International Journal of Scientific Engineering and Science
Volume 9, Issue 1, pp. 27-29, 2025. ISSN (Online): 2456-7361

The Impacts of Restrictions on Cross-Border Data Transfers and Policy Recommendations for Nations

Huong Quan Do[1], Lam Anh Le[2], Diep Anh Nguyen[3]
[1, 2, 3]Faculty of Economic Law, Hanoi Law University, Hanoi, Vietnam

Abstract**—***Data has become a core driver of the global digital economy and a valuable resource in international commerce. However, the ease of external access to domestic data flows presents significant challenges for national governance. As a result, many countries impose restrictions on cross-border data transfers to control or prevent the outflow of domestic data beyond territorial borders. Within the scope of this article, the authors analyze and evaluate the economic and legal impacts of current cross-border data transfer restrictions on countries and propose recommendations for policy development to support data governance.*

Keywords**—***Cross-border data transfer restrictions, impacts, international trade, legislation, recommendations.*

I. INTRODUCTION

In the era of digitalization, data has become an essential resource, forming the foundation for economic growth, technological innovation, and global integration. The rapid increase in data collection, processing, and cross-border transfers, however, has created significant legal and economic challenges. To safeguard privacy, national security, and other interests, many countries have introduced regulations to restrict cross-border data transfers. As of 2021, there were 92 such measures in place across 39 countries, with more than half introduced in the past five years. [1] These measures vary in purpose, data types, implementation methods, and scope. For instance, Australia restricts the transfer of health data out of the country, while Russia mandates that personal data be stored domestically. Methods range from requiring individual consent for data transfer to domestic data replication and even data export taxes... [2]

While cross-border data transfer restrictions aim to mitigate escalating risks related to cybersecurity and privacy, they often create conflict between domestic and international legal frameworks. This is particularly problematic given that many existing international trade agreements lack clear, specific, and updated provisions regarding data. This discord heightens the likelihood of disputes and threatens the development of economies heavily reliant on digital trade. Thus, it is essential to assess the impacts of these regulations on nations to inform and refine national legal policies.

II. AN OVERVIEW OF CURRENT CROSS-BORDER DATA TRANSFER RESTRICTIONS

The term “cross-border data transfer restrictions” has gained prominence in the digital age, yet it lacks a universally accepted definition, reflecting the complexity and evolving nature of data governance. However, based on international and national documentation and existing research, the authors define this term from a legal perspective *as a set of regulatory and legal measures implemented by governmental authorities to control, limit, or prohibit the transfer of data from one nation’s territory to another (hereinafter collectively referred to as "regulations").*

These regulations differ significantly in their approaches and levels of impact. Therefore, classifying and understanding each type of regulation is essential to evaluate their effects on international trade and governmental objectives accurately. Various classification systems have been proposed, such as those by the OECD, which categorizes them based on the degree of restriction, [3] or Martina Ferracane, who categorizes them by the "methods" of restriction. [4] This article proposes a new classification framework based on the "barriers" to trade created by these measures, including procedures, approval/authorization, technical standards, technical infrastructure, and "core input" in cross-border service production and distribution.

First, the group of regulations concerning procedures involves legal or regulatory requirements that compel entities to undertake additional administrative procedures and technical processes before data can be transferred across borders. For instance, there may be rules requiring the creation of a domestic copy of the data to ensure its availability even if transferred abroad, or provisions mandating the signing of contracts between the sending and receiving parties based on standardized templates prescribed by competent authorities to safeguard data when it leaves the national territory.

Second, the group of regulations concerning approval/authorization requires consent from relevant parties before data can be transferred. For example, Japan does not permit the cross-border transfer of personal data without the permission of the data subject (except in certain cases), [5] and many countries such as India and Vietnam require prior approval from government authorities for the transfer of sensitive or important data to mitigate security risks.

Third, the group of regulations concerning technical standards requires data to meet specific security standards. For instance, Singapore mandates that businesses ensure data is encrypted or undergoes security assessments before being transferred abroad, and the EU allows data transfers to countries with an equivalent level of protection according to the European Commission's "adequacy decision”. [6]

Fourth, the group of regulations concerning technical infrastructure requires businesses to invest in domestic technology and facilities to store or process data. A notable

example is Russia, which mandates that companies place data storage servers within the country. [7]

Fifth, the group of regulations concerning "core input" in the production and distribution of cross-border services emphasizes the essential role of data as a resource. As a result, government measures that effectively render this valuable resource unusable could create barriers in the production and distribution of services, especially for those operating across borders. This group typically includes requirements for data storage coupled with restrictions on transferring data permanently or for a limited period outside the national territory. For example, India prohibits the transfer of payment system data abroad. [8]

Due to the complex nature of these restrictive regulations, a single regulation may belong to multiple groups. When a regulation incorporates numerous elements, the level of trade disruption often increases, requiring careful consideration to ensure a balance between data protection and economic development.

III. The Impacts of Cross-Border Data Transfer Restrictions on Nations

Restrictions on cross-border data flows can have varying effects on different countries. This section analyzes the economic and legal impacts of regulations that limit cross-border data transfers.

A. Economic Impacts

Strict regulations on cross-border data transfers can enhance consumer and investor confidence, especially in sensitive sectors such as finance, healthcare, and technology. Additionally, requirements for local data storage in countries like China and India can promote investment in domestic data centers and technology infrastructure.

However, for other sectors, numerous studies have shown that regulations restricting cross-border data transfers have a significant impact on the foreign investment rate in a country. Specifically, regulations requiring technical infrastructure may lead to a substantial increase in investment costs for businesses, as companies must build their data centers. Additionally, regulations concerning technical standards may require companies to allocate physical resources to ensure data security before transferring it across borders. As a result, certain foreign businesses are deterred from investing in countries with "a range of complex data compliance requirements", which can slow down business growth and expansion, thereby reducing the foreign investment rate (FDI) in host countries. This highlights the economic incompatibility of restricting cross-border data transfers in trade activities, especially given the global scale of today’s technology-driven economy.

Quantitative analyses further illustrate the negative impacts of data restrictions on trade and investment. According to an econometric model by the Information Technology and Innovation Foundation (ITIF), a one-unit increase in a country's Data Restriction Index (DRI) corresponds to a 7 percent decline in trade volume for goods and services. The model further identifies countries such as China, Indonesia, Russia, and South Africa as experiencing greater foreign price pressures and reduced trade investment due to their stringent data restrictions. [9] Moreover, statistics from the World Bank and the Organization for Economic Cooperation and Development (OECD) indicate that countries could achieve an average increase of about 4.5 percent of GDP if they eliminate data restriction policies. [10] Another example is a 2014 study by the US International Trade Commission (USITC) showed that increasing digital trade barriers for foreign businesses would cause the US GDP to decrease by 0.1 to 0.3 percent, and the national wage coefficient to drop by 0.7 percent to 0.14 percent in digital-intensive sectors. [11]

B. Legal Impacts

Some of the current overly stringent regulations may be considered non-tariff barriers, potentially increasing the risk of the country facing legal challenges under international trade commitments. In principle, when countries sign international trade agreements, they are obligated to adhere to and fully implement the commitments outlined in those agreements. If a country's domestic laws are incompatible with these commitments, there is a significant risk of being challenged by other member countries of the agreement. The General Agreement on Trade in Services (GATS), which was established before the Fourth Industrial Revolution, is somewhat outdated, with many provisions not accounting for developments such as cross-border data flows. However, since all World Trade Organization (WTO) member countries (over 160 members) are parties to this agreement, the number of countries committed is vast, and thus, the likelihood of being challenged increases if countries do not comply with GATS principles and commitments, contrary to the WTO's trade liberalization goals. Currently, many regulations restricting cross-border data transfers globally may violate GATS, leading to the risk of disputes. For example, the Russian Federation's Federal Law 152-FZ (amended by Federal Law 242-FZ in 2014) in Article 12.1 states that cross-border data transfers are allowed only when the data is transferred to countries that are parties to the Council of Europe's Convention on the Protection of Individuals with regard to Automatic Processing of Personal Data or other countries that offer adequate protection for the rights of data subjects (related to technical standard regulations). This provision could lead to discrimination between countries that meet these data protection standards and those with different or no clear standards, thus potentially violating the Most-Favoured Nation (MFN) principle. Another example is in Article 2 of the same law, which mandates that foreign Internet service providers must establish necessary infrastructure or servers within Russia. This implies that Internet service providers must have a physical presence in Russia, changing the mode of cross-border service delivery (mode 1) to commercial presence (mode 3). As a result, although this cross-border data transfer restriction is not directly numeric, it could limit the number of Internet service providers (mode 1), and in some cases, this number could be reduced to zero. In the case of United States – Measures Affecting Cross-Border Gambling Services (US – Gambling Services), [12] the Appellate Body found that a "numeric quota" under Article XVI:2(a) includes restrictions

that, while not numeric in nature, possess characteristics of a numeric restriction [13] and thus could potentially constitute a violation of Article XVI:2(a). Another example is India's regulation requiring insured organizations to store insurance data within the country, as stipulated in the IRDAI (Insurance Record Keeping) Regulations 2015. This requirement can prevent foreign insurance businesses from collecting customer information, thereby hindering the provision of certain insurance and financial services. Such a regulation could potentially be incompatible with India's market access commitments under Article XVI:(c) concerning the insurance services sector in the country's GATS Schedule of Commitments.

Beyond GATS, cross-border data transfer restrictions are currently a key topic in trade negotiations and are included in numerous bilateral and multilateral Free Trade Agreements (FTAs). For instance, the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) includes binding provisions on data localization restrictions and cross-border data transfer requirements in Chapter 14 (E-commerce). Specifically, Articles 14.11 and 14.13 establish rules regarding the extent to which businesses can transfer and store data across borders, such as stipulating that "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", among other provisions. Notably, many other trade agreements also share similarities with the CPTPP, such as the Chile-Uruguay FTA in 2016, the updated Singapore-Australia FTA in 2016, and the U.S.-Japan Digital Trade Agreement (DTA) in 2019. Consequently, countries that are members of the CPTPP or other agreements with provisions on cross-border data transfers must adhere to these rules and align their national laws with their commitments. Failure to comply with these rules could lead to disputes that are difficult to resolve or avoid.

IV. Some Recommendations for Countries

In light of the current trend toward trade liberalization, regulations restricting cross-border data transfers may be subject to challenges under international agreements. In such cases, countries may invoke exceptions within the framework of these agreements to justify domestic regulations, such as the general exceptions and security exceptions under Articles XIV and XIV: bis of the General Agreement on Trade in Services (GATS), or exceptions related to government procurement and legitimate public policy as outlined in Articles 14.2 and 14.3, Chapter 14 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). However, to successfully invoke these exceptions, countries must demonstrate that their measures do not significantly affect the free flow of data between economies, do not incur substantial costs, and do not hinder the objective of trade liberalization in their trade commitments.

While exceptions may provide a justification, minimizing the risk of litigation remains paramount. One effective approach for countries to achieve the dual objectives of protecting cross-border data flows while maintaining compliance with their commitments is to engage in international cooperation mechanisms for data protection and cross-border data transfers. This would help establish common standards, thereby reducing conflicts between national regulations. Furthermore, countries should be encouraged to invest in domestic data storage and processing technologies and develop transparent monitoring and evaluation mechanisms to assess the implementation of cross-border data flow management measures.

V. Conclusion

While regulations restricting cross-border data transfers can help countries secure certain benefits, they also lead to significant negative impacts, such as reducing the competitiveness of businesses in the national economy, limiting the attraction of investment and research and development, and risking violations of international trade commitments like the General Agreement on Trade in Services (GATS) or other free trade agreements. To mitigate these impacts, the article suggests that countries should establish a legal framework in line with international standards, maintain healthy domestic data control, and create bilateral or multilateral cooperation mechanisms to ensure the safe flow of data and prevent legal disputes. By balancing national interests with global trade requirements, countries can protect data security while fostering innovation and international cooperation.

References

[1] López González, J., F. Casalini and J. Porras, "A Preliminary Mapping of Data Localisation Measures", *OECD Trade Policy Papers*, No. 262, OECD Publishing, Paris, 2022, available at https://doi.org/10.1787/c5ca3fed-en [accessed 10/01/2025].

[2] Chander, Anupam, Uyên P. Lê, "Data nationalism", *Emory LJ* 64(3), pp. 677-680, 2015.

[3] Casalini, F. and J. López González, "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris, pp. 16-24, 2019.

[4] Ferracane, Martina F., "Restrictions on cross-border data flows", *ECIPE Working Paper*, No. 01/2017, European Centre for International Political Economy (ECIPE), Brussels, pp. 3-6, 2017.

[5] Act on the Protection of Personal Information (APPI), article 24, available at https://www.cas.go.jp/jp/seisaku/hourei/data/APPI.pdf [accessed 09/01/2025].

[6] General Data Protection Regulation (GDPR), article 45(1), available at https://gdpr-info.eu/ [accessed 09/01/2025].

[7] Federal Law 242-FZ, article 2, available at https://pd.rkn.gov.ru/authority/p146/p191/ [accessed 04/01/2025].

[8] RBI Circular, available at https://rbi.org.in/Scripts/BS_CircularIndexDisplay.aspx [accessed 10/01/2025].

[9] https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost/ [accessed 06/01/2025].

[10] https://globaldataalliance.org/wp-content/uploads/2023/07/07192023gdaindex.pdf [accessed 07/01/2025].

[11] Rajat Kathuria, Mansi Kedia, Gangesh Varma and Kaushambi Bagchi, available at https://icrier.org/pdf/Economic_Implications_of_Cross-Border_Data_Flows.pdf [accessed 10/01/2025].

[12] United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services, available at https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds285_e.htm, [accessed 03/01/2025].

[13] Appellate Body Reports, "United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services", WT/DS285/AB/R, paras. 227, 238.