Conflicts and Coordination in Data Localization in China and International Trade Law

Hao Tao

University of Melbourne, Melbourne, Australia

httao1@student.unimelb.edu.au

Abstract. The purpose of this article is to explore the current status of cross-border data flows and data localization, with a focus on Chinese data localization measures. The article firstly outlines the importance of cross-border data flows and the national security and personal privacy challenges they pose, then it draws out in detail the necessity and different modes of data localization, as well as combs through the legal provisions of data localization in China, and then, through the analysis of China's data localization policy and the relationship with international trade law, it reveals a series of challenges faced by the data localization measures from China's perspective, and provides a certain theoretical foundation for the development of cross-border data flow, providing a certain theoretical foundation for the development of cross-border data flow.

Keywords: cross-border data flow data localization international trade law.

1 Introduction

In the wave of the digital age, the world has entered a new era of free flow of data, a process catalyzed by the rapid development of information and network technologies. With the explosive growth in the volume of data brought about by technological advances and the increasingly frequent flow of data across borders, the accuracy and efficiency of global trade and investment decisions have been significantly enhanced. However, this unimpeded data flow also poses unprecedented challenges to national security and individual privacy, forcing countries around the world to adopt measures to restrict data exit to find a balance between economic growth, national security and individual privacy protection. Among them, data localization measures, as a strategy to counter the challenges of data globalization, have become an important part of international data flow control.[1]

This paper could fill a significant gap, especially by combining China's domestic regulations, policies, and practices with international trade law standards. This could provide a unique perspective on the global and regional issues of data assets in international trade law.

Z. Zhan et al. (eds.), *Proceedings of the 2024 10th International Conference on Humanities and Social Science Research (ICHSSR 2024)*, Advances in Social Science, Education and Humanities Research 858,
https://doi.org/10.2991/978-2-38476-277-4_49

2 A New Era of Global Cross-border Data Flows

In the context of international trade law, data localization measures - such as restricting international transfers of data, requiring data to be stored locally, and subjecting data transfers to strict scrutiny - are often criticized as a new form of trade barrier. These policies are not only seen as an expression of trade protectionism, but also as an obstacle to the free flow of global trade.

There is no internationally standardized definition of the cross-border flow of data, but the basic concept involves the transfer of data across national borders from one place to another. The OECD gives a preliminary interpretation of this, stating that the cross-border flow of data implies the crossing of national borders. In the borderless world of the Internet and the intangible nature of data, the flow of data, unlike traditional trade in goods, does not require physical means to cross borders or receive customs approval. In short, as long as data can be accessed from one country by an entity in another country, it can be regarded as having crossed borders. Broadly speaking, cross-border movement of data includes not only transmission and offshore processing, but also covers situations where data within a country is accessed by entities outside the country.[2] For example, countries such as Australia and China have expanded their horizons to include personal data stored within their borders but accessible outside their borders.

The governance of cross-border data flows is an expression of national sovereignty, and countries around the world have developed their own cross-border data flow regimes based on their own national circumstances. However, at the global level, uniform rules are still missing, and different policies on cross-border data flows aim to maximize the protection of the legitimate rights and interests of the country and its citizens, but this also creates difficulties for other countries in terms of trade and law enforcement.

3 Data Localization Model

Data localization is not the same as complete data immobility. Even if certain data are not explicitly required to be stored locally, data localization can actually be achieved through a series of strict restrictions. The current understanding of data localization is not general, and can be divided into four main types: first, it requires all data (including copies) to be retained domestically, essentially forcing foreign companies to set up servers and data centres in their home countries; second, it allows for the transfer of copies of data outside of their home countries while storing copies in their home countries; the third type doesn't specify the location of storage, but requires that cross-border transmission of data The third type does not specify the location of storage, but requires the consent or permission of the data subject for cross-border data transfers; and the last type sets a series of criteria that can be met before data can be transferred outside the country, indirectly achieving a localization effect.[3]

Considering different classification criteria and drawing on relatively new literature,[4] this paper categorizes data localization into three modes: strict data localization

mode, substantive localization mode that restricts data exit conditions, and targeted localization mode. This classification aims to provide a clearer and more practical framework for understanding and analysing data localization policies.

3.1 Strict Localization Model in the Case of Russia[4]

The Russian government requires that all personal data generated domestically be stored domestically and prohibits cross-border access to, acquisition of, or processing of such data. This policy stems from the aftermath of Prism Gate and has been implemented through federal decrees and amendments to existing laws. Specifically, Russia requires that personal data be collected, recorded, organized, or accessed in domestic databases and that the Russian data protection authorities be notified of any use of these databases.

3.2 Substantial Localization Model Exemplified by the EU GDPR

The EU has implemented a substantive data localization model through the General Data Protection Regulation (GDPR) that does not directly require data to be stored on home soil, but effectively restricts the cross-border flow of data by setting stringent conditions for data to exit the country. The GDPR, through two mechanisms-sufficiency of protection determinations and safeguards The GDPR uses two mechanisms - adequacy protection determinations and security safeguards - to filter the conditions under which data is allowed to leave the country, and data can only leave if the receiving country provides a level of data protection equivalent to that of the EU.

3.3 Targeted Localization in the U.S. Case

Data localization requirements in the United States are clearly targeted and selective, with no uniform rules for the exit of personal data, but rather special restrictions for specific countries and businesses. This approach can be viewed as a trade barrier to specific targets. [4]

4 Connotation of Data Localization in China

4.1 Provisions for Data Localization in China

China's data localization measures are articulated in a series of laws and regulations, notably the Cybersecurity Law, the Personal Information Protection Law and the Data Security Law. These laws form the core of China's data localization policy, which aims to protect the security of personal data, safeguard national security, and promote the development of the digital economy.

China's data localization measures primarily emphasize data security reviews and export controls for specific types of data. The Data Security Law specifies that the state establishes a data security review system, and with reference to the relevant provisions

in the Measures for the Management of Data Security (Draft for Public Comments), it can be seen that important data should be assessed for security risks and reported to the relevant authorities for consent before being made available outside the country; and the Cybersecurity Law stipulates that specific types of data collected by operators of critical information infrastructures should be stored within the country, as well as a security assessment mechanism for the transmission of data outside the country.[5] The Cybersecurity Law stipulates that certain types of data collected by operators of critical information infrastructure should be stored within the country and provides for a security assessment mechanism for the transmission of data abroad. Similar provisions are contained in the Personal Information Protection Law.[6] The Data Security Law provides for export control of data related to the fulfillment of international obligations and the maintenance of national security.[7] The Personal Information Protection Law stipulates that personal information processed by state organs should be stored within the country, and if it is necessary to provide it outside the country, a security assessment should be carried out, and similar provisions are found in the Measures for the Security Assessment of Personal Information Exiting the Country (Draft for Public Comments)[8] and the Measures for the Security Assessment of Data Exiting the Country (Draft for Public Comments)[9]. In terms of specific implementation, China's data localization policy reflects strict controls on cross-border data transfers. In addition to the above laws, China has further refined its data localization requirements by issuing guidance documents and standards. For example, data exit review guidelines for different industries require data security impact assessments to ensure that data are protected outside of China to no lesser extent than required by Chinese law.

4.2 China's Model of Data Localization

Therefore, Chinese law requires that certain types of data be stored domestically, and it imposes clear restrictions on cross-border transfers, similar to the practice in Russia. Such measures reflect strict requirements for data control and are designed to protect the security of personal information and national security. At the same time, China's policy ensures that data is protected at the same level as in China by setting up a review and assessment process for cross-border data transfers, requiring companies to assess the risks of data transfers, obtain relevant approvals, and, in some cases, requiring contracts to be signed with offshore data recipients. These measures are similar to the requirements for cross-border data flows in the EU's GDPR and are designed to ensure that data is properly protected abroad.

China's data localization initiatives do not fit neatly into any of the models in the previous section, but rather combine elements of strict localization and substantial localization to form a hybrid localization model. This model reflects China's comprehensive consideration of personal data protection and national security, ensuring through laws and regulations that data is strictly managed domestically while also establishing specific conditions and requirements for cross-border data transfers. Therefore, it can be argued that China's data localization measures represent a new, customized model based on its specific national conditions and policy objectives.

4.3 Problems with Data Localization in China

Currently, China's rules on cross-border data flow are getting better and better, but in general, they are still in the early stages of legislation, and the international community's doubts about China's data localization are mainly focused on the blurring of the boundaries of data localization, and the risk of generalization in practice, which would go beyond the boundaries of the exceptions of the GATS regulations, and also be hindered in joining the negotiations of the CPTPP and so on. In the following, we will discuss the problems of China's data localization under GATS, which are in essence a conflict of laws between global data localization measures and the provisions naturally contained in GATS.

5 Compliance Analysis of China's Data Localization in Gats

China is precisely a member of the WTO, and some of the provisions of the WTO can provide for the analysis of cross-border data flow regulation, even if there is no relevant provision in the WTO agreement, the behaviour related to cross-border data flow may be adjusted by the WTO agreement in practice. Cross-border data flows, as a new type of business form, may be most relevant to cross-border data flows in the WTO package of agreements is the General Agreement on Trade in Services (GATS), as cross-border flows of data in general do not require the transfer of data with the physical carrier. Other WTO agreements may also apply, such as the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) when intellectual property rights are involved, or the provisions of the General Agreement on Tariffs and Trade 1994 (GATT 1994) if digital goods are involved.

Regarding the existence of data services in the services sector of GATS, CPC843 and CPC844 of the United Nations Provisional Rules for the Categorization of Products (CPC) deal with data-related services, and a number of subsectors under the "Communication Services" sector also deal with cross-border data-related services. The retrieval, reading and storage of data are categorized under computer and related services, and the transmission and exchange of data can be categorized under the "communication services" sector. Therefore, the movement and storage of data belong to trade in services, and the regulatory measures related to cross-border data movement are within the scope of adjustment of GATS. In the case of data processing services and database services under CPC 843 and 844, all data-related activities should be covered, even if they are not specified in the classification, if a member does not impose special restrictions at the time of commitment.[10]

5.1 China's Data Localization Measures and Obligations under GATS

Chinese Data Localization Measures and Market Access

Article 16 of GATS deals with market access obligations, directly ties into China's data localization provisions.[11] Under GATS Article 16, a Member State with market access commitments in a particular sector may not limit the number of service providers

or the total number of service operations unless the Member State's Schedule of Commitment Reductions contains relevant limitations and conditions. China may be in breach of its market access commitments under GATS if its legal provisions result in implementing a total prohibition on cross-border data flows or setting general bans on specific categories of cross-border data flows. In this regard, in order for China to comply with GATS, China must demonstrate that these measures are motivated by the need to protect individual privacy and cybersecurity, and that it has set aside corresponding restrictions and conditions in its trade in services commitments, thereby ensuring that these regulations are consistent with its GATS commitments.

China's Data Localization Measures and National Treatment

Article 17 of GATS provides for the obligation of national treatment, which is mainly concerned with the fact that, on the same conditions, the treatment accorded to a foreign country must not be less favourable than that accorded to a domestic country. In the Mexican Telecommunications Services case, the criteria for determining whether the national treatment commitment was violated were established: first, whether and to what extent the measure at issue was committed; The second is whether the measure treats the foreign service or service provider less favourably than similar domestic service or service providers. The question of whether and to what extent a Member State has committed to the disputed measure needs to be explored on a country-by-country basis, but commitments vary from country to country according to their own realities. China has made a "None" commitment to the cross-border delivery model under the national treatment obligation, where "None" means that no further restrictions can be imposed on the commitment made, i.e., no further restrictions can be imposed on foreign data service providers under the assumption that they are different from domestic data service providers.[12] Under this assumption, no further restrictions can be imposed on foreign data service providers that are different from those imposed on domestic data service providers. Here, the discussion focuses on the second question, i.e., whether the regulatory measures on cross-border data flows put foreign service providers at a disadvantage compared to domestic service providers. The key to determining whether a foreign service provider is disadvantaged is the subjective scope of application of its regulatory measures. A Member State does not violate the national treatment obligation if it expressly provides that the regulatory measures apply equally to domestic and foreign service providers, and vice versa.

China's data localization measures are designed to protect its citizens' data by adhering to certain privacy standards, and are equally applicable to domestic and foreign service providers, rather than being specific to a particular country or company. Therefore, I believe that China's data localization measures do not violate the national treatment commitments made by the relevant authorities under GATS in terms of purpose. Of course, in specific cases, the determination of the nature of a certain act may still be controversial, i.e., the legal provisions still need to be refined.

5.2 Chinese Data Localization and the Exception Clause

Even if in some cases China's data localization policies appear to conflict with the requirements of the Global Agreement on Trade in Services (GATS), China has the opportunity to rely on the exception clauses in GATS in its defines. These exception clauses, including the general and national security exceptions, are the result of a balancing act between trade liberalization and public policy objectives, and have been developed through amicable negotiations among member countries. Reference to the general exceptions in Article 14 of GATS and the national security exceptions in Articles 20 and 21 of GATT can provide a possible basis of legitimacy for China's data localization measures.

China's Data Localization and the General Exception

Article 14 of GATS allows member states to impose restrictive measures if specific conditions are met, which relate to areas such as the protection of public morals, the maintenance of public order, the safeguarding of human, animal and plant life and health, and the protection of individual privacy and data security. The provisions of China's data localization measures that require data to be stored within the country are designed to protect public safety, individual privacy and ensure data security, and are rightfully subject to the general exceptions in Article 14 of GATS. China's data localization measures reflect the goal of protecting public morals and order and are necessary to achieve those goals, and while technological alternatives such as encryption may exist, data localization may still be the most effective option in certain contexts. However, in order to reasonably apply this exception, China needs to ensure that its measures do not result in unreasonable discrimination or disguised trade restrictions in order to meet the prerequisites of the Introduction to Article 14 of GATS.

China's Data Localization and National Security Exception

Article 14bis of the GATS provides a national security exception, which gives member states autonomy in safeguarding national security. This includes restricting the cross-border flow of data in connection with military activities or other emergencies. China's data localization policy, which restricts the cross-border transfer of certain data for the protection of national security, is consistent with the spirit of the GATS national security exception. In the digital information age, I believe that the protection of personal information is particularly critical to national security, and China's efforts to guard against potential cyber threats and data misuse through its data localization measures are a reflection of the need for national security. Of course, in order to apply this exception, China needs to demonstrate that its measures are tailored to address specific security risks and are not a blanket ban on cross-border data flows, and that the measures are implemented based on the principle of good faith and are intended to genuinely protect the interests of national security, in order to avoid abuse of the security exception.

6 Data Localization and Regional Trade Agreements in China

Regional trade agreements, particularly the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP), represent the direction of global digital trade rules, emphasizing the growth of digital trade and the importance of the free flow of data. The CPTPP specifically sets a framework for practices that restrict the flow of data in order to prevent these restrictions from becoming trade barriers that affect the development of the digital economy.

6.1 Prohibition of Personal Data Localization in Principle

The CPTPP The regulation of cross-border flows of data provides for three levels: (1) Parties are required to allow data exits to flow between members.[13] (2) Localized storage of data is prohibited. (3) Articles 14.11.3 and 14.13.3 of the CPTPP provide for a "legitimate public policy objective" exception to localized storage for valid public policy goals, provided it doesn't lead to unfair trade practices or unnecessary equipment usage restrictions, aiming only to meet the stated objective.

The premise for the application of CPTPP data localization can be glimpsed in Article 14.2. CPTPP Chapter 14 is aimed at e-commerce, so the three layers of regulation described above only apply to cross-border flows of data between members in e-commerce, not to government procurement or information related thereto. A government's requirement to localize government-related data does not violate Chapter 14 of the CPTPP, even if a commercial subject is employed by the government to provide certain services related to government. The coverage of data localization does not include cross-border financial service providers.[14] Therefore, if a member requires a financial institution with a foreign component to localize certain data in such a way that the foreign shareholders are not made aware of it, that would not be contrary to the data localization requirements of Chapter 14 of the CPTPP.[4]

6.2 Application of the "Legitimate Public Policy Objective" Exception

Article 14.11.3 and 14.13.3 of the CPTPP introduce the exception of "public policy objectives", which is more ambiguous than the exception of public interest or national security in the GATS, and the CPTPP has not defined the specific content of "public policy objectives" in any annotation or public document. The CPTPP does not clearly define the specific content of "public policy objectives" in any annotation or public document. Based on the principle of interpretation of international conventions, this paper tries to interpret the meaning of "public policy objectives".[14]

First, "public policy objectives" may cover a wide range of objectives pursued by member States, such as data sovereignty, access to justice, protection of key industries, etc., which are not limited by the CPTPP, thus increasing the flexibility of member States to invoke this exception. Secondly, the CPTTP leaves it to the CPTPP expert group to judge whether the public policy objectives of a measure are "legitimate" in a specific case, and then a comprehensive assessment should be made based on the content of the measure and the text of each chapter of the CPTPP, to see whether the act

can reflect the common intention of member states. Finally, regarding the judgment of whether the measure exceeds the "necessary limit", the CPTPP uses "are required to" instead of "are necessary to" commonly used in the WTO. According to the practice of RTAs, developed country-led agreements tend to use "necessary", while "required" is used when there is an imbalance in the level of development among members. The use of "required" in the CPTPP may imply that a strict necessity test is not required. However, in the context of the CPTPP, which was designed to promote the free flow of data among members, "required" should be interpreted in a manner consistent with "necessary".[15]

In summary, the CPTPP provides broader exceptions than GATS, and the introduction of "legitimate public policy objectives" has increased the room for member countries to operate their data localization policies, but it has also undoubtedly increased the challenges faced by member countries in complying with the CPTPP provisions, and China's data localization measures are more difficult to invoke in the face of the CPTPP's requirements compared to the GATS provisions.[14] Compared to the GATS provisions, China's data localization measures will have a more uncontrollable situation when invoking the CPTPP provisions.[16]

7 Conclusion

Data localization is an important means of regulating cross-border data flows and is gradually attracting worldwide attention. While China's restrictions on personal data flows are intended to protect individual privacy and national security, they also have the effect of actually restricting trade due to the imperfections of the system. China has signed free trade agreements with more than twenty economies, and with respect to the WTO and CPTPP alone, China's data localization rules for cross-border data flows may be suspected of violating economic and trade agreements, and it may be difficult to invoke the relevant exceptions to defend against them.[17] Based on China's level of Internet technology development and the principle of national security first, China cannot give up its data localization policy in a short time, but it needs to clarify the boundaries of the application of data localization, and introduce relevant rules as soon as possible to fill the gaps and omissions in the practice, and to reduce the possibility of the data localization policy to be recognized as a trade barrier while adhering to China's security concept, meanwhile, I think it is even more important to have unified international standards.[18] At the same time, I think a more important point is that there should be a unified standard in the international arena. Just one country’s effort can not solve the disagreements and problems faced by the cross-border flow of data, and the problem must be solved in a unified international system. The issue of regulation of cross-border data flows, and in particular data localization as a general measure, remains worthy of deeper scrutiny.

Bibliography

1. W. Kuan Hon, H. (2017) Data Localization Laws and Policy: The EU Data Protection International Transfers Restriction Through a Cloud Computing Lens. Edward Elgar Publishing. https://doi.org/10.4337/9781786431974.
2. Zhang Monan, M. (2020) Cross-border Data Flow: Global Situation and China's Countermeasures. Open Leadership. 10.19625/j.cnki.cn44-1338/f.2020.0025.
3. Martina F. Ferracane, F. (2017) Restrictions on Cross-border Data Flows: A Taxonomy. ECIPE working paper. https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf.
4. Ran Fangqi, F. (2022) Research on Personal Data Localization from the Perspective of International Trade Law. East China University of Political Science and Law. 10. 27150/ d. cnki.ghdzc.2022.000948.
5. Cybersecurity Law of the People's Republic of China 2017, Article 37.
6. Personal Information Protection Law of the People's Republic of China 2021, Article 40.
7. Data Security Law of the People's Republic of China 2021, Article 24.
8. Measures for the Security Assessment of Personal Information Outbound of the People's Republic of China (Draft for Comments) 2021, Article 2.
9. Measures for the Security Assessment of Cross-border Data Transfer of the People's Republic of China (Draft for Comment) 2021, Article 2.
10. Jiao Huiping, H. (2023) Research on the Compliance of Cross-border Data Flow Regulation and International Economic and Trade Rules. Yunnan University of Finance and Economics. 10.27455/d.cnki.gycmc.2023.000482.
11. General Agreement on Trade in Services, Article 16.
12. China Services Commitments. https://www.wto.org/english/tratop_e/serv_e/telecom_e/telecom_commit_exempt_list_e.htm.
13. Comprehensive and Progressive Agreement for Trans-Pacific Partnership, Article 14.11.2.
14. Wang Juan, J. (2020) On the Digital Trade Rules of CPTPP and Their Impact on China. Shandong University. 10.27272/d.cnki.gshdu.2020.003917.
15. Zhang Ming, M. (2021) The Boundaries and Coordination of Data Localization Measures from the Perspective of International Trade Law: Taking the 'Personal Information Protection Law' as the Starting Point. 10.13519/b.cnki.nulr.2021.06.002.
16. Zhang Yu, Y. (2021) The Applicability Dilemmas and Their Mitigation of International Investment Protection Rules in the Context of the Rise of Data Localization Measures. Wuhan University International Law Review. 10.13871/j.cnki.whuilr.2021.04.012.
17. Li Yunsi, S. (2022) Research on Legal Regulation Issues of Cross-border Data Flows in Digital Trade. Gansu University of Political Science and Law. 10.27785/ d.cnki. ggszf. 2022.000206.
18. Lu Jia, J. (2022) Research on the National Treatment of Data under International Investment Law. Southwest University of Political Science and Law. 10. 27422/ d. cnki. gxzfu. 2022. 000232.