Proceedings of the 3rd International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/55/20240067

Issues in China's Alignment with DEPA Data Cross-Border Regulation

Ziyu Xu[1,a,*]

[1]*School of Law, Shanghai University of International Business and Economics, Wenxiang Road, Songjiang District, Shanghai, 201600, China*
a. 21062187@suibe.edu.cn
**corresponding author*

Abstract: In the global digital governance game, the *Digital Economy Partnership Agreement* (DEPA) features innovative designs for digital trade, aligning with China's goals of internal data sharing openness and external breaking of "rule locks". However, China currently exhibits significant legislative differences in the "Data Issues" section of DEPA's fourth module, adopting stricter regulatory measures for cross-border data flow and data localization. Addressing DEPA's "principle & exception" regulatory standards, this paper argues that legitimate public policy objectives can be aligned with DEPA through proportionality principles, WTO general exception clauses, etc. By innovating customs supervision methods and following the path of the Hainan Free Trade Port trial, connecting international trade new rules, orderly implementing law enforcement systems and supporting mechanisms to ensure data security and orderly flow, China can gradually align with DEPA.

Keywords: DEPA, digital cross-border flow, data localization, legitimate public policy objectives

1. Introduction: Urgency and Necessity of China's Alignment with DEPA

With the development of global digital trade, regional Free Trade Agreements (FTAs) are deepening within and among countries and international organizations. Unified regulation of cross-border data flow is becoming increasingly important, yet countries are unable to negotiate their close interests in the field of digital flow, leading to a lack of breakthroughs and progress in the services trade under the WTO, involving only basic principles of data protection and personal information protection. Against this backdrop, the *Digital Economy Partnership Agreement* (DEPA) was signed in 2020 by Singapore, Chile, New Zealand, and other countries, establishing typical "new" digital trade rules. In 2021, China also applied to join DEPA. DEPA's application can effectively solve various micro-subject information barriers in China's national economy and reduce the customs trade cost burden of being an exporting country, while also creating a data regulation sandbox for governments and industries, generating more economic benefits and enhancing China's international digital governance competitiveness.

Therefore, through text analysis of DEPA and China's domestic laws and regulations, clarifying differences and obstacles to aligning with DEPA, and exploring different rules in the field of digital economy and mobility, it is crucial for China to improve its alignment with DEPA for its application and accession.

DOI: 10.54254/2753-7048/55/20240067

2. Obstacles for China's Alignment with DEPA

Although China has implemented many effective digital governance policies, the system of enterprise data sharing and government data opening is still in its infancy. From a legal perspective, there are still significant conflicts between China's legal norms and DEPA's requirements in the areas of cross-border data flow and data localization in Module Four of DEPA.

2.1. Various Issues Concerning Data in Module Four

Module Four of DEPA deals with Data Issues, involving aspects such as personal information protection, cross-border transmission of information via electronic means, and the location of computing facilities. According to the alignment of DEPA with China's laws and regulations, China has established laws and regulations such as *the Personal Information Protection Law*, *the Data Security Law*, *the Measures for the Security Assessment of Exporting Data*, t*he Guidelines for Data Export Security Declaration*, and *the Implementation Rules for Personal Information Protection Certification*. Personal information protection has been discussed earlier with no alignment obstacles, while the remaining two aspects, through textual comparison of laws and regulations, can be clearly listed to demonstrate alignment conflicts.

2.1.1. Comparison of DEPA and China's Mechanisms for Cross-Border Data Flow

Controlling and restricting data export is a key focus of safeguarding national digital security. It was not until 2022 that China's Measures for the Security Assessment of Exporting Data defined data export as the act of data handlers providing important data and personal information collected or generated domestically to overseas entities. [1]Firstly, the connotation of data cross-border flow is different from DEPA's Section 4.3, with China using the term "provide" while DEPA, similar to the EU GDPR, uses the term "transfer." From an interpretive perspective, the scope defined by transfer is obviously larger than that of provide, where transfer includes both active provision and passive transmission [2],while "provide" may have loopholes and may not be recognized domestically as data cross-border transmission, but under DEPA, it could be deemed as "cross-border transmission of information via electronic means."

In terms of data cross-border regulatory issues, China is more stringent, as shown in Table 1:

Table 1: Comparison of China's Data Export Mechanism with DEPA Requirements

DEPA Data Cross-Border Flow Requirements	China's Data Export Mechanism
Section 4.3: Cross-Border Transfer of Information by Electronic Means The Parties affirm their level of commitments relating to cross-border transfer of information by electronic means, in particular, but not exclusively: 1. The Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.	China's current legal framework for information export: 1. Security Assessment Measures (administrative licensing): The Personal Information Protection Law regards security assessment as a necessary condition for data export, and its administrative declaration needs to comply with the Guidelines for Data Export Security Declaration. After complying with the Security Assessment Measures, the data is "unblocked."

DOI: 10.54254/2753-7048/55/20240067

Table 1: (continued)

2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or (b) does not impose restrictions on transfers of information greater than are	2. Standard contract terms: China currently has only one standard contract sample, and it requires strict compliance. Although the recipient or sender of the information does not hold Chinese nationality, stricter contract terms require overseas parties to meet the same level of protection. 3. Personal Information Protection Certification (pre-approval supervision): The promulgation of the Implementation Rules for Personal Information Protection Certification has established dual supervision of regulatory and certification agencies for the cross-border movement of personal information data.

From the textual comparative analysis, it can be concluded that DEPA's clauses on cross-border data circulation have fewer restrictions, encouraging high degrees of freedom for development and contracting countries to set their own regulations. However, in China, there are three parallel mechanisms for the regulation of cross-border data circulation, rather than overlapping, which are conducted in parallel. The security assessment method is a specific administrative licensing act, standard contract terms exist in the commercial field, and personal information protection certification is a third-party regulatory action. China has strict and complex regulations in all three areas of cross-border data circulation, indicating a clear gap in the level of freedom and DEPA's textual representation of freedom. The requirement for "individual regulation" is clearly based on the mutual recognition of regulatory standards and levels among contracting parties, allowing for "free" establishment. However, the establishment of exceptions in the DEPA also indicates that member countries are not entirely devoid of the right to set regulatory requirements [3]. Article 4.3 of the DEPA stipulates exceptions for legitimate public policy objectives, which China should consider how to interpret and apply to actively seek a balance between data security and sovereign interests.

Nevertheless, due to the ambiguous nature of the exceptions provided by the DEPA, contracting parties will inevitably fully utilize these exceptions, leading to potential abuse. If China’s methods, interpreted as legitimate public policy objectives, are deemed abusive by other contracting parties, establishing post-dispute resolution strategies is something China needs to consider. Furthermore, given that China has already committed to market access and national treatment for most service sectors under the WTO framework in cross-border delivery modes, measures restricting the cross-border flow of personal data are likely to be seen by other countries as a violation of these commitments, leading to potential litigation. The abuse of legitimate public policy objectives and subsequent litigation for violating national treatment are defenses China needs to explore when applying for DEPA.

2.1.2. Comparison Between DEPA and China's Data Localization Requirements

Article 4.4 of the DEPA specifies the location of computing facilities, thus addressing data localization requirements. Data localization requires data controllers to store data within the country's borders or set up facilities domestically. This topic, often considered a trade barrier in academic discussions, is sensitive due to intellectual property protection concerns. For example, Japan and

DOI: 10.54254/2753-7048/55/20240067

Canada resist data localization, insisting on the principle that countries should have autonomy in the digital network realm unless it pertains to legitimate public interests. Conversely, the EU, Russia, and China support data localization, citing the need for domestic citizen privacy and public cyberspace governance, establishing data storage centers in the host country [4].

According to the textual comparison (see Table 2), there is a conflict between China's mandatory local data storage requirements and DEPA's data localization regulations.

Table 2: DEPA Data Localization Requirements vs. China's Data Localization Requirements

DEPA Data Localization Requirements	China's Data Localization Requirements
Article 4.4: Location of Computing Facilities The Parties affirm their level of commitments relating to location of computing facilities, in particular, but not exclusively: 1. The Parties recognise that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications. 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory. 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure: (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.	Types of Data Required to be Stored Locally: 1. Article 36 of the *Personal Information Protection Law* stipulates that personal information processed by state organs must be stored within the People's Republic of China. 2. Article 37 of the *Cybersecurity Law* requires that personal information and important data collected and generated by critical information infrastructure operators within the territory must be stored domestically. This data can only be transferred abroad after a security assessment (administrative permit) [5] . 3. Article 73(3) of the *Network Data Security* Management Regulations (Draft for Comments) specifically lists seven types of data that, if altered, destroyed, leaked, or illegally obtained or used, could endanger national security or public interests [6].

The DEPA explicitly prohibits member countries from requiring data localization as a precondition for conducting business, while China prioritizes national security and public interest, mandating that personal information handled by international organizations and operators of critical information infrastructure collected and generated domestically must be stored locally through legislation. Addressing this conflict hinges on how to reasonably interpret and apply the exception rule—legitimate public policy.

3. China's Strategies for Joining DEPA

Based on the comparison and discussion of the obstacles and conflicts in the fourth module related to China's alignment with the DEPA, China needs to focus on how to argue that its mandatory legal requirements comply with legitimate public policy objectives when formulating strategies for joining DEPA. Currently, academia has proposed new requirements for customs' regulatory duties in relevant fields and suggests that China should first experiment with DEPA alignment in free trade ports.

3.1. Exception for Legitimate Public Policy Objectives

3.1.1. Legitimacy and Public Policy of Cross-border Data Flows

Whether China's domestic measures regulating cross-border data flows can invoke DEPA's exception

DOI: 10.54254/2753-7048/55/20240067

clauses depends on whether China can apply legitimate public policy objectives.

According to the legal norms for cross-border data flow regulation in various countries, the use of personal information protection certification and standard contractual clauses is common, making the legality of cross-border data flow restrictions align with the values of protecting cross-border data in these countries [7]. Besides these two methods, China also employs specific administrative actions—namely, the security assessment system.

The application of the security assessment system can be justified through the principle of proportionality in China's administrative law system [8], which has three judgment points: appropriateness, necessity, and proportionality (moderation). Given that China is in the early stages of developing cybersecurity, with many laws and regulations still incomplete, adopting stringent regulatory and reporting details to safeguard national and personal information security is entirely legal and appropriate. Therefore, the argument for the security assessment system should consider both necessity and moderation.

From the perspective of necessity, many uncontrollable factors exist in the cross-border transportation of data. Without a sound cooperation mechanism between the two trading countries, Chinese data risks losing control, being illegally processed, and misused [9] . Compared to such significant risks, China's specific administrative licensing actions, requiring entities to report to relevant authorities before transferring data abroad and having these authorities review and evaluate whether they meet China's legitimate public policy security objectives before granting permission, are logical and necessary.

From the perspective of moderation, it is essential to balance and compare the public interest damage caused by implementing the security assessment system and the purpose and objectives achieved. Currently, due to significant differences with other countries advocating data openness and freedom, China has faced considerable criticism. How to quantify the legal harm caused by the security assessment system and achieve justified goals to avoid being deemed excessive due to vague provisions is crucial for China's DEPA alignment expert group to focus on.

3.1.2. Data Localization as a Legitimate Public Policy Objective

China's mandatory data localization requirements for certain important and sensitive data can also be discussed through the necessity and appropriateness criteria of the proportionality principle. To prove necessity, one can argue inversely that without local storage, information security cannot be maintained. To justify the appropriateness of localization, one needs to balance the value of localization measures and the economic costs of choosing localization. Regarding the value of localization measures, China can argue that given the limited and special nature of the areas restricted by localization measures, sacrificing some value to achieve more important national and social security value is justified. From an economic cost perspective, China can demonstrate feasibility by showing the financial costs of operating data storage centers in the long run or by taking effective measures (outsourcing, cooperation, etc.) to reduce operating costs [10].

3.1.3. Other Approaches to Arguing Legitimate Public Policy Exceptions

As a digital version of the WTO, DEPA aligns its exception rules highly with WTO's exception rules by emphasizing terms like "it considers" to seek greater autonomy in applying exception rules. However, for the "legitimate public policy" exception rule, DEPA uses the term "not...greater than," indicating that the right to judge whether something is considered a public policy does not lie with the members but adopts an objective standard. In resolving disputes in the digital trade field, DEPA explicitly states that reference can be made to the practices of the WTO expert groups and appellate bodies.[11] Therefore, referring to and borrowing from the general exception clauses' "necessity test"

DOI: 10.54254/2753-7048/55/20240067

in existing WTO dispute resolution practices to interpret and apply the "legitimate public policy exception" is feasible.[12] Although the general exception clauses are seldom used, according to WTO adjudication practices, as long as the contested trade measure does not restrict trade or the purpose of the contested member is not entirely unrealistic or insignificant, the panel will first recognize the necessity of the contested measure's temporary implementation, which is advantageous for China. China can argue that its measures contribute to achieving domestic implementation objectives.

Whether invoking the principle of proportionality or WTO clauses, China must first rationally and logically define what constitutes a legitimate public policy objective and strive to explain it through annotations to ensure national security interests are included [13].

3.2. Transformation of Digital Trade Customs Regulation

Customs, as the key point for various goods entering and exiting the country, plays a significant regulatory role in digital trade. Digital trade relies on information networks and digital technologies. Notably, the innovative DEPA agreement stipulates the digital development of trade objects and methods. As the primary entity for entry and exit review, customs should propose higher requirements for its regulatory targets and scope, continually aligning with internationally recognized economic and trade rules. DEPA requires adopting internationally recognized standards for electronic payments in approval, licensing, and technical standards. However, with the interconnection between domestic electronic payment and foreign systems, issues concerning the protection of Chinese citizens' information, consumer rights, and transaction procedure disputes arising from new cooperation and interconnection will gradually emerge. This imposes new requirements on China's legal norms supporting the digital transformation of customs regulation [14].

3.3. Pilot Implementation in China's Free Trade Ports

Unlike other developed countries, China has significant development level disparities among its provinces and regions, with varying levels of electronic invoice infrastructure, digital trade development, and customs regulation. To test China's alignment with DEPA, the Hainan Free Trade Port should first be allowed to connect with international high-standard economic and trade rules.

Singapore is a successful island economy and free trade port, while Hainan is a new island economy in China with a natural geographical advantage and national foreign trade policies, making it more representative in digital trade. Hainan Province has also established the country's first Big Data Administration and a provincial big data industry alliance, providing effective management institutions for cross-border data flows.

However, with the implementation of RCEP, Hainan Free Trade Port's competitive advantage in goods trade will diminish. It should draw on international successful experiences, further reduce the number of negative lists for foreign investment, and quickly align the investment dispute resolution procedures with CPTPP standards, actively introducing third-party evaluations under fair competition policies [15].

In addition, transitional provisions should be introduced in China's free trade ports to facilitate the alignment with international economic and trade rules. Similar to Vietnam's extensive domestic legislative changes to fulfill CPTPP obligations, such an approach is not feasible in China. Instead, China should emphasize the path of piloting first in free trade zones, providing gradual legislative guarantees through transitional provisions and establishing temporary or trial laws and regulations for effective coordination, promoting a smooth transition from old to new laws [16].

DOI: 10.54254/2753-7048/55/20240067

4. Conclusion

DEPA innovatively introduces a modular design, establishing a "new" model in the digital trade field. DEPA encourages data openness and sharing, aligning with China's contemporary policies of digital transformation and trade facilitation, aiding China in leading the digital governance track. Currently, China has stringent regulations on cross-border data flows, mandating necessary conditions for local data storage for certain sensitive and important data. These legislative and licensing differences have been widely discussed and identified as issues and conflicts in China's alignment with DEPA. In considering how to align with DEPA, China should not limit its thinking to the digital trade field but expand its argumentative scope to the administrative proportionality principle and WTO's general exception clauses. Besides arguing for legitimate public policy objectives and improving domestic systems, China should also initiate cooperation with international standardization organizations such as RCEP, first piloting and testing in the Hainan Free Trade Port, and gradually aligning with international and unified standards in electronic payments and customs regulation.

References

[1] *Regulations on Security Assessment of Data Exit, Article 2.*
[2] *Cai, Y. J. (2023). Definition and regulatory system of data exit. Journal of China University of Political Science and Law, 3.*
[3] *Xu, M. L., & Dong, J. X. (2023). DEPA data cross-border flow rules orientation and response. Scientific Management Research, 5.*
[4] *Sun, N. X. (2022). CPTPP digital trade rules: Institutional games, regulatory differences, and China's response. Academic Forum, 5.*
[5] *Cybersecurity Law, Article 37.*
[6] *Network Data Security Management Regulations (Draft for Comments), Article 73(3).*
[7] *Xu, L. (2023). Regulation of cross-border data flows: "Legitimate public policy objectives exception" and China's practice. Qiusuo, 4.*
[8] *The principle of proportionality has penetrated into various Chinese laws, such as Articles 5, 6, 13, 19, 28(2), 30, 47, etc., of the Personal Information Protection Law.*
[9] *Yao, X. (2019). EU governance of cross-border data flow: Balancing free flow and regulatory protection. Shanghai People's Publishing House, p. 24.*
[10] *Wang, C. Q. (2023). Compatibility review and optimization path of China's data governance in the context of applying for DEPA membership. Pacific Journal, 3.*
[11] *DEPA, section 14-C.6, paragraph 3.*
[12] *See Yoshinori Abe, David Collins, The CPTPP and Digital Trade: Embracing E-Commerce Opportuniti--es for SMEs in Canada and Japan, Transnational Dispute Management, 3-16(2018).*
[13] *Wang, R., & Pan, Y. C. (2022). Insights from the differences between CPTPP and RCEP for China's response to digital trade rules competition. International Trade, 3.*
[14] *Jin, S. Y., & Shen, W. (2022). Digital trade facilitation in EPA: Rule investigation and China's response. Customs and Trade Research, 4.*
[15] *Gan, L. (2023). Aligning RCEP, CPTPP, and DEPA rules to promote institutional opening of service trade in Hainan Free Trade Port. South China Sea Studies, 3.*
[16] *Cui, H. R., & Li, B. (2022). Coping with the challenges of CPTPP state-owned enterprise rules: Vietnam's domestic law adjustments and their implications. International Trade, 8.*