ISSN 2959-6130

# Cross-border Data Flows: Regulations in international digital trade and China's solution

**Hao Xu**

Guangdong University of Finance & Economics, 510320, China
E-mail: Carinaxuh@outlook.com

**Abstract:**

International digital trade is accelerating the speed of economic globalization and is becoming a new driver of economic growth. Data, as a key production factor, is ubiquitous in digital trade. This paper combines research on the topics of economy and trade in the digital era and further relates to cross-border data flows, to analyze regulations and governance of data flows in different economies, especially comparing the core elements involving cross-border data flows in regional agreements such as the CPTPP, the DEPA and the RCEP, to explore the rationality and necessity of various types of regulations. Besides, from investigating the specific development of the international community to discuss the real governance dilemma about strict regulation and fragmentation of data flows, to explore the solution to the problem of balancing cross-border data flows and risk prevention in international trade from legal regulation.

**Keywords:** International digital trade, Cross-border data flows, Global governance, Sovereignty and human rights

## 1. Introduction

Digital technology and smart manufacturing in the fourth industrial revolution have been widely used in various fields around the world, making digital trade a strong driving force for the growth of the global economy. According to McKinsey's forecasts, every 10% increase in data flows will promote 0.2% growth of GDP. By 2025, the contribution of global data flows to economic growth is expected to reach 11 trillion dollars. Cross-border data flows are intricately linked with cross-border digital services and products, serving as a fundamental supporting element in digital trade. However, data flows possess a dual nature, resembling a "double-edged sword". From a beneficial standpoint, as an intangible asset, cross-border data motivates digital trade to develop in resource sharing. From a challenging standpoint, it is difficult to bridge the gap about standpoints in regulations on data flows in different nations. Different legal frameworks result in data being unable to flow smoothly on issues related to national sovereignty, public security, personal privacy, enterprise development and so on. This affects international trade and even brings barriers and legal risks.

The scale of data flow ought to match the need of digital trade accordingly. Cyberspace Administration of China released data showing that the scale of the Chinese digital economy and data production is stably ranked as the second market in the global digital economy, but China's network data flows have a quite gap with some economies such as the United States and the European Union. In the construction of the double-cycle pattern, China has not yet formed a thorough legal system for data governance. On account of data flows being positively correlated with GDP, China should carefully consider in the rapid process of globalization: How can a relatively small scale of data flows make data elements work in digital trade? How to ensure the safety of data and digital trade when cross-border data flows? How can data resources be fully utilized to foster a deeper integration into economic globalization? Based on the co-existence characteristic of opportunities and inherent risks in cross-border data flows, this paper endeavors to categorize the concerns and divergences among various data flows rules, aiming to explore the global regulatory framework in such flows.

## 2. Status and challenges in cross-border data flows

For the international community's "stock competition", digital trade as a new driven force, takes data-driven as the core, rendering cross-border data flows a crucial topic. However, the international community has not yet formed a global set of rules about data flows, rendering it incapable of keeping pace with advancements in trade and data.

This is due to the intricate relationship between digital trade, which spurs data flows, and various regulations of national sovereignty and individual human rights in diversified regulations. Consequently, this poses numerous challenges.

## 2.1 Links between cross-border data flows and free digital trade

During the period of digital revolution, digitization of trade and trade of digitalize are booming developed, cannot be divorced data. Nevertheless, excessively free data flows will produce risks of trade across borders, while excessively restrictive data flows will bring out some shrinkage in trade.

With regard to the position on maintaining free digital trade, countries and regions, mainly represented by the United States, advocate to promote data flows freely. The Organization for Economic Co-operation and Development (OECD) promulgated Guidelines on Personal Data Privacy and Protection of Cross-Border Data Flows to harmonize privacy and personal information protection across nations, and issued Declaration on Transborder Data Flow calling nations to open up and accommodate data flows. Asia-Pacific Economic Cooperation (APEC) launched Cross-Border Privacy Rules (CBPR) to establish a certification mechanism of a "soft law" for free digital trade, which was formed and improved on the basis of the OECD. If enterprises join the organization, they will be able to freely transfer data across borders to each other once they are certified. In addition, the North American Free Trade Agreement (NAFTA) also formulated the relevant rules, symbolically combining data flow with digital trade, The United States-Mexico-Canada Agreement (USMCA), places a significant emphasis on digital trade, with a key objective of promoting the free flow of data among the participating countries while emphasizing the elimination of trade barriers. It firstly creates a "digital trade" section, emphasizing that neither party can restrict data flows of personal information unless it is for a legitimate public purpose and under non-discriminatory terms[1]. This perspective is to take a positive attitude and arrange bottom-line measures.

However, the risks posed by data flows to free trade in data cannot be ignored. Nowadays, for companies with businesses, suppliers or customers across borders, no one can afford to leave cross-border data transfers to gain competitive advantages or for normal business operations and therefore would be harmed by data flow restrictions for any nation in which it operates[2]. Taking a comprehensive view of data flows within the framework of digital trade: loose rules on data flows may facilitate the growth of digital trade, but they also heighten the challenges associated with risk control, which might jeopardize the developing countries' interests, while helping developed countries to implement global economic control with data. Strict rules on data flows are not conducive to the development of digital trade, but they can control risk with less difficulty, and developing countries, can avoid the data hegemony of developed countries[3]. Whether it is loose or strict, regulations in the international community on data flows pose challenges to national security, protection of business interests and individual privacy.

## 2.2 Connections between Cross-border data flows, data sovereignty and digital human rights

In the digital era, cyberspace, with its blurred margins and complex transmissions, challenges national sovereignty and people's private rights in terms of territorial principles and information privacy.

About data sovereignty, data, as a new form of national sovereignty evolution, is a new type of competitive resource for countries in cyberspace, economies in international trade have manifested pluralistic positions on cross-border data, which are mainly represented by data without borders and data-localization. The theory of data without borders was reflected in the early concept of cyberspace sovereignty, which emphasized that data should flow freely and independently. In *Law and Borders*, it is suggested that the Internet naturally has the characteristic of transcending sovereignty, and the Internet law is not suitable for national sovereignty and territorial regulations. With the increase in data risks and the need for national security, the "Snowden affair" was the trigger for the increased legal regulation of data localization, preserving data within countries or regions and treating data flows with restriction. From the perspective of analyzing the layered legal forms of cyber sovereignty, data-localization reaffirms that sovereign states have the right to control data within their borders, marking the Westphalian Sovereignty tradition returns to cyberspace[4].

The attitude of data sovereignty is reflected in the developing position of whether data is considered to affect sovereign security. The United States views data sovereignty as an element of the cooperation and competition among countries in the field of data, with an overall focus on the market approach, representing "data without borders"; the European Union intends to realize its own data sovereignty through the protection of data rights, focusing on fundamental rights, reflecting in the model that Sovereignty internalizes into the private rights, representing "data localization". Even though there has a conflict between the U.S. and the European Union's position on data sovereignty, both of them might embody "trade protectionism"

or “long arm jurisdiction”. For the position of the United States, if view data flows solely in terms of trade, essentially, it amounts to promoting American data position indiscriminately to other countries and regions. Such an approach appears to be ostensibly “neutral”, however, it actually threatens the rights and interests of regulations of data for other sovereign nations[5]. For the position of the EU, which has a negative impact on national or regional GDP and offsets productivity gains from major trade agreements, so that any gains from data-localization far outweighing losses[6].

The human right to data is reflected in whether the safeguarding of data and information is recognized as a fundamental human right. The Data Protection Directive, enacted by the EU emphasized to protection of personal data information and regulate data privacy laws within countries that have participated in the EU. It is feasible to identify elements that can reasonably be labeled as “European influences” and certain contemporary national data privacy laws beyond Europe indicate that “European standards” have exerted a significantly greater influence beyond the continent, and this influence is rising.[7]. The General Data Protection Regulation (GDPR), has proved to implement the adequate level of protection rule, also has changed clearly. This regulation insists essential principles, including controlling the flow of data for individuals and strengthening data supervisory for professional works on regions, leakage regulation, and sanctions. GDPR rose regulations’ standards about the protection of global data, This reform, to a large extent, is the most ambitious attempt so far to guarantee the individual rights of a generation in the digital field[8]. However, the United States, adapts an alternative model, places data protection within the framework of commercial interests, which is a typical model of industry self-regulation. Built upon the principle of “accountability,” this model presupposes the free flow of data as a prerequisite, requiring data holders to take reasonable and lawful measures to ensure the security of the data that maintain in their operations[9]. In essence, it emphasizes the facilitation of cross-border data flow to the maximum extent possible to accommodate the development of the economic and trade. Its attitude showed for the first time in the text was the Trans-Pacific Partnership Agreement (TPP), imposing binding commitments to ensure the free flow of data across borders within its e-commerce chapter. With human rights developing deeply, CBPR system signed by APEC, is similar to a combined version of the EU and America on regulations in data flows, but it is still inclines to the industry self-regulation model. Under the regulations of the CBPR, every economy member seeking to take part in the system ought to first nominate at least one privacy certification authority for participating in the Cross-Border Privacy Enforcement Arrangement (CPEA), and who will join in the CPEA should develop standards based on nine principles of the APEC Privacy Framework about the data flows across borders.

The different attitudes of States towards the human right to data also have different implications. Although the position of human rights to data has a variety of reasonability, it could also lead to unilateralism and long-armed jurisdiction, even worse to civilisational supremacy. Therefore, for the issue of data flows, more consideration are needed with regard of the human rights. China has paid attention to human rights protection to data in data flows, adhering to the guiding principle of putting the people first. Measures for Security Assessment for Outbound Data Transfer in China carries the spirit of the principle of proportionality through to the regulation, striving to strike a balance between data security and development.

Through the transition of novel ideas, products, technologies, and business models, info-globalization facilitates the flow and expansion of cross-border information and resources[10]. Indeed, relationships among data flows, data sovereignty and digital human rights in different countries or regions are often reflected in various legal regulations.

## 2.3 Conflicting legal regulations of cross-border data flows

Currently, the international community lacks a unified perception and regulation regarding cross-border data flows. Rules represented by the “US model”, the “EU model”, the “Singapore model” and the emerging “China model” reflect more clearly different positions. Consequently, from analyzing different models with a view to focusing on the impediments to the development of digital trade posed by the problem of global cross-border data fragmentation, drawing lessons from experiences and providing references for subsequent practice.

The first category is represented by the United States, which has long relied on industry self-regulatory mechanisms in the free trade of data, insisting on the priority of economic interests and supporting the free data flows maximally. Access to information and contacts in other countries through data flows so as to gain an upper hand in economic development. The second category is represented by the EU, emphasizing the priority of data privacy and national security, and imposes data flow restrictions and protections. One the one hand, the EU realizes this objective by making the data flows freely inside the EU as a legal principle, on the other hand, by distinguishing flows from the transfer of data outside. European data protection law channels data processing in many ways: it fabricates spaces within which personal data shall not

cross unless following ad-hoc paths and erects legal routes through which personal data might move[11]. The standard of data flows freely has been completed in GDPR, making rules more resilient. The third category represented by Singapore, seeking data flows in a dynamic balance that safeguards digital security and efficiency are concerned. To provide resources and security for personal and business data and reduce the threat of internet data risks, Singapore, together with Chile and New Zealand, signed the Digital Economy Partnership Agreement (DEPA), as the first regional agreement to make specific provisions for the digital economy, it states that each contracting party should allow the data flows in principle, prohibits the requirement for data to be stored locally, and build rules for the open sharing of data in order to achieve data-driven innovation. The fourth category is the developing countries represented by China, which mostly adepts the path of balancing data security protection and data flows. China released Global Initiative on Data Security and joined the RCEP to actively promote the global economy and engage in consultations on governance about data, responding to the complex positions of different economies. In 2022, after announced Data Exist Security Assessment Measures, together with Laws in the Cyber Security, the Data Security and the Personal Information, China has formed a data regulatory framework. Combined with Chinese characteristics of prior to carry and try, China has fully used Shanghai's advantages in the flow and trading of data elements, explored new mechanisms regarding data flows in digital trade.

As the main channel for upholding the multilateral trading system, the WTO, which was formed before the Internet era and has a large membership, was difficult to form a unified view on data flows. With new opportunities, Free Trade Agreement (FTA) have become an important venue for discussing data governance issues under the WTO framework.The CPTPP and the USMCA have basically agreed on data flows, supporting free data flows with the "principles and exceptions" model, setting a bottom line of limitations while paying attention to maximizing the data flows. Which means though data flow is an obligation, it is still inherently limited. As the world's first regional agreement on digital economy, DEPA emphasizes data as a key factor of production through in "Innovation and the Digital Economy", building rules on open data sharing to reach data-driven innovation. RCEP stands as the largest and most important free trade agreement in the Asia-Pacific region, in support of the premise that the parties have different requirements for the regulation of data, has also implemented "principles and exceptions". The difference is that it also adds specific exceptions, which is legitimate public policy objective, expanded the right of parties to safeguard data security, while also affording discretionary discretionary space for restrictions.

## 3. China's Programme in Data Flows

As a global digital power, China is at the centre of international trade. Focusing on Chinese proposal on regulations of data flows, it is not only necessary to improve relevant domestic legislation and strengthen risk control in this issue, but also should actively integrate into the international governance mechanism, complying with the trend of economic globalization and fostering the digital economic development.

For domestic regulations, China, grounded in the Data Security Law, China emphasizes the achievement of a dynamic balance between enforcing the legality of data and facilitating its open sharing.. Article 11 stipulates, "China actively carries out international exchanges and cooperation in the fields of data security governance, data exploitation and utilisation, participating in the formulation of international rules and standards related to data security, so as to promote the safe and free of data flows." In addition, China has gradually refined the scope of data flows and corporate compliance standards, with classified and graded management, which is to fill the data protection gap on the basis of individual privacy and national security, ultimately to regulate and promote data flows.

In international regulatory participation, China has actively engaged in competition and cooperation in the digital economy and trade. In 2020, China introduced the Global Data Security Initiative, aiming to regulate data through a multilateral lens, while balancing considerations of both security and development. It calls on the world to build a peaceful, open, shared and secure system of cross-border data flows. China also actively participates in FTA, exerts power in RCEP, participates in the discussion and formulation of rules for data, and applies for membership in CPTPP and DEPA, proactively benchmarking international high-standard economic and trade rules. In the future, China should balance the restriction and circulation of data in the complex and diverse data flows rules. The key is to build a compatible regulatory framework, which includes clarifying the scope of important data to define the "Negative List" for preventing national security risks, improving the cross-border accountability for protecting personal information rights and interests to ease pre-supervision pressure, and focusing on data access rights instead of data localization for upholding the jurisdiction of justice and enforcement[12].

## 4. Conclusion

With the rapid growth of digital economy, along with the

seamless cross-border flow of data, is evolving into a pivotal platform for international trade. We must be clear that data flows is a product of digital trade that combines reality and networks, human rights and sovereignty, regulation and development. Although economies have regulated data flows under the WTO framework and established multiple agreements to weaken the obstacles to this issue, it is clear that existing fragmented regulations meet the needs of a safe and free flow. Therefore, it is particularly important to establish a global regulation of data flows which not only requires WTO to play a key role, but also requires economies to be able to consider others' interests while considering themselves. For China, it should absorb and learn from parts of different data cross-borer regulation models that promote the development of digital trade about safeguard sovereignty and human rights, support global international organizations to carry out cooperation on data governance.

## 5. Reference

[1]Ding, X. D. (2023). "Rethinking Jurisprudence and Institutional Reconstruction of Cross-border Flow of Data --An Appraisal of the Measures for Data Exit Security Assessment." Administrative Law Studies (01): 62-77.

[2]Castro, B. D. and F. A. M (2015) "Cross-Border Data Flows Enable Growth in All Industries." Information Technology and Innovation Foundation.

[3]Ma, Q. J. and Li, X. N. (2021). "A Study of Regulatory Rules for Cross-Border Data Flows in the Context of International Digital Trade." international trade (03): 74-81.

[4]Liu, H. and Ye, K. R. (2020). "Layered legal forms of cyber sovereignty." Journal of East China University of Political Science and Law 23(04): 67-82.

[5]Yakovleva, S. and K. Irion (2020). "Pitching trade against privacy: reconciling EU governance of personal data flows with external trade." International Data Privacy Law 10(3): 201-221.

[6]Matthias, B (2017). "The Cost of Data Localisation: Self-Defeating Behaviour in a Recovering Economy (quoted)." Journal of Shantou University(Humanities & Social Sciences Edition 33(05): 44-47.

[7]Graham, G. (2012). "The influence of European data privacy standards outside Europe: implications for globalization of Convention 108." International Data Privacy Law (2): 2.

[8]Buttarelli G, (2016) "The EU GDPR as a clarion call for a new global digital gold standard", International Data Privacy Law 6(2),77-78.

[9]Zhang, D. (2018). "A brief discussion of legal standards for the cross-border flow of personal data." Journal of China University of Political Science and Law (3): 12.

[10]Ramzan, M., et al. (2023). "A step towards achieving SDG 2030 agenda: Analyzing the predictive power of information globalization amidst technological innovation-environmental stewardship nexus in the greenest economies." Journal of Environmental Management 335.

[11]González Fuster, G. (2016). "Un-mapping Personal Data Transfers." European Data Protection Law Review 2: 160-168.

[12]Liu, J.R. (2022). "Towards a Global Regulatory Framework for Cross-Border Data Flows -Fundamental Concerns and the China's Approach." Frontiers of Law in China 17(3): 412-439.

[13]Meltzer, J. P. (2015). "The Internet, Cross-Border Data Flows and International Trade." Asia & the Pacific Policy Studies 2(1): 90-102.

[14]Aaronson, S. A. and P. Leblond (2018). "Another Digital Divide: The Rise of Data Realms and its Implications for the WTO." Journal of International Economic Law 21(2): 245-272.

[15]Aaronson, S. (2015). "Why Trade Agreements are not Setting Information Free: The Lost History and Reinvigorated Debate over Cross-Border Data Flows, Human Rights, and National Security." World Trade Review 14(4): 671-700.

[16]Azmeh, S., et al. (2020). "The International Trade Regime and the Quest for Free Digital Trade." International Studies Review 22(3): 671-692.

[17]Ferracane, M. F. (2019). "Data flows and national security: a conceptual framework to assess restrictions on data flows under GATS security exception." Digital Policy Regulation and Governance 21(1): 44-70.

[18]Gao, F.P.- (2016). "International rules for the protection and utilisation of personal data: sources and trends." China Law Press.

[19]Johnson, D. R. and D. Post (1996). "Law and borders - The rise of law in Cyberspace." Stanford Law Review 48(5): 1367-1402.

[20]Portes, R. and H. Rey (2005). "The determinants of cross-border equity flows." Journal of International Economics 65(2): 269-296.

[21]Susan Ariel Aaronson, "Why Trade Agreements Are Not Setting Information Free: The Lost History and Reinvigorated Debate over Cross Border Data Flows, Human Rights, and National Security", 14 World Trade Review 671, 672 (2015).

[22]Svetlana Yakovleva & Kristina Irion, "Pitching Trade against Privacy: Reconciling EU Governance of Personal Data Flows with External Trade", International Data Privacy Law, Vol.10, No.3, 2020; Svetlana Yakovleva & Kristina Irion, "The Best of Both Worlds-Free Trade in Services and EU Law on Privacy and Data Protection", Eur.DataProt.L.Rev.,Vol.2,No.191, (2016).

[23]Voss, W. G. (2022). "Cross-Border Data Flows, the GDPR, and Data Governance." Vestnik Mezhdunarodnykh Organizatsii-International Organisations Research Journal 17(1): 56-95.