

A Study of China's Cross-Border Data System and Compliance of Multinational Enterprises in China

Jiawei He^{1,a,*}

¹Melbourne Law School, The University of Melbourne, Parkville, VIC 3052, Australia
a. jiawei.he4@student.unimelb.edu.au

**corresponding author*

Abstract: In the era of digital economy, states pay more attention to data as it is the key factor of economic development. And they have also made different actions to regulate cross-border data flow. Nowadays, due to the China's rapidly growing digital economy, more and more multinational enterprises are choosing to invest in China. Through evaluating multinational cross-border data regulatory system and focusing on the current status of China's cross-border data system, this essay summarizes China's laws and regulations about data supervision. On this basis, this essay provides specific data compliance advice for multinational enterprises operating in China. In order to better adapt to Chinese regulatory environment, companies should accurately understand data outbound security assessment mechanism and data localization principle stipulated by Chinese law. By establishing data classification and grading the management system, regular audit and risk assessment mechanism, and employee compliance training system, the enterprise can achieve both the digital trade business growth and cross-border data security compliance.

Keywords: Cross-border data flow, data compliance, data governance.

1. Introduction

Digitalization plays a major role in globalization, and today China's digital economy is growing rapidly. With around 1 billion Internet users, China's e-commerce market reached \$1.7 trillion in 2020, or 30% of the country's total retail sales. China now becomes one of the biggest digital economies in the world.[1]. With the development of China's digital economy and favourable policies, many multinational enterprises (MNEs) have come to China to invest. By the end of June 2024, foreign investors have cumulatively invested more than 1.2 million enterprises in China, including many multinational digital enterprises [2]. At the same time, nearly three-fifths of MNEs operating in China also intend to grow in the next 1-3 years, focusing on digital innovation to win new markets [3]. This shows that more and more MNEs recognize the huge growth potential of the Chinese market and hope to gain a place in the development of China's digital economy.

In the era of digitalization, cross-border data flow is a key element in the development of international digital trade and a problem that MNEs must face. Data carries a huge amount of information, which is often closely related to national security, personal privacy, data sovereignty, geopolitics and other factors, so countries continue to strengthen the cross-border data regulation based on the protection of national interests. However, different countries often have different regulatory rules for data, and such decentralized rules can easily lead to regulatory conflicts.

Therefore, for MNEs, building a data compliance system within a multiple data regulatory framework and steadily developing international trade business under the data compliance is an important issue in the digital economy era[4].

This essay offers practical compliance guidelines for MNEs in China by studying the current condition of China's cross-border data flow rules. There are two sections to the essay's primary body. The first part provides a definition of cross-border data flow and world trends in the regulation of cross-border data flow, reviews China's existing regulations on it. Within the framework of the Cybersecurity Law, the Data Security Law, the Personal Information Protection Law, and other supplementary laws and regulations, it examines the data localization concept and the data outbound security evaluation process in China. The second part is based on the relevant regulations on cross-border data flow in China in the first part and provide relevant suggestions for the compliance of cross-border data flow of MNEs in China, including systems, mechanisms, employee education.

It is important to study China's cross-border data system and data compliance of multinational enterprises in China. With the background of increasingly frequent cross-border data flows, the study in this essay provides theoretical references for balancing data protection and free flow of data. By analyzing the compliance strategies of MNEs in China, this paper provides a useful supplement to the corporate compliance management theory in the context of globalization. At the same time, this essay provides specific data compliance suggestions for MNEs in China and provides practical guidance for them to adapt to the Chinese regulatory environment, which can not only reduce legal risks, but also help companies improve operational efficiency so as to better conduct cross-border data business.

2. Overview of China's data cross-border system

2.1. Definition of cross-border data flow

The Organization for Economic Cooperation and Development (OECD) initially introduced the idea of cross-border data flow in the Guidelines on the "Protection of Privacy and Transborder Flows of Personal Data" published in 1980 (hereinafter referred to as the 'Guidelines'). According to the "Guidelines," it is the transfer of personal information across national boundaries [5]. This means that in the early days of data flow, data only included personal information. The idea of cross-border data flow has expanded in diversity as the digital economy has grown. Today, data includes not only personal data but also corporate information, business secrets and other forms of digital data. 'Cross-border' includes two situations: one is the act of transferring data from one jurisdiction to another; the other is that even though the data has not crossed the border, entities in one jurisdiction can access and process data in another jurisdiction. 'Flow' is divided into three stages: data generation and collection, data transmission, and data reception.

In short, cross-border data flow refers to the process in which digital data such as personal information and corporate information are collected, transmitted, and received between different legal jurisdictions through technical means such as the Internet and cloud services, and are therefore subject to different legal supervision.

2.2. World regulatory trends

At present, most countries have developed their own cross-border system of data flow regulation and they are different from each other, which brings great difficulties to the data compliance of MNEs. This essay focuses on the cross-border systems of the European Union and the United States, and compares them with the system in China, in order to providing compliance references for MNEs in China.

With regard to cross-border data flow between EU member states and non-EU member states, the EU has taken a contrasting attitude, exhibiting a regulatory pattern that is 'loose inside and strict outside'. The cornerstone of EU data protection is the General Data Protection Regulation (GDPR), created by the EU. It controls the movement of data both inside and outside the EU. For member states, the EU promotes the free exchange of data among its member states. All member nations are subject to the GDPR, which unifies the framework for data protection. This uniformity ensures that data is uniformly protected, eliminates barriers to data transfer within the EU, and thus promotes the economic development of the EU. For non-member states, the EU tightens data flow restrictions and improves personal data protection [6]. First, the adequacy principle is used to assess whether third countries have adequate data protection levels and list whitelist countries. If a country is deemed "adequate" (such as Japan, Canada), personal data from the EU can flow freely to that country without additional approval and authorization. Secondly, in the absence of 'adequacy' requirements, the EU also provides some mechanisms that allow companies to transfer data under appropriate safeguards. These include Standard Contractual Clauses (SCCs), which are pre-approved contract templates for transfers between different companies. It gives the data subject the right to access, rectify and delete the data. At the same time, It calls on data receivers to implement suitable technical and organisational actions safeguarding personal data security. It also includes Binding Corporate Rules (BCRs), which are a type of data flow regulation applicable to multinational companies. Companies that implement BCRs must ensure that all subsidiaries involved follow consistent data protection measures that comply with the GDPR when cross-border data flows.

Control of cross-border data flow in the United States differs greatly from that in the EU. Because the US lacks standardized laws governing cross-border data movement, companies must abide by a complicated web of state laws and industry-specific rules. Companies find it more challenging to stay in line with cross-border data as a result. The U.S. cross-border data flow regulation is mainly reflected in the agreements signed between itself and other countries or economies. Due to its dominance in the digital economy, the US consistently adds clauses allowing for "free cross-border data transfer" to the accords. The EU-US Data Privacy Framework (DPF), which was agreed in 2023 by the US and the EU, enables US companies to prove that they adhere to the DPF's standards by themselves. In essence, it provides exemptions for US companies from the application of GDPR, promoting the free flow of cross-border data between the EU and the United States [7]. In addition to formulating bilateral or multilateral agreements, the United States has also expanded the scope of data regulation through "long-arm jurisdiction". The Clarifying Lawful Overseas Use of Data Act (CLOUD), passed by the US in 2018, allowed US law enforcement to access user data that US companies had stored on overseas servers[8]. This means that U.S. law enforcement agencies have law enforcement powers both at home and abroad, which has been criticized by many countries as a serious impact on their data sovereignty.

2.3. Existing regulations on cross-border data flow in China

The following three laws primarily represent China's existing policies on cross-border data flows: the Personal Information Protection Law, the Data Security Law, and the Cybersecurity Law. At present, China has formed a data governance and cross-border data flow framework with these three laws as the core and other supporting regulations.

The concept of data localization and a data outward security assessment process were first put forth legally by the Cybersecurity Law, which went into force in 2017. The law's Article 37 expressly mandates that operators of vital information infrastructure keep private data and significant information created and gathered in China [9]. The operator must perform a security assessment before transferring data across borders. This assessment's goal is to ascertain whether the data transfer will jeopardize social interests, national security, or other people's legitimate rights and interests. And

the Data Security Act and the Personal Information Protection Act have inherited this requirement and made more detailed provisions. Article 21 of the Data Security Law stipulates that “important data” must be classified and managed in a hierarchical manner, and requires that when cross-border data flows, important data should be stored locally first and undergo security assessments[10]. Article 40 of the Personal Information Protection Law also explicitly requires that personal information processors must follow the principle of data localization when processing personal information, especially when it involves cross-border transmission of user personal information and undergo security assessments [11]. This assessment must confirm that the receiving nation's protection level is in line with Chinese legal requirements. Supporting specifications such as ‘the Measures for Security Assessment of Data Cross-Border Transmission’, ‘Guidelines for the Submission of Security Assessment of Data Cross-Border Transmission (First Edition)’, and ‘Guidelines for the Submission of Security Assessment of Data Cross-Border Transmission’ further clarify the regulatory body, assessment objects, and implementation process of security assessment of data cross-border transmission.

Combined with the laws and regulations mentioned above, it can be seen that the objects of storage under the principle of data localization in China include personal information (e.g., sensitive personal data or personal data involving over 100,000 individuals) and important data (e.g., key data about economic growth, public priorities, and national security). And the storage of data must be classified and comply with security requirements. Specifically, to prevent unwanted access or data leakage, enterprises must first implement organizational and technical safeguards for data storage, such as access control, data encryption, and data backup. Secondly, enterprises need to classify different types of data, and the storage method should be consistent with their sensitivity. For example, the storage of sensitive personal information may require a higher level of protection measures, such as data isolation and high-intensity encryption. When storing data locally, companies must first classify and evaluate data to identify which data needs to be stored. This process must ensure all data that meets the local storage requirements is processed and stored within the country.

In terms of the China's data outbound security assessment mechanism, it adopts a method that combines prior assessment with continuous supervision, and self-assessment with institution assessment. Mainly through the national and local Internet Information Offices to conduct overall supervision of enterprises. These mechanism includes the following processes: First, the data that needs to be evaluated is picked out based on data classification. Then the company needs to assess the risks of data outbound flow by itself, including a comprehensive risk analysis of the nature of the data, the legal environment of the recipient, the security of the data transmission method, etc. Secondly, after completing the assessment, enterprises need to prepare the declaration materials, including data exit assessment forms and data transmission agreements. The materials will be submitted to the Internet Information Office for review. And the Internet Information Office will conduct a comprehensive assessment of the legality, reasonableness and security of the data, which includes the necessity of the data processing activities, the level of data protection of the receiving party, and the sensitivity of the transmitted data. If the assessment result fails, the enterprise is required to rectify and re-declare; if the assessment passes, the enterprise can carry out legal cross-border transmission of data [12].

3. Compliance advice for multinational companies on cross-border data flows in China

3.1. Establish a data classification and management system

Companies must set up a data classification and management framework in order to comply with Chinese law's requirements for the data localization principle and the data outbound security assessment process.

First, companies should develop data classification and grading standards based on their specific business needs and compliance requirements to ensure compliance with Chinese laws and regulations. Personal information and vital data are the two main categories covered under China's existing cross-border data flow regulations, but the meaning of vital data is not entirely clear [13]. To improve data protection, MNEs can further refine data classification based on relevant laws. According to the nature, source and purpose of the data, companies can classify the collected data into personal information, business data, financial data, government data, public data, etc. At the same time, companies should classify data into different security levels according to sensitivity, importance and the harm of leakage.

Second, different data levels require different data protection strategies. For example, highly sensitive data (involving national security, sensitive personal information, core business secrets, etc.) should be stored securely using powerful encryption technologies. For general data, only basic security measures need to be formulated. Meanwhile, hierarchical access control measures are implemented for different levels of data. Data access rights are allocated according to employees' responsibilities and permissions to ensure that only authorized employees can access certain important data, thereby enhancing the security of data storage [14]. In addition, different types of data will correspond to different regulatory requirements. Data classified as "important data" and "personal information" should be stored locally. Other data can be transferred across borders after security assessment.

3.2. Improve Regular Audit and Risk Assessment Mechanisms

Regular data audits and legal risk assessments by multinational organisations are important steps to ensure data compliance and can help them improve data compliance at both the technical and legal levels. Through audits, companies can identify technical issues in data operations and improve data management strategies; through risk assessments, companies can identify legal risks to data policies, update compliance policies and reduce the likelihood of data leakage and breaches. Since most MNEs in China lack knowledge of relevant Chinese laws and national conditions, they can choose local audit and legal teams with experience in data security compliance. These teams are familiar with Chinese laws and practices and are able to implement and manage risk mitigation strategies [15]. The audit team conducts a systematic inspection of the implementation of enterprise data classification, security control measures, data protection mechanisms, etc. Through technical means and regular monitoring. It assesses whether there are technical problems in the enterprise's data processing process, data protection measures, and the actual operation of cross-border data transmission. The legal team reviews the enterprise's data files and procedures, assesses the data compliance legal risks faced by the enterprise, and provides legal advice to assist the enterprise in formulating and updating its internal data compliance policies [16].

Improving regular audit and risk assessment system have few benefits: First, by regularly evaluating the company's data classification and grading management system, it can ensure that the company dynamically adjusts data classification and management strategies based on changes in laws, regulations and business needs. Secondly, by auditing the data storage system, it can ensure that technical measures such as data encryption, access control and firewalls meet security requirements. Furthermore, by real-time monitoring of the enterprise data transmission system, it can ensure the security of data during data transmission and check whether the transmitted data meets the security assessment requirements. Finally, by reviewing relevant data documents and data policies, it can ensure that data processing and transmission agreements between multinational corporations and their partners comply with the law. At the same time, it can also ensure that companies improve their internal policies, e.g., when the risk of data leakage is high, companies should develop contingency plans to prevent data leakage.

3.3. Strengthen employee compliance training

MNEs in China should enhance employee training to ensure that all workers involved in data processing are fully aware of China's data protection regulations and cross-border transmission requirements. Through regular training and compliance awareness education, employees should be made more aware of their responsibilities when processing data.

First, it should provide basic training for relevant employees, including the basic knowledge of data security and explanations of China's major data laws and regulations. This will enable employees to understand how to identify and respond to data security risks in daily work based on China's national conditions and clarify the processes and requirements for data compliance. Secondly, employees in different departments face different data compliance risks due to their jobs. Therefore, multinational companies need to provide specialized training based on different jobs. For example, for data storage workers, special training on data classification and grading should be provided to ensure that they master the correct method of storing data; for data transmission workers, special training on data security assessment should be provided to ensure their compliance in cross-border data transmission. Meanwhile, companies need to regularly update employees' training to ensure that they understand the latest laws, regulations and internal policies. In addition, MNEs should also train their employees on how to respond to data leakage. This can be done by combining explanations of scenarios with simulations to improve employees' ability to respond to emergencies.

4. Conclusion

In order to better develop international digital trade, multinational companies must fully implement data compliance. This essay helps MNEs understand the current data governance regulatory environment in China and provides practical compliance recommendations, including data classification management, regular audits, risk assessments, and compliance training. These recommendations can help them minimise legal risks and thus improve data security and operational efficiency. However, this essay focuses on the compliance of MNEs in China, but does not fully explore their two-way compliance issues in data importing and data exporting countries. Therefore, future research can focus on exploring the conflicts between Chinese laws and those of other countries in data supervision and provide relevant suggestions for MNEs on how to comply with data in a conflicting regulatory environment.

References

- [1] McKinsey Global Institute (2021). *The Future of Digital Innovation in China: Megatrends Shaping One of the World's Fastest Evolving Digital Ecosystems*. Retrieved from <https://www.mckinsey.com/featured-insights/china/the-future-of-digital-innovation-in-china-megatrends-shaping-one-of-the-worlds-fastest-evolving-digital-ecosystems>.
- [2] UN Trade and Development (2022). *How digital multinationals are transforming global trade and investment*. Retrieved from <https://unctad.org/news/how-digital-multinationals-are-transforming-global-trade-and-investment>.
- [3] PricewaterhouseCoopers (2022). *Multinational corporations in China: Capture market and growth opportunities*. Retrieved from <https://www.pwccn.com/en/research-and-insights/belt-and-road/hotspot/mncs-in-china-apr2022.html>.
- [4] Ao mei, Zijun pan.(2024) *Governance Models, Challenges and Compliance Approachs for Cross-Border Data Compliance of Enterprises*. *Intelligence Theory and Practice*, 47(6), 60-67.
- [5] OECD (2024). *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*. Retrieved from https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.
- [6] European Union. (2016). *General Data Protection Regulation (GDPR)*. Retrieved from <https://eur-lex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN>.
- [7] *Data Privacy Framework Program (2023). EU-U.S. Data Privacy Framework (DPF)*. Retrieved from <https://www.dataprivacyframework.gov/EU-US-Framework>

- [8] United States Congress. (2018). *Clarifying Lawful Overseas Use of Data (CLOUD) Act*. Retrieved from <https://www.congress.gov/bill/115th-congress/house-bill/4943>
- [9] See Article 37 of Chinese Network Security Law.
- [10] See Article 21 of the Chinese Data Security Law
- [11] See Article 40 of China's Personal Information Protection Law
- [12] See Chinese Data Export Security Assessment Measures
- [13] Gabriela Kennedy & Joshua T. K. Woo (2023) *China Proposes Easing of Cross-Border Data Controls*. MAYER BROWN. <https://www.mayerbrown.com/en/perspectives-events/publications/2023/10/china-proposes-easing-of-cross-border-data-controls>
- [14] Eryurek, E., Gilad, U., Lakshmanan, V., Kibunguchy-Grant, A., & Ashdown, J. (2021). *Data governance: The definitive guide*. O'Reilly Media, Inc.
- [15] Christopher Tan. (2024) *The Great Cyberwall: Navigating China's Cross-Border Data Laws*. B.C. INTELL. PROP. & TECH. F. <https://sites.bc.edu/iptf/>. 169 Id.18.
- [16] Sargiotis, D. (2024) *Data Governance: A Guide*. Springer Nature Switzerland, 445-466.