA on November 1, 2021. The new digital trade rules proposed by DEPA are very innovative and deal with new challenges like digital identity and industry standard-setting in new technologies and emphasize more on the development and collaboration of small and medium-sized enterprises (SMEs)

than RCEP, CPTPP, and the Japan-EU Economic Partnership Agreement (Zhou and Yu 2022). For example, DEPA advocates the establishment of interoperable and interconnected electronic payment systems[1]. It obliges members to embrace applicable international standards, guidelines or recommendations in developing electronic invoicing measures[2]. It is also the first to establish regulations on digital identity, financial technology, and artificial intelligence governance[3]. Moreover, regarding data innovation and sharing, DEPA presents new sophisticated systems, including regulatory sandboxes and government data openness systems[4]. Here, China must take an open and learning attitude towards DEPA, actively enhancing exchanges and cooperation with its members on the basis of current domestic practice, and selectively absorbing the experience of advanced regulation.

Article 4.3.2 of DEPA clearly states that personal data is contained in information sent through electronic means as compared to RCEP. It eliminates the so-called essential security exception of RCEP and puts more stress on restrictive measures that are reasonable in the context of the legitimate public policy goals. Moreover, DEPA also enhances the principle of non-mandatory data localization and explicitly demands the non-discriminatory treatment of digital products. In the case of China, besides the introduction of a tiered data protection system, domestic laws and regulations regarding the mandatory data localization should be reviewed and aligned, as much as possible, with international requirements in accordance with the national circumstances. Data jurisdiction also needs to be clarified to minimize possible regulatory conflicts. Concerning the non-discrimination principle applied to digital products, China must evaluate the possible effects on its domestic market of digital products after the liberalization of the market. Since DEPA now has a small number of member states, a gradual and staged liberalization strategy can also be taken into account (see Table 1).

Table 1
Comparison of Rules on Cross-border data Flows among DEPA, CPTPP, RCEP

Key Provisions	DEPA	CPTPP	RCEP
Elimination of Customs Duties on Digital Products and Electronic Transactions	Yes	Yes	Yes
Non-Discriminatory Treatment of Digital Products	Not explicitly stipulated	Yes	Not explicitly stipulated
Electronic Authentication and Signatures	Yes	Yes	Yes
Paperless Trading	Yes	Yes	Yes
Domestic Electronic Transaction Framework	Yes	Yes	Yes
Online Consumer Protection	Yes	Yes	Yes
Personal Information Protection	Yes	Yes	Yes, but only a principled provision
Measures against Unsolicited Commercial Electronic Messages (SPAM)	Yes	Yes	Yes
Cybersecurity	Yes	Yes	Yes, as a cooperation framework
Cross-Border Transfer of Information	Yes, permitted in principle, with encouragement of interoperability	Yes, cross-border transfer is permitted, subject to legitimate public policy exceptions	Yes, cross-border transfer is permitted, with considerable room for exceptions
Prohibition of Data Localization	Prohibited, with encouragement of interoperability of data storage and processing models	Prohibited, but subject to exceptions for legitimate public policy objectives and regulatory review	Yes, localization is not required in principle, but members may adopt restrictive measures for "legitimate public policy" purposes
Cross-Border Transfer of Information by Electronic Means and Prohibition of Data Localization in Financial Services	Yes	Yes	No

Key Provisions	DEPA	CPTPP	RCEP
Liability of Intermediary Service Providers	Yes	No	No
Confidentiality of Software Source Code and Algorithms	Yes	No, but trade secrets are protected under the Intellectual Property chapter	No
Open Government Data	Yes	No	No

4. Practical Challenges to China's Digital Governance Posed by Joining the DEPA

Currently, China is actively seeking accession to DEPA, signaling its commitment to harmonizing with high-caliber international rules on transborder data flows and presenting a favorable window for progress. That said, it is worth recognizing that China's participation and influence in the global governance of digital trade and the digital economy are still inadequate relative to the sheer scope of its digital market. As it advances along the path of digital governance reform, China must also brace itself for a series of potential risks and challenges.

4.1. Issues of Data Sovereignty

At its core, data sovereignty refers to a state’s authority over data within its territorial jurisdiction. This concept not only serves as a rationale for imposing statutory restrictions on cross-border data transfers on national security grounds, but also raises the broader question of how to strike a proper balance between the dual objectives of openness and data security in the realm of data governance.According to some scholars, the idea of data sovereignty can be perceived in two dimensions. Domestically, it is the most powerful exclusivity of data created by domestic players. Externally, it means the independence of a state in the development of data policies and involvement in the global data governance (Wang and Chen 2022). Data sovereignty is legally founded on the principle of state sovereignty. Nevertheless, in the system of governance of the global digital market and trade regulations, the conflicts between data sovereignty and free movement of data across borders have become even more acute. There are major disparities in national standards of data use and protection, which has resulted in numerous clashes between data sovereignty and territorial jurisdiction of data in cross-border situations. As an example, in the case of Schrems II in 2020, the Court of Justice of the EU struck down the Privacy Shield agreement between the US and the EU (Ulu 2026). The judgment further underscored that the legal regime of the recipient country must be assessed on an individual basis, even when standard contractual clauses (SCCs) are employed. Specifically, the U.S. CLOUD Act,which authorizes US authorities to access data held overseas—a provision deemed potentially detrimental to EU data sovereignty. The case demonstrates that when a state implements data restriction policies under the banner of national sovereignty, these policies can be questioned by other contracting parties as being inconsistent with

international commitments, thus creating more fundamental structural tensions over data sovereignty in international governance.

Moreover, the underlying consequences of the data sovereignty conflicts cannot be ignored(D'Hauwers et al. 2025). In case the data sovereignty measures of China are considered to be inconsistent with the requirements of DEPA in the framework of Cross-border data flows, member states can refer to the international rules of dispute settlement mechanisms. This may have a negative effect on international arbitration and may add to the compliance cost of the enterprises that are subject to more than one regulatory regime. That is, the cross-border enterprises might be obliged to meet the standards of the domestic regulatory review and the requirements of the free flow of the Cross-border data at the same time as the requirements of DEPA.

4.2. Compatibility between Domestic Cross-border data Flow and International Rules

The domestic legal system is an essential basis of a country to be involved in the development and application of international norms. In an era of digital globalization, the relevance of China's regulatory and policy framework with respect to cross-border data flows is steadily increasing (Zhang and Gao 2025). Nevertheless, currently, the domestic laws of China are not entirely up to the high-standard standards of international regulations regarding data flows and digital trade, and some discrepancies still exist between China and DEPA regulations in certain aspects. As an example, Article 4.3(3) of DEPA provides that any restrictions imposed on transborder data transfers must be grounded in the principle of legitimate public policy objectives[5]. It means that these measures should be legal and should be based on the considerations of the public interest, which will guarantee their need and reasonableness. Nevertheless, the internationally accepted definition of legitimate public policy objectives does not exist at the moment (Shi 2025). When applying this provision in future, China will have a lot of difficulties in proving its case in the elaborate legal and policy talks with the developed economies like the US and the EU.

Moreover, there are variations in data localization needs. Institutional differences between the current legal standards of China in determining exceptions in data localization and the corresponding provisions in the DEPA framework are significant. In particular, the main idea of DEPA is to facilitate and encourage the Cross-border data flows and, in theory, forbids the localization of data as a condition of data processing or storage in a foreign country. In comparison, the laws of China are more focused on data security (Guo and Wang 2026). Article 24 of China's Data Security Law stipulates that critical data associated with economic development, national security, and public interests must be stored within the territory of China. In cases where such data needs to be given abroad under special conditions, stringent security evaluation measures should be undertaken[6]. The legislative purpose of this provision is to protect the main national interests against possible threats. In comparison with the relatively high-level approach of DEPA to Cross-border data flows and more lenient regulatory position, domestic laws are more demanding and restrictive in terms of data flow regulation and localization (Huo 2024). With the

possible future inclusion of China in DEPA, it will be necessary to further rationalize its institutional and policy arrangements so as to strike an appropriate balance between the unimpeded movement of cross-border data and the safeguards for security, while ensuring that national data security interests remain uncompromised.

4.3. Data Review and Data Regulatory Capabilities Still Need to Be Strengthened

Regarding the data review mechanisms, despite the establishment of the legal framework of data export security review by the foundational laws, including the Cybersecurity Law, the Data Security Law, and the Personal Information Protection Law, China has not yet created a unified, comprehensive, and standardized operational framework. Such a framework would have to explicitly specify the scope of review, the content of assessments, and the review methodologies to be used (Guo and Li 2025). As a result, differences in interpretation and enforcement persist across regions and industry sectors in practice, which weakens the predictability and consistency of the data review system (Ma et al. 2026). As an illustration, the security evaluation system of important data under the Data Security Law has not been consistently applied to various areas. This has resulted in the absence of clear and binding implementation guidelines on important issues like what is considered important data, how the assessment is to be done and who is to review (Ma and Wu 2026). Thus, the creation of a hierarchical, categorized, and dynamically adjusted data security assessment system has become an urgent task to be promoted. This kind of system is necessary to enhance data governance capacity and minimize institutional ambiguity.

Moreover, the ability of China to supervise Cross-border data is still in its infancy, and there is still a gap between the current technical capabilities, including data traceability, risk monitoring, and abnormal flow early warning, and regulatory requirements suggested by DEPA. On the one hand, over-regulation can make Chinese digital businesses lose the benefits of efficient data factor mobility in international competition, and thus slow down the internationalization of the digital industry(Liu et al. 2026). Conversely, a lack of regulation or technical protection can lead to more vulnerabilities in Cross-border data transfers, and it is challenging to adequately monitor key national strategic data and mass personal data. DEPA creates a well-tuned balance mechanism to regulate the Cross-border data flows in the digital age. Its institutional structure does not only respect the regulatory sovereignty of member states but also sets legal limits to digital trade liberalization (Yu and Wang 2025). It is against this background that China ought to appropriately balance the connection between facilitating data mobility and preventing risks, and continuously improve its data governance abilities. This is essential not merely for safeguarding fundamental data security, but also for determining whether China can assume a more prominent position in global digital governance.

4.4. Emerging Technological Issues in the Field of Digital Governance

Chapter 8 of DEPA, Emerging Technology Trends, is dedicated to such issues as artificial intelligence(AI) ethics and financial technology coordination. Its focus on the interpretability and the human-centered principle is very much aligned with the legislative trend of the Interim Measures of the Management of Generative Artificial Intelligence Services in China[7]. DEPA has worked hard in the area of digital economic governance to facilitate institutional innovation, such as personal data protection systems and regulatory sandbox systems. Its essence is to create compliance channels in a risk-managed environment, thus facilitating the secure and well-ordered management of transborder data transfers (Zhou 2025). Nevertheless, the emergence of new technologies has also brought a set of new governance issues. Although China is highly concerned with data security and risk management, the emergence of new technologies also needs to be regulated prudently, as well as innovation should be encouraged. According to Article 8.2 of DEPA, the use of artificial intelligence in social and economic activities is becoming more and more widespread[8]. It also highlights the fact that AI systems must be ethical and must be created and implemented based on the principles of fairness, transparency, and accountability.Some scholars have pointed out that AI’s rapid advancement is profoundly influencing global governance over cross-border data flows, a topic of widespread international concern (Xu et al. 2025). To conclude, DEPA is a new trend in digital governance, and the corresponding legislation in China has also left institutional space to the development of new digital technologies.

5. Strategies for China's Cross-border data Flow Regulation under the DEPA Framework

A scholar has pointed out that effective global governance of transborder data flows hinges upon a clear understanding of their principal characteristics and upon China's capacity to play a formative role in rule development (Ma 2026). In the DEPA context, China must manage the pressures of international regulatory rivalry, while also devoting sustained efforts to upgrading its domestic institutional capacity, thus ensuring robust support for the enduring prosperity and high-quality evolution of its digital economy.

5.1. Data confirmation

When data move across national borders, the issue of rights verification cannot be overlooked. Some scholars have pointed out that the precise identification of data proprietors and their statutory benefits during the entire process of data element transactions, in tandem with the establishment of a comprehensive rights protection mechanism, is indispensable for ensuring both the security and the efficiency of data circulation (Zhao et al. 2025). Currently, China is experiencing a phase of increased digital transformation, whereby the societal awareness of data is still growing with digitalization. The ambiguous definition of data ownership has been one of the major issues that have emerged as a major challenge that needs to be tackled in this transformation process (Shi 2025). To this end, data rights confirmation should adhere to three basic principles: balancing development and standardization, maintaining a bottom-line regulatory approach, and implementing classification-based governance.

There are three dimensions of specific measures that can be taken. On the legal front, a system of classified data governance must be adopted and a basic data management system must be introduced to postpone the complex ownership issues and provide users with more control over the rights to use data. On the regulatory level, corporate data processing transparency should be increased, monopolistic data concentration by platform enterprises should be avoided, and a data black box approach may be considered to allow data sharing between enterprises and government authorities, which will gradually enhance the institutional framework of data rights in practice. At the technical level, it is possible to use key technologies like blockchain, as well as other data security and sharing technologies, to facilitate data rights generation, valuation, and asset allocation mechanisms. With these integrated legal, regulatory, and technical strategies, one can achieve a more balanced set of interests of all stakeholders, encourage a win-win situation between data rights protection and data value creation, and address the underlying issues related to data rights confirmation.

5.2. Promoting Effective Alignment between Domestic Data Flow Regulations and DEPA

To be more consistent with the DEPA, a high-quality international digital trade agreement, and to prevent the institutional fragmentation between domestic and international governance norms, China should actively think about the systematic compatibility and further integration of its domestic digital governance framework with the rules of DEPA, without infringing the various value preferences and differentiated development interests of all parties (Chen 2024). The exception of legitimate public policy objectives under DEPA is not clearly stated and this ambiguity can result in possible conflicts of rules (Huang and Lei 2022). It is against this background that China ought to follow a principle of balancing security and openness in dealing with DEPA rules in order to achieve successful institutional alignment. There are three dimensions in which this process can be developed. First, regulatory transparency must be enhanced and a standardized information-sharing and consultation system must be put in place. In the process of introducing or modifying regulatory measures like data localization, data processing, and data circulation requirements, all contracting parties must follow the principles of transparency strictly, meet the requirements of timely notification, and actively disclose the information related to it, including the legal basis, policy reasons, and scope of application of localization measures, which will ensure that the relevant parties can comprehend and comply with such measures in a timely manner (Pogoretskyy and Riaz 2025). This would assist in alleviating compliance frictions that are brought about by information asymmetry. Second, collaboration in data protection standards and data localization needs must be enhanced. The mechanisms of multilateral consultation and dialogue should be employed to promote more harmonisation of domestic legal frameworks of contracting parties with the basic principles of data governance under DEPA. This includes establishing an agreement on key institutional elements such as data classification, tiered governance and security protection requirements. Compliance costs can be reduced and a more inclusive and coordinated governance network can be established through mutual recognition mechanisms and coordinated lists of technical standards. Third, the relevant limits between the DEPA rules and domestic legal systems need to be clarified, and conflict of law resolution mechanisms need to be streamlined. The parties to the contract can specify the legal

relevance of the rules on data localization and Cross-border data flows by means of additional agreements or memoranda of understanding. When domestic data security requirements are stricter than DEPA standards, domestic law should prevail to safeguard baseline sovereign security. On the other hand, in the case where the data flows do not involve fundamental security issues and are in line with the provisions of the DEPA, the DEPA framework can be applied to provide uniformity in the application of rules across borders.

5.3. Further Improving the Domestic Data Security Management Mechanism

The overall development of China's digital trade is progressing rapidly. Digital content and data services exports are growing rapidly, the active promotion of cloud services abroad is being pursued, and cross-border e-commerce services show high growth prospects(Jiang 2024). In this context, it is crucial to plan strategically in advance, accurately define China's positioning, fully leverage the roles of government, industry associations, and enterprises, and promote the all-round development of digital trade. China needs to embrace a general principle that balances data security and free flow of Cross-border data, and implement a pilot-based data security governance system. By so doing, it will be able to accumulate institutional benefits in information security and effective global connectivity. On the one hand, efforts should focus on proactively exploring domestic and international digital economy and trade markets, while supporting digital trade enterprises in deeply participating in infrastructure development such as data centers and cloud service interconnection networks in ASEAN countries and regions along the Belt and Road Initiative. The focus should be on cross-border e-commerce and other areas, and the strategy of going global of digital trade enterprises should be further applied. Conversely, China must be proactive in complying with the most recent DEPA regulations in the fields of cross-border e-commerce and electronic payments, and constantly consider international collaboration in data interoperability, regulatory framework mutual recognition, and service sharing. Simultaneously, the studies on the data rights confirmation mechanisms need to be reinforced to facilitate more efficient involvement in the global digital governance.

5.4. Actively Exploring an Open and Transparent Data Governance Regulatory System

China must take advantage of its digital economy and digital trade to actively consider the creation of an open and transparent data governance regulatory framework. On the one hand, China can use the institutional benefits of Pilot Free Trade Zones and Hainan Free Trade Port to test and experiment with data governance systems (Ma and Hu 2025). As an illustration, based on the Shanghai Lingang New Area, it can consider low-risk Cross-border data flow models and build offshore data center infrastructure. With its position as a special economic zone, Hainan is able to establish a Cross-border data security oversight framework and facilitate the creation of a national digital free trade port. The other Pilot Free Trade Zones are to enhance coordination, pilot programs on safe Cross-border data transmission, and increase the influence of China in the global digital economy and trade governance.

Conversely, to address the new challenges in digital governance, China must embrace the concept of dynamic balance as the guiding principle and enhance a multi-stakeholder governance system with transparency throughout the data lifecycle. The digital rules of DEPA are of high quality, which imposes greater demands on digital technologies and infrastructure (Zhang 2026). China needs to establish a clear boundary between public data, enterprise data, and personal data and leave some room to institutional innovation by using regulatory instruments like sandbox mechanisms and algorithmic impact assessments.

Moreover, transparent infrastructure with data traceability and usage tracking needs to be developed, and the effectiveness of governance should be increased with the help of technologies like blockchain and privacy-preserving computation, and social trust and accountability should be improved. To sum up, to establish an open and transparent data governance system, it is necessary to further enhance the compatibility of the domestic regulations in China with the international standards, which will help to build the global digital economy.

Conclusion

Being the first trade agreement in the world specifically oriented to the digital economy, DEPA not only proves to have unique benefits in its form and content, but also promises to become a significant platform of future international collaboration and creation of the global digital economy. The principles of openness, inclusiveness, and collaboration that DEPA champions are closely aligned with China's aspiration to foster a community with a shared future in cyberspace. Being an active member of DEPA is not only a strategic decision that would help China to deepen its integration into the global digital trade value chain, but also a major avenue of facilitating domestic governance reform by exerting external institutional pressure. It is also a significant chance to facilitate the systematic harmonization of the domestic digital trade standards in China and the international economic and trade standards of high level. Moving forward, when developing convergence of digital rules, China should also consider the practical issues of multilateral data protection and mutual recognition mechanisms, and actively seek dynamic adjustment channels of Cross-border data flows in various aspects, such as Cross-border data authentication standards and international law enforcement cooperation. China must take advantage of the historical opportunity offered by DEPA, constantly increase its influence and voice in the global digital trade governance, strengthen international cooperation, and play a role in the creation of a more equitable, reasonable, and inclusive global data governance system.

Declarations

Data availability

No new empirical datasets, statistical code, survey data, interview transcripts or proprietary materials were generated or analysed in this study. The analysis is based on official policy documents, public case materials, news reports and published scholarly literature cited in the manuscript. A source and

materials inventory identifying the public materials used, their access information is supplied as Supplementary File for peer review and publication. All data generated or analysed during this study are included in this article and its supplementary information files. For any further clarification regarding data sources or materials, the corresponding author can be contacted through the journal's editorial office.

Acknowledgements

This work was supported by the China Postdoctoral Science Foundation "Research on International Coordination of Cross-border Data Flow Regulation and China's Response" (Grant No.2024T171046)

Author contributions

YS:writing–original draft,writing–review & editing, conceptualization.

JL:writing–original draft,investigation,resources.

Competing interests

The authors declare no competing interests.

Ethical approval

This article does not contain any studies with human participants performed by any of the authors.

Informed consent

This article does not contain any studies with human participants performed by any of the authors.

Additional information

Correspondence and requests for materials should be addressed to Yuanhong Shi.

References

1. Chin YC, Zhao J (2022) Governing Cross-Border Data Flows: International Trade Agreements and Their Limits. Laws 11(4):1–22
2. China News Service (2026) The Tenth Chief Negotiators' Meeting of the Working Group on China's Accession to the Digital Economy Partnership Agreement (DEPA) Held. https://www.chinanews.com.cn/gn/2026/04-29/10612892.shtml
3. Chen M (2024) Developing China's Approaches to Regulate Cross-border Data Transfer
4. Relaxation and Integration Comput Law Secur Rev 54:105997
5. D'Hauwers R, Vandercruysse L, Ballon P (2025) Data sovereignty in personal data mobility ecosystems: A business model perspective. Technol Soc 83:102953

6. Guo D, Wang G (2026) Regulations on Cross-Border Data Flow under the DEPA Framework and China's Response. Citiz Law (Law Edition) 1:27–31
7. Guo S, Li X (2025) Cross-border data flow in China:Shifting from restriction to relaxation?
8. Computer, Law & Secur Rev 56:106079
9. Huang G, Lei Y (2022) The Norms on Cross-Border Data Flows in the RCEP. Asian J Law Economic 13(3):375–404
10. Huo J (2024) DEPA Cross-Border Data Flow: Regulatory Differences and China's Response. Int Econ Trade Explor 40(03):107–120
11. Jiang F (2024) China's legal efforts to facilitate cross-border data transfers: a comprehensive reality check.Asia. Pac Law Rev 32(1):81–101
12. Liu Y, Song G (2023) Opportunities and Strategies for China's Participation in the Rule-Making on Cross-Border Data Flow under the DEPA Agreement. Rule Law Forum 2:17–35
13. Liu X, Lee M, Kim T (2026) Regulatory Fragmentation in Digital Services Trade and Carbon Intensity: Hard and Soft Barriers and the Role of Environmental Policy. Sustainability 18(8):4031
14. Ma H, Kang C (2025) The impact of US-style digital trade rules on digital services trade between China and CPTPP member countries. Technol Soc 83:103040
15. Ma G, Wu H (2025) Cross-border data flow supervision in China's free trade zones: security and compliance rules.Asia. Pac Law Rev 32(2):231–262
16. Ma HY, Yusoff ZM, Romli FB (2026) -People Process Policy 20(3):469–484The dynamic balance between data development and data security in China’s cross-border data flows.Transforming Government
17. Ma G, Wu H (2026) China’s data export regime:an evolutionary trajectory and its practical challenges. Asia Pac Law Rev 34(2):459–487
18. Ma Z (2026) International legal regulation of cross-border data. flow and China's response.Political
19. Science and Law Review (1):3–18
20. National Development and Reform Commission of the People's Republic of China (2026) China Officially Filed an Application to Accede to the Digital Economy Partnership Agreement (DEPA). https://www.ndrc.gov.cn/xwdt/ztzl/zgdmydylcntzhz/202112/t20211202_1328080_ext.html
21. Pogoretskyy V, Riaz MU (2025) Regulating Data in a Fragmented World:Any Scope for Multilateral Cooperation, or a Path Towards Regulatory De-coupling? Legal Issues Economic Integr 52(2):119–153
22. Qi P (2025) China and DEPA Cross-Border Data Flow: A Study on Regulatory Differences and Institutional Docking. Law Rev (Bimonthly) 3:30–43
23. Shi Y (2023) China's shipping market supervision system under theRCEP: Influence, challenges and countermeasures. Front Mar Sci 10:1155452
24. Shi Y (2025) Challenges in governing global digital trade barriers and China’s position. Int J Legal Discourse 10(2):1–17

25. Shi Y (2025) Risk Prevention in Global Cross-Border Data Flows:Challenges and China’s Strategic Responses. Int J Digit Law Gov 2(2):1–27
26. Ulu AB (2026) Cross-Border Transfer Of Personal Data. Istanbul Hukuk Mecmuasi 84(1):1–25
27. Voss WG (2022) Cross-Border Data Flows,the GDPR and Data Governance. Vestinik Mezhdunarodnykh Organizatsii-International Organ Res J 17(1):56–95
28. Wang M, Chen Y (2022) The Legal Implications and System Construction of China's Data Sovereignty. J Intell 6:92–98
29. Xu WX, Wang S, Zuo XD (2024) Global data governance at a turning point? Rethinking China-US cross-border data flow regulatory models. Comput Law Secur Rev 55:106061
30. Zhou N, Yu M (2022) How Should China Align with DEPA? — A Perspective Based on the Comparison between DEPA and RCEP. Theory J 3:55–64
31. Xu WX, Wang S, Zuo XD (2025) Whose victory?A perspective on shifts in US-China cross-border data flow rules in the AI era. Pac Rev 38(6):963–989
32. Yu MN, Wang L (2025) China’s cross-border maritime data flow governance:progress,challenges
33. and prospects. Frontiers in Marine Science 12:1600050
34. Zhang S, Gao H (2025) Bridging the Great Wall: China's Evolving Cross-Border Data Flow Policies and Implications for Global Data Governance. Comput Law Secur Rev 59:106208
35. Zhou T (2025) Research on China's Digital Trade Cross-Border Data Flow Rules under the DEPA Background. China J Commer 18:118–121
36. Zhao J et al (2025) A five rights separation framework for data rights confirmation in data element circulation. Humanit Social Sci Commun 12:1–17
37. Zhang Y (2026) China’s Conflicts with DEPA Data Cross-border Flow Rules and Its Responses. North Legal Sci 20(115):106–120

Footnotes

1. Article 2.7.1 of the DEPA
2. Article 2.5 of the DEPA
3. Chapter 7 and Chap. 8 of the DEPA
4. Article 9.4.3 and Article 9.5 of the DEPA
5. Article 4.3.3 of the DEPA
6. Article 24 of the Data Security Law
7. Chapter 8 of the DEPA
8. Article 8.2 of the DEPA

Supplementary Files

This is a list of supplementary files associated with this preprint. Click to download.

- SupplementaryFile1.doc