Proceedings of ICILLP 2025 Symposium: Digital Governance: Inter-Firm Coopetition and Legal Frameworks for Sustainability
DOI: 10.54254/2753-7048/2025.BR26001

Tendency of Trade Barriers in Data Localization Policies and International Legal Responses

Hanyu Zheng

School of Humanities and Law, North China Institute of Science and Technology, Langfang, China
Z1878287979@outlook.com

Abstract. With the in-depth development of the digital economy, the need for regulating cross-border data flows is intertwined with the game of national interests. This paper explores the paths through which developed countries expand their digital hegemony as well as the response logic and practices of developing countries. Using literature research and case analysis methods, the study finds that developed countries expand their digital hegemony by long-arm jurisdiction and dominance in rulemaking. They extend their judicial power to the global data field through relevant laws and rely on their rule systems to interfere in other countries' data localization measures. In response, developing countries adopt approaches such as classified and hierarchical management and regional cooperation, reduce compliance costs through technical means, and explore flexible space for cross-border data flows within regional frameworks. This study reveals the differences in data localization policies and the power imbalance between developed and developing countries, providing theoretical references for developing countries to cope with digital hegemony and protect their own data security, and contributing to the construction of a fair global data governance system. It is suggested that developing countries should improve data security assessment mechanisms and deepen regional cooperation to enhance their right to speak. At the international level, efforts should be made to promote the reform of international investment law, clarify the attributes of data assets, and establish a multilateral cooperation framework to counter unilateral hegemony, to achieve a dynamic balance between security and development in the context of data globalization.

Keywords: data localization, trade barriers, digital hegemony, data sovereignty, cross-border governance of data flows.

1. Introduction

In the era of the digital economy, data, as a core production factor, has increasingly highlighted its value and become a key driver of high-quality economic development. Meanwhile, with the deepening of economic globalization, the need for regulating cross-border data flows is intertwined with the game of national interests. To safeguard national security, data sovereignty, and industrial competitiveness, various countries have introduced data localization policies, requiring critical data to be stored or processed within their borders. For example, China's Cybersecurity Law stipulates that important data of operators of critical information infrastructure must be stored domestically;

DOI: 10.54254/2753-7048/2025.BR26001

although the United States has not joined the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), it still promotes the concept of free data flow through its own influence. Relying on the global layout of its domestic tech giants, it strengthens its discourse power in the digital economy through the export of technical standards and market access rules, essentially promoting the tilt of data flows toward the United States and American enterprises [1]. Some scholars argue that such barriers are essentially a reflection of developed countries advocating free flow by virtue of their technological first-mover advantages, while developing countries attempt to cultivate local ecosystems and prevent data hegemony through localization [2].

At the same time, due to differences in countries' demands for data localization, the incompatibility between traditional international investment law and such policies has become increasingly prominent. The definition of "investment" in current international investment concepts is mostly tied to the tangibility and fixed location of the real economy. However, as a new type of intangible property, data assets, with their non-exclusivity and non-territoriality, have logical conflicts with existing rules [1]. Some scholars also point out that developed and developing countries have divergent stances on data localization: developed countries, which dominate the rules, regard data localization as trade barriers, while developing countries pay more attention to policy sovereignty. This divergence reflects the inequality in the power structure of the digital economy-for instance, the United States expands its jurisdiction through the "data controller standard," while emerging economies like China assert data sovereignty through "security assessment" mechanisms [1].

Based on this, this study focuses on the tendency of data localization policies to become trade barriers, with a particular focus on the phenomenon where developed countries promote their hegemony through long-arm jurisdiction and the internationalization of domestic laws. Using literature research and case analysis methods, it explores and summarizes how data localization policies have transformed from "protective measures" into "trade barriers," analyzes the impact of developed countries' use of policy-based long-arm jurisdiction on the digital economies of developing countries, and puts forward relevant suggestions.

2. Literature review

Regarding the issue of addressing the tendency of trade barrierization in data localization policies through international law and the construction of domestic rule systems, some scholars argue that international investment law needs to break through the limitations of traditional "physical investment" and clarify the nature of data assets. Specifically, data assets can be divided into two categories: "ordinary data" and "sensitive data." The former shall apply the principle of free flow, while the latter allows developing countries to implement localized storage based on national security and set a transition period through security assessment mechanisms [1]. Other scholars believe that countries need to strengthen procedural justice and international cooperation at the level of international rules and actively use multilateral frameworks to counter countries that attempt to interfere with other nations' data autonomy, preventing them from expanding data hegemony through long-arm jurisdiction or unilateral rules [3].

In addition, some scholars suggest that solutions can be found by examining different attributes of data sovereignty. On the one hand, a country should possess "hard power" over domestic data, such as jurisdiction, independence, and the right to self-defense. China classifies and grades data through the Data Security Law and Personal Information Protection Law, requiring sensitive data related to national security to be stored domestically and subject to outbound security assessments, which can effectively protect national data security. On the other hand, it is also possible to exert the

DOI: 10.54254/2753-7048/2025.BR26001

"soft power" of data sovereignty by building an international data governance cooperation framework through multilateral cooperation-for example, establishing a Digital Silk Road data cooperation circle and conducting cooperation with a large number of developing countries to enhance international competitiveness in the data market [4]. Some scholars have summarized that the core of the dispute over data localization lies in the conflict between data security and technological innovation: complete localization will hinder the development of technologies such as cloud computing and artificial intelligence that relieve global data circulation, while excessive free flow may leave developing countries unable to protect their own data security [5].

Based on this, this study holds that existing research has provided diverse ideas for addressing the tendency of trade barrierization in data localization policies from the dual dimensions of international rules and domestic laws. Therefore, this study will explore the differences and impacts of data localization policies between developed and developing countries from three perspectives: how data barriers emerge, the unfair phenomena in cross-border data cooperation rules, and how to address trade barriers at both domestic and international levels, so as to provide countermeasure references for developing countries to reduce or avoid the long-arm jurisdiction of developed countries.

3. Current status of data governance across nations

In the field of data governance, there are significant differences in concepts between developed and developing countries. The core lies in how to position data localization measures. Developing countries emphasize the security protection attribute of data localization. They prevent leakage risks by storing critical data within their borders. Essentially, they exercise sovereign jurisdiction over data by controlling the location of data storage. Take China as an example. The Cybersecurity Law requires operators of critical information infrastructure to store data within the territory and even extend the scope to all network operators. It holds that localization is a core means to resist data leakage and ensure national security. Russian legislation clearly stipulates that citizens' data must be stored on domestic servers and prevents the risk of external data abuse through strict domestic storage rules. Among ASEAN countries, Indonesia requires that data centers and disaster recovery centers of operators of public service electronic systems must be located within the territory. Vietnam stipulates that service providers such as social networks and online games must be equipped with local servers to store user data. Malaysia and Singapore require that the receiving country must provide an equivalent level of protection before personal data is transferred abroad [6,7]. This paper holds that the series of data localization policies introduced by developing countries always revolve around the core logic of data sovereignty. Various countries establish institutional frameworks through legislation or rely on technical means to achieve data control and reduce potential external risks. This is consistent with the practical demands of developing countries to safeguard data sovereignty and ensure data security.

Different from developing countries, developed countries, relying on their dominant position in the rule system, continue to promote the free flow of data. The United States clearly required in the renegotiation of North American Free Trade Agreement (NAFTA) that contracting parties must not implement measures restricting cross-border data flows or mandating local storage. It holds that these regulations artificially increase corporate compliance costs and hinder the free trade of digital services. Although the European Union (EU) claims to pay attention to data protection, its adequacy determination mechanism essentially takes its own rules as the evaluation standard and relies on rule dominance to interfere with the implementation of data localization measures in other countries [7].

DOI: 10.54254/2753-7048/2025.BR26001

This tendency essentially regards the security protection measures of developing countries as trade barriers.

In judicial practice of data governance, developed and developing countries show significant differences in their positions on the scope of jurisdiction and principles of data flow. Developed countries take the free flow of data as the core and expand digital hegemony through long-arm jurisdiction. Take the "football data company case" as an example. A non-EU football data company sold data products in some EU countries. The EU Court of Justice, when making a ruling, denied the practice of determining jurisdiction only based on server location. It ruled that jurisdiction requires proof that the defendant intentionally targets specific member states, such as whether it intentionally provides goods or services to data subjects in specific EU countries, or monitors data subjects in these countries. The United States requires foreign enterprises to provide data through the Cloud Act, directly extending its domestic judicial power to the global data field [8]. This judicial practice essentially breaks through the limitations of territorial jurisdiction by virtue of rule advantages, transforms the concept of free data flow into expansive power at the judicial level, and essentially strengthens digital hegemony.

Developing countries emphasize the priority of data sovereignty and achieve security and development through classified management. Developing countries represented by China have always emphasized the priority of data sovereignty at the judicial level. Their judicial practice highly reflects the principle of territorial jurisdiction. Courts can exercise jurisdiction over non-resident defendants only based on the location of servers. In the case of Danish Rockwool Company suing a Dalian company in China, the Jiangmen Court exercised jurisdiction because the third-party server of the defendant's website was located in Jiangmen, Guangdong, reflecting the core position of server location as the basis for jurisdiction [8]. This approach is closely related to China's data localization policies. Laws require that data in key fields such as finance and medical care be stored within the territory. Server location has become a key point connecting data activities and judicial jurisdiction. It not only ensures data security but also provides a clear judicial framework for domestic data activities.

4. Choices for different entities in responding to data trade barriers

In addressing data trade barriers, developed countries often rely on rule-making power and technological discourse power to consolidate their advantageous positions. The European Union promotes data mutual recognition mechanisms with compliant countries, allowing data to flow only to regions that meet its privacy requirements. In May 2023, the EU fined Meta 1.3 billion US dollars for transferring data from the EU to the United States in violation of rules. It essentially uses law enforcement to counter data flow arrangements that do not meet its own standards and strengthens its leading power in regional data governance. Some developed countries choose to rely on technological advantages to deal with data trade barriers. Switzerland, though not a traditional major power, links user privacy with the safety symbol of Swiss manufacturing through public-private sector collaboration. Its encrypted communication application Thema emphasizes its security and advantages of local data centers on its official website, attracting 11 million users to choose its services to avoid external data control, thus indirectly breaking through the restrictions of single data localization [9].

Developing countries, restricted by the level of digital technology, are more inclined to make gradual adjustments within regional frameworks to deal with data trade barriers. China is an example. Its special economic zones have improved regulatory efficiency through blockchain technology. Beijing's blockchain-based single window data storage box integrates trade, logistics

DOI: 10.54254/2753-7048/2025.BR26001

and customs data, realizing electronic submission and automatic verification of documents, reducing manual intervention and repeated review, and indirectly lowering enterprise compliance costs and government regulatory expenditure [10]. China's big data exchanges promote circulation on the premise of ensuring data security through technical design, providing a referential technical adaptation scheme for regions with relatively backward digital infrastructure, that is, there is no need to build high-end facilities in one step, and the governance threshold can be reduced through targeted technical means; on the other hand, relying on regional alliances to strive for a transition period is also an important strategy [10]. Due to weak digital infrastructure affecting the ability to participate in regional negotiations, developing countries often seek buffer space through regional frameworks. China, within the RCEP framework, has explored the conditional opening of cross-border data flows through pilot projects in special economic zones. The cross-border data transmission pilots carried out in industries such as automobiles and medical care in Shanghai Lingang New Area are such cases. They abide by the basic requirements of domestic data localization and strive for flexible space for specific fields [10]. In addition, there are differentiated response methods at the enterprise level. Under the highly restrictive data localization system, enterprises in developing countries have the advantage of not needing to bear cross-border compliance costs, and consolidate their domestic market share by optimizing service quality and maintaining price competitiveness; the state needs to balance between protecting domestic industries and maintaining market vitality, and by setting differentiated data type rules, it not only reduces the obstacles of compliance costs to global enterprises, but also retains development space for local enterprises [11].

At present, developed countries expand their digital hegemony by virtue of long-arm jurisdiction and rule-making power, and define the reasonable data localization measures of developing countries as trade barriers, which leads to the predicament of game between data sovereignty maintenance and data free flow in global data governance. The international community needs to call on developed countries to abandon discriminatory rules, and on the basis of respecting the data sovereignty of all countries, build a cross-border data flow framework that takes both security and development into account, so as to avoid alienating technical standards and judicial jurisdiction into tools to contain developing countries [5].

Developing countries represented by China should deal with challenges by strengthening classified and hierarchical data management and deepening regional cooperation. As a representative of developing countries, China adheres to the principle of giving priority to data sovereignty in data governance and realizes the balance between data security and economic development through classified management. This feature is prominently reflected in the new competition system of the digital economy. To solve the problem of high concentration in the digital market, China has built a new competition framework including ex-ante and ex-post supervision, explicitly implementing ex-ante approval for enterprise concentrations with specific structures, and formulating ex-post remedies such as data divestiture and platform opening for behaviors like data abuse. This classified management strategy has achieved remarkable effects in core markets of leading platforms such as Baidu, Alibaba and Tencent, reducing market concentration through precise supervision, breaking power monopoly in the data field, and providing support for formulating fair and reasonable data trade rules, avoiding excessive control of data governance power by a few enterprises or countries [12].

The current global data governance pattern is diverse. On one hand, some entities promote free data flow through technical design or rule negotiation, which is consistent with the trend centered on free data flow; on the other hand, the issue of extraterritorial effect involved in data sovereignty

DOI: 10.54254/2753-7048/2025.BR26001

implies the logic that some countries break through regional restrictions through laws or rules, which is indirectly related to the connotation of long-arm jurisdiction [13]. This complex situation highlights the importance of developing countries to strengthen their own governance capabilities and enhance discourse power through regional cooperation. China can gradually transform from a rule receiver to a co-builder by issuing laws on cross-border data flow management, establishing independent data supervision commissions, promoting mutual recognition of digital rules under the Belt and Road Initiative and other measures, promote global data governance to develop in a more fair and reasonable direction, and achieve a dynamic balance between security and development in the process of data globalization.

5. Conclusion

This paper adopts literature research and case analysis methods to explore the tendency of data localization policies to become trade barriers and the phenomenon where developed countries expand their digital hegemony through long-arm jurisdiction and rule dominance. It summarizes that data localization policies have duality, and there are significant differences in data governance concepts between developed and developing countries. It further points out that developing countries should respond to challenges by strengthening classified and hierarchical data management and deepening regional cooperation, so as to balance security and development in data globalization.

Data localization has both advantages and disadvantages in international economic and trade cooperation. For example, developing countries such as China can ensure their own data security through it. By mandating domestic storage of critical data, they can effectively prevent data leakage, abuse and monitoring by foreign forces, and protect national sovereignty, security and citizens' privacy. However, it can easily give rise to trade barriers, restrict data flow, push up corporate compliance costs, and hinder the implementation of the "going global" strategy.

But data protection is not an exclusive strategy for developing countries. Developed countries, through means such as setting invisible thresholds, are more inclined to reach cooperation with countries and regions with developed market economies. They also use their discourse power to define reasonable protection measures of developing countries as trade barriers, putting developing countries in a passive position in terms of rules in cross-border data activities.

Facing this situation, as mentioned above, developing countries have initially formed regional data cooperation circles. China can issue laws related to cross-border data flow management, establish an independent data regulatory commission, promote mutual recognition of digital rules under the Belt and Road Initiative, and gradually transform from a rule receiver to a co-builder.

References

[1] Zhang, Y. (2025) On the Protection of Data Assets by International Investment Law. China Maritime Law Research 36(01), 77-90.
[2] Chen, Z. (2024) Research on the Protection of Overseas Digital Assets of Investors under the Framework of International Investment Law. Master's Dissertation, Southwest University.
[3] Li, J.N. and Han, L. (2023) Study on the Influence of American Long-Arm Jurisdiction on Foreign-Related Enterprises in China and Its Countermeasures: Taking TikTok as an Example. Tsinghua Law Review 11(01), 232-255.
[4] Kuang, M. (2025) Protection of Data Sovereignty under the Background of Long-Arm Jurisdiction. Legal Science (Journal of Northwest University of Politics and Law) 43(01), 132-145.
[5] Taylor, R.D. (2020) "Data Localization": The Internet in the Balance. Telecommunications Policy 44(8), 102003.

DOI: 10.54254/2753-7048/2025.BR26001

[6] Wong, B. (2020) Data Localization and ASEAN Economic Community. Asian Journal of International Law 10, 158-179.
[7] Bennett, C. and Oduro-Marfo, S. (2018) Global Privacy Protection: Adequate Laws, Accountable Organizations and/or Data Localization? Proceedings of the 2018 ACM International Joint Conference and 2018 International Symposium on Pervasive and Ubiquitous Computing and Wearable Computers, 880-890.
[8] Huang, J. (2019) Chinese Private International Law and Online Data Protection. Journal of Private International Law 15(1), 186-209.
[9] Fratini, S. and Musiani, F. (2025) Data Localization as Contested and Narrated Security in the Age of Digital Sovereignty: The Case of Switzerland. Information, Communication & Society 28(8), 1368-1386.
[10] Huang, J.J. (2023) Digitalization of Special Economic Zones in China. The Elgar Companion to the World Trade Organization, 186-206.
[11] Potluri, S.R., Sridhar, V. and Rao, S. (2020) Effects of Data Localization on Digital Trade: An Agent-Based Modeling Approach. Telecommunications Policy 44(9), 102022.
[12] Baum, L. and Bryson, J.J. (2023) Policy Lessons from China: A Quantitative Examination of China's New Competition Regime for the Digital Economy. Doctoral Dissertation, Hertie School, Berlin.
[13] Hummel, P., Braun, M., Tretter, M. and Dabrock, P. (2021) Data Sovereignty: A Review. Big Data & Society 8(1), 2053951720982012.