

Research on the International Coordination Mechanism of Data Jurisdiction and Corporate Cross-Border Compliance in the Context of the Digital Economy in China

Aijia He^a

Tianjin University of Finance and Economics, Tianjin, China

^aheaijia929@163.com

Abstract

Cross-border data flow has become the fundamental link for promoting the development of global digital trade in the era of the digital economy. Since there is no international coordination mechanism for data jurisdiction, China cannot join the world system of data governance. This paper takes the international coordination of data jurisdiction as its subject, defines key concepts, analyzes conflicts and causes in China's cross-border data flow jurisdiction, and based on international practices, proposes a path for building China's international data jurisdiction coordination mechanism by "adhering to core principles-building a three-dimensional coordination mechanism-improving supporting measures." Finally, it addresses enterprise compliance needs by proposing compliance strategies for different markets and enterprise sizes to reduce the cost of cross-border compliance, help China maintain data sovereignty, and engage in deep participation in global data governance, thereby promoting high-quality development of the digital economy.

Keywords

Data jurisdiction, international coordination mechanism, cross-border data flow, corporate compliance.

1. Introduction

Data serve as the foundation for the new-era productive forces in the digital economy. Digital technology will be used to achieve the digital transformation of the entire economic system; as a result, the world's industrial and trade chains are being reshaped into digital forms, and cross-border data flow will serve as the foundation for supporting digital trade and cross-border e-commerce cooperation, thus promoting all-around development of the global digital economy. Therefore, the volume of cross-border data flow has been on the rise gradually. According to the *Digital China Development Report* (2022) released by the Cyberspace Administration of China, the amount of data generated in China in 2022 reached 8.1 ZB, accounting for 10.5% of the world's total and ranking second in the world (Cyberspace Administration of China, 2022). Cross-border data flows are now necessary to promote the development of global trade and technological progress at present. At present, the world's system of data governance is still relatively fragmented. Due to different ideas of data sovereignty, regulatory priorities and national interests, the countries have built various systems for data jurisdiction. For example, the United States has a model of personal jurisdiction and long-arm jurisdiction, and the European Union employs an adequacy decision system. The above ways are not in line with China's current data jurisdiction system. Based on the above, the problems of cross-border data flow and the domestic regulatory system are mainly due to the lack of an effective coordination mechanism for international data jurisdiction in China. Therefore, we need to find a way for the company to avoid such conflicts in cross-border data processing. At present, there are no

standardized international rules on data jurisdiction, and China's current data regulatory system lacks an effective and seamless coordination mechanism with recognized international rules; thus, uncertainty exists in the application of these rules and compliance problems have arisen for Chinese enterprises involved in cross-border data transfer. It will be difficult to form a stable sense of compliance, and thus the healthy and orderly development of the digital economy will be impeded[1-2].

In light of the above deficiencies, China has now been pursuing two feasible paths that are equally flawed. First, the company will be motivated to comply with the cross-border data rules in the CPTPP through a *compliance system*. However, the cross-border data rules of the CPTPP still advocate for the "free flow of data principle with exceptions", set a high compliance bar, and thus imposed significant time, labour and technical costs on enterprises, making compliance less feasible. As a result, the compliance cost does not justify the corresponding benefits; therefore, it cannot be applied to the actual needs of Chinese companies of different sizes, and the pressure for compliance is even higher for small and medium-sized enterprises (SMEs). The second is to build pilot projects in free trade zones. The construction of free trade zones in Shanghai, Hainan and other places offers a path for exploring cross-border data flow in accordance with China's national conditions. However, the pilot models in these areas still have shortcomings in terms of development positioning and implementation path, do not meet the practical data cross-border needs of large and small Chinese enterprises, especially startups, and fail to fully meet the cross-border data compliance requirements for SMEs compared with the mature experience of data governance interaction between China and the EU.

Therefore, many Chinese enterprises have encountered compliance problems in the course of cross-border operations. Although there are probably some reasons related to foreign relations, the primary cause is that these enterprises do not fully comprehend the data-sovereignty regulations in the country where they operate. At the same time, the legal systems in various parts of the world also have different ideas about data rights, regulatory models and enforcement mechanisms, etc.; thus, enterprises find it challenging to identify and address cross-border data compliance risks. Therefore, Chinese enterprises engaged in overseas expansion need to adapt better to the data governance systems of host countries, take into account the rising trend of including privacy rights in the overall system of human rights, and adjust their compliance practices according to local regulatory requirements under the dual considerations of data security and the right to privacy. To achieve this end, the mechanisms of China's international cooperation in data jurisdiction also need to be strengthened further. Therefore, improving the system for international cooperation and studying feasible compliance paths for enterprises in China's participation in global data governance have become pressing issues.

2. Dilemmas and Causes of China's Cross-Border Data Flow

2.1. Three Major Dilemmas in China's Cross-Border Data Flow

2.1.1. Conflicts of Multiple Jurisdiction Rules

Different countries have taken different paths in developing the area of cross-border data flows and data jurisdiction. These are because of their different concepts of sovereignty and regulatory priorities, etc. Therefore, there are frequently conflicts due to an uneven application of rules and varying scopes of jurisdiction. The United States generally favours a model that promotes the free flow of data and uses long-arm jurisdiction. Under the primary legal basis of the Clarifying Overseas Use of Data Act (CLOUD Act), US authorities can compel US companies and other foreign parties that have received data of US citizens to disclose such data under certain circumstances. The European Union is also more focused on privacy and the protection of fundamental rights. The EU's adequacy decision mechanism will determine whether a non-

EU country has reached an equivalent level of data protection. If the standard is not met, then for cross-border transfers, safeguards will be required; otherwise, it will not be needed. China has set up a regulatory system for data protection and constructed multiple tiers of data. The kindness and necessity of the data differ; therefore, so do their regulations. Although these models are based on valid policy reasons, they create practical problems for enterprises engaged in cross-border business activities by doing so. Jurisdictional division of China will likely lead to an increase in compliance costs. Chinese internet companies operating in Europe may need to comply with both China's Measures for Security Assessment of Cross-border Data Transfer and the EU's General Data Protection Regulation (GDPR) at the same time. In practice, this may mean that core data remain subject to domestic restrictions, complete the domestic security assessment procedures, and at the same time, meet GDPR obligations related to data subject rights and assessments for high-risk cross-border transfers. The compliance process will be relatively slow and costly. Different regulatory standards may also be applied to the company, and it will be difficult to meet all of them at the same time.

2.1.2. Fragmentation of Regional Data Governance Rules

Most of the existing international data rules are based on regional agreements, and there are significant differences in their main provisions; thus, a fragmented rule system has been formed. The first few major world regional data frameworks are the CPTPP, the *Digital Economy Partnership Agreement* (DEPA), the Regional Comprehensive Economic Partnership (RCEP) and the EU-US agreement. *Data Privacy Framework*, and all of them differ significantly in their core institutional arrangements.

On the problem of cross-border data flow, the CPTPP explicitly does not impose mandatory data localisation requirements and requires member countries to allow the cross-border transfer of data unless such restrictions are necessary for "legitimate public policy aims" or "basic security interests" (Bi, 2025). Although the RCEP generally supports the free flow of data, it still provides for exceptions based on "basic national security interests", and furthermore, the RCEP stipulates that such security exceptions are unilateral in nature and are not subject to the proportionality rule (Tang, 2025). At the same time, the DEPA has adopted a "modular + regulatory sandbox" model and can choose various modules according to the actual circumstances of the participating economies; some flexibility for data-related innovation is also provided. The division of these regulatory systems requires Chinese enterprises to adapt their compliance strategies continuously during overseas expansion. For example, the enterprise in the Asia-Pacific region needs to develop two or three separate data governance plans for different areas and thus reduces supply chain efficiency and increases compliance costs. Finally, this results in a cost-benefit imbalance that further hinders the construction of a unified digital common market (Tang, 2025)[3-5].

2.1.3. Institutional Dilemmas in Resolving Cross-Border Data Disputes

At present, there is no unified system for cross-border data jurisdiction disputes in the world, and therefore, the enforcement and dispute resolution mechanisms in different countries vary. The lack of coordination is thus a source of some uncertainty for Chinese enterprises under the scope of multi-jurisdictional enforcement. On the one hand, there is no general-purpose framework for dealing with conflicts of data jurisdiction, and many disputes have been settled by unilateral enforcement measures. For example, the United States has at various times extended long-arm jurisdiction to conduct data-related investigations on Chinese companies and imposed corresponding penalties. At the same time, most existing international dispute resolution systems, such as the WTO's, also cover only the traditional areas of trade in goods and services and intellectual property rights. They are not suitable for data-related jurisdictional disputes, and there are no special adjudicatory bodies or procedural rules for such problems. *Microsoft v.* is a typical case. The US law enforcement agency has asked

Microsoft to disclose the user data stored in Ireland; however, Ireland has refused on the grounds of the EU's *General Data Protection Regulation* (GDPR) and the principle of data sovereignty (Xu, 2022). The dispute went on for several years, and Microsoft was in a bad way legally. The root of the problem in such cases is a clash between the national data protection system and the authority of jurisdiction, not a violation of WTO trade rules. Therefore, they do not fall under the scope of the WTO dispute settlement mechanism. Chinese enterprises also have the same compliance problems for their overseas operations due to different national data laws and multiple jurisdictions. In the absence of an institutional system to coordinate and handle disputes over cross-border data issues, firms will be unable to use such institutions for risk management, and thus the cost of compliance will be higher and operating uncertainty will be more pronounced[6].

2.2. Analysis of the Dilemmas of China's Cross-Border Data Flow

First of all, the current global data governance system is still largely based on the United States and the European Union, and the participation and voice of developing countries are relatively weak. The two sides have created a self-referential system to act as leading forces for new rules in the world of data governance. In fact, the Design of these rules may have certain interests. The United States has been applying the extended-arm jurisdiction to expand its “digital space”, and citing national security reasons, has frequently taken unilateral enforcement measures against Chinese enterprises. TikTok's U.S. regulators have issued a fine for the cross-border transfer of U.S. user data due to data security risks. In short, this is an extension of the US's data jurisdiction through long-arm enforcement, and the rules for data are increasingly used for geopolitical ends (Xu, 2022). In response, the European Union has extended its regulatory power through the “Brussels Effect” of GDPR and applied its domestic rules abroad; as a result, the division of global data governance has deepened (Liu, 2023). At the same time, both the U.S. and the EU are actively promoting regional or plurilateral data arrangements to form relatively exclusive rule blocs and thus deepening regulatory fragmentation. Given the above circumstances, Chinese enterprises have been in a defensive posture and are compelled to comply with multiple, and at times contradictory, rule systems, resulting in both compliance risk and increased costs. TikTok is a typical case that demonstrates this phenomenon and has had an impact on cross-border data flows (Xu, 2022). Therefore, the US and the EU operated under two relatively independent jurisdictional logics. The United States did not give significant weight to the cross-border character of data flow and instead imposed unilateral jurisdictional standards by expanding the scope under the guise of “children's privacy protection”. The European Union, on the other hand, introduced compliance obligations through a system such as the requirement for an “adequacy decision” under the GDPR. Neither party considered China's differentiated and tiered regulatory system or the actual compliance capacity of Chinese enterprises. The two different systems will not be unified; therefore, compliance with one system cannot guarantee compliance with the other, and failure to comply will result in penalties imposed by the host country[7-9].

Secondly, there has been a lack of development in the system of overseas cooperation and poor coordination among various systems. China's cross-border data jurisdiction coordination mechanism is still in the early stages and has several defects. At the level of many sides, China has failed to promote rule coordination in important platforms such as the UN and the WTO, and thus has had a limited impact on the world's discourse on data governance. Alignment with the high-standard agreements of CPTPP and DEPA has not been realised at the regional level. In addition, the pilot schemes of free trade zones tend to focus on high-end industries and large enterprises, with relatively complex compliance requirements and insufficient lightweight pathways for small and medium-sized enterprises, leaving a coverage gap for startups (Ma Zhongfa, 2024). China has promoted the “Belt and Road” Initiative and signed many bilateral

cooperation agreements, but the whole scale of these initiatives is still relatively small. In particular, there are still no targeted cross-border data coordination or judicial assistance mechanisms with major economies such as the United States and the European Union, and thus the efficiency of regulatory mutual recognition and legal cooperation is relatively low (Tang, 2025). In the TikTok case, the US pressure to access data and the resulting fine occurred without a special bilateral judicial assistance mechanism, so Chinese authorities and the company had few institutional paths for effective response and were left in a relatively passive position[10-11].

In addition, the relatively weak compliance capability of Chinese enterprises is also one of the reasons for these problems. Many enterprises have not established all-encompassing compliance systems in line with foreign rules. The three main reasons are that there is no knowledge of the regulatory differences, a weak compliance system, and a failure to use the existing coordination mechanism. The TikTok fines have shown the same shortcomings again. Firstly, many enterprises, especially small and medium-sized ones, do not have an independent compliance office or stable information channels; as a result, they are unable to learn about changes in foreign regulations and enforcement conditions in time. Second, compliance is often dealt with in a reactive way rather than proactively, and comprehensive-process risk control systems have not been established. Third, the company has not used the available international mechanisms for compliance reduction. The APEC Cross-Border Privacy Rules (CBPR) certification system and the EU data protection certification mechanism are devices to lower cross-regional compliance costs, but many enterprises have not yet adopted them and have not realised any cost reductions.

3. Practical Experience in International Coordination of Data Jurisdiction

3.1. Multilateral Coordination Practices

3.1.1. United Nations *Global Digital Compact*

In 2024, the UN has signed the Global Digital Compact (GDC) and made some progress in data governance. Establish the basic ideas of data sovereignty equality and classified, tiered data flow. It promotes the value of security and development, advocates inclusive and equitable governance, provides a foundation for multilateral rules on state-to-state dispute settlement over data jurisdiction, and so on. Compact must also respect the data sovereignty of other countries, avoid the abuse of “data hegemony” and “long-arm jurisdiction”, and propose differentiated regulation according to the sensitivity of the data to provide strong protection for core data while promoting the free flow of general data. The foundation of the practice logic for coordination is a tiered classification system. The Compact will also provide a platform for the voices of developing countries in the world of data governance and help build an all-inclusive, equitable and rational system of global data governance. Multilateral practice offers a foundation for China to defend its data sovereignty and promote a model of classified jurisdiction recognised internationally. In the construction of the foundation and spirit for governance, it also provides a basic direction for establishing a global coordination mechanism that balances data security and the digital economy, asserts national sovereignty, and serves the global public interest.

3.1.2. APEC Cross-Border Privacy Rules (CBPR) System

The APEC-led Circular Economy Package is a typical case of multilateral soft-law cooperation that has set uniform standards and built a system of mutual recognition to reduce overlapping compliance obligations for enterprises. This system has privacy protection rules, a certification mechanism and regulatory cooperation mechanisms, and is based on the “one certification, multi-country recognition” design concept. After passing the CBPR certification, the enterprises in the participating economies have had their privacy protection standards recognised by all

other parties in the network and are thus exempt from individual compliance certifications in each country. The United States led the design and promotion of the CBPR, introduced a market-oriented approach and minimum regulatory digital governance concept, and thus included it in the Asia-Pacific regional rule system. Compared with the EU's "mandatory rule export" under GDPR, the soft-law model of CBPR is more acceptable to economies at different stages of development in the Asia-Pacific region, and thus indirectly extends the reach of US data governance. CBPR certification may be required for U.S. companies to enter the Asia-Pacific market and improve their competitiveness in digital trade (Tang, 2025). APEC has formed a regulatory cooperation and dispute-settlement mechanism for the cross-economy. The company's regulatory office will mediate the compliance dispute and thus reduce the cost of handling it. The U.S. practice fully demonstrates that regulatory mutual recognition is an effective way to reduce compliance costs and provides a direct-application soft-law coordination model for China in constructing a multilateral coordination system to alleviate the compliance burden on small and medium-sized enterprises (SMEs)[12].

3.2. Regional Coordination Practices

3.2.1. EU-U.S. Data Privacy Framework (DPF)

The EU-U.S. The Data Privacy Framework (DPF) in 2023 is a typical case of resolving cross-border jurisdiction conflicts. By adopting a "substantial equivalence" test for privacy protection levels, the system can meet the goals of regulatory mutual recognition while introducing some differentiation or layering in governance to address the long-standing problem of transatlantic data flow friction (Liu, 2023). Although the agreement was signed by the EU and the United States, it has not been limited to these two countries; rather, it has spread to other parts of Europe as well and is therefore often referred to as a type of regional cooperation. In short, based on the "adequacy decision", the EU believes that the level of data protection in the United States meets its own standards for the *General Data Protection Regulation* (GDPR). Thus, the original contradiction between the EU's adequacy-based data transfer system and the US model of extraterritorial "long-arm" jurisdiction has been eased. Under the "UK extension of the EU-US" Data Privacy Framework, UK entities are permitted to transfer personal data to U.S. organisations certified under the framework without needing to implement additional safeguards such as transfer risk assessments (Ji, 2024). At the same time, the Data Privacy Framework (DPF) introduces a multi-layered governance system and is supervised by the US Department of Commerce and supervision by the EU *Data Protection Board*. It will also provide individual judicial remedies, and together the two will offer a more foreseeable and organised compliance path for businesses. The two-way recognition and multi-level supervision system of this regulation will provide China with an institutional reference for constructing a data-jurisdiction coordination mechanism with the EU and resolving compliance conflicts that may arise from overseas expansion by enterprises. The model offers a reference for the change from regional to bilateral cooperation. For example, in 2025, China and Germany signed a memorandum of understanding on cross-border data flow cooperation, established a bilateral regulatory exchange and cooperation mechanism, explored data standard alignment and regulatory mutual recognition, balanced enterprise compliance convenience with data security protection, and became the first practical application of the DPF model (Cyberspace Administration of China, 2025). The above provisions will help the enterprise address the compliance problems in Europe during its expansion[13-15].

3.2.2. DEPA Regulatory Sandbox Mechanism

The new regulatory sandbox mechanism by DEPA will provide a safe environment for the trial of innovative data services (Ma, 2024). Thus, the new-era enterprises will avoid a compliance trial-and-error process and gain the benefits of technology. By November 2020, 73 regulatory sandboxes had been set up in the 57 jurisdictions around the world, and both developed and

developing countries were actively involved. The regulatory sandbox mechanism at DEPA directly addresses the shortcomings of China's free trade zone pilot projects in meeting the needs of startup enterprises, and flexible regulation is now being fully implemented. The member countries can provide regulatory space for data-innovation enterprises in some areas, and at a limited extent, allow the company to experiment with new cross-border data flow models and technologies in a sandbox environment without strict compliance with the existing regulatory regime. Based on the test results, the regulator will adjust the rules and achieve a dual-track development of regulation and innovation. The DEPA is a module system that can be adopted at different times according to the level of development for many regulatory systems; thus, the burden of harmonisation is reduced. This flexible regulatory approach provides some institutional design ideas for China to optimise its free trade zone pilot areas and build a light-touch compliance channel for startups. In fact, the Shanghai Free Trade Zone has been exploring "secure computing sandboxes" for related services, and the accumulated experience can also provide a reference for the development of data regulatory sandboxes to further promote the transition of China's full-process data regulation to post-event and mid-event monitoring and unlock the value of data elements (Ma, 2024).[16-17]

3.2.3. CPTPP "Principles + Exceptions" Rule Model

The CPTPP has a "principles + exceptions" rule system for cross-border data flow and offers a very good practical reference for China to harmonise with high-standard regional rules by balancing the freedom of data flow and national data security. This model does not require data localisation and, in general, facilitates the free flow of personal information and non-sensitive business data; however, it has clearly outlined exceptions for national security, public order, the right to privacy of individuals, and protection of critical infrastructure, and under these exception conditions, member countries can still exercise data jurisdiction and take measures such as data localisation. Given that there are some exceptions, this system will still meet the demands of high-standard international norms and data-sovereignty claims from multiple countries simultaneously. China can apply the model of the CPTPP to adjust the relevant exceptions for "essential and important data" in line with the CPTPP, meet the basic requirements of the agreement, ensure national data security, and reduce the compliance burden for domestic enterprises under the high-standard regional rules.

3.3. Bilateral Coordination Practices

3.3.1. U.S.-UK Data Access Agreement

In 2019, the United States and the United Kingdom signed a *Data Access Agreement on electronic data* for serious crime investigations, which was the first cross-border electronic data forensics bilateral agreement based on the U.S. model. Cloud Act. Set up a normal procedure for cross-border data forensics in both countries under this agreement. The agreement will resolve jurisdictional conflicts and address the inefficiency of the old way of cross-border criminal enforcement data requests; it will also provide China with a model for building a bilateral judicial assistance system and handling issues of U.S. long-arm jurisdiction. The agreement specifies the scope and procedures for data requests, guarantees the rights of data subjects, sets limits on exceptions to cross-border data access, and prevents "borderless cross-border data retrieval" through the exercise of long-arm jurisdiction.

In accordance with this agreement, if a UK law enforcement agency requires the data stored by a US company, it can directly submit a request to the US. Department of Justice via official channels. Review and confirm; then, the Department of Justice will require the company to comply. Therefore, it can avoid the problems of multi-tiered traditional judicial assistance and improve enforcement efficiency. More importantly, the institutionalized government-to-government mechanism will provide enterprises with a clear path for compliance and avoid the problem of legal conflicts between the two countries for these enterprises; thus, it can be

effectively circumvented. Microsoft, Amazon, and Facebook (Meta) are examples of U.S. tech companies that have established specialised cross-border data forensics compliance processes in practice according to this agreement, only responding to official directives from the U.S. and UK Departments of Justice, and rejecting non-agreement data access requests from unilateral law enforcement agencies; thus, compliance conflicts that previously arose from the need to comply simultaneously with U.S. Cloud Act and UK data protection law (Caixin, 2022; Global Security Wire, 2025). In the absence of a unified data governance system globally, bilateral agreements can be employed to define the responsibilities for law enforcement, standardize assistance obligations, and limit the scope of jurisdiction to reduce cross-border data jurisdiction disputes through a balance of security and efficiency.

In light of the above provisions, when a UK law enforcement agency requires access to data stored by a US company, it can submit a formal request directly to the US authorities through the established channel. Department of Justice. Based on the above findings, the Department of Justice will issue a binding order requiring the relevant enterprise to rectify the violation. This way does not require the several levels of the traditional mutual legal assistance system and will be more efficient. The institutionally established government-to-government channel will also provide stronger compliance signals for the company. It will be simpler for the company to meet the differing legal requirements in various areas around the world, so the compliance problem will be reduced to some extent. Microsoft, Amazon, Meta (Facebook) and other large US technology companies have begun building cross-border data access and forensic compliance workflows based on this system in practice. They generally only respond to official requests from the competent authorities in the U.S. or the U.K., and refuse data-access demands made by unilateral enforcement bodies outside the agreement. This way will prevent earlier compliance conflicts caused by the concurrent operation of the U.S. *CLOUD Act* and UK data protection regulations (Caixin, 2022; Global Security Wire, 2025). Generally speaking, this case shows that in the absence of a unified global data governance system, specifying the enforcement authority, standardising the assistance obligations, and drawing jurisdictional boundaries through bilateral agreements can be employed to address cross-border data jurisdiction conflicts in practice and achieve a balance between security concerns and operational efficiency

3.3.2. *China-Singapore Free Trade Agreement (CSFTA) Data Cross-Border Cooperation*

In 2008, China and Singapore signed the *China-Singapore Free Trade Area (CSFTA) Agreement*, and as a result, cross-border data transmission between the two countries was legalised. In 2024, both sides have upgraded the free trade agreement and added data cooperation to the core of the bilateral economic and trade rules. The implementation of this improved agreement also shows that the data cross-border flow cooperation between China and Singapore is a successful case of harmonising bilateral rules with compliance empowerment for SMEs. In 2019, the China-Singapore International Internet Data Dedicated Channel was officially launched in Singapore, and as one of the main data cross-border infrastructure projects, it entered operation. This project will use technology to provide a secure and convenient support for cross-border data flow and directly connect Western China with Singapore. Reduce the delay in transmitting data across borders and achieve real-time data interaction for cross-border e-commerce, financial technology and cloud computing, etc. The channel is a whitelist-entry type and only allows enterprises that have passed the security test to use it. This first established a channel + whitelist control model (Cyberspace Administration of China, 2019; China-Singapore (Chongqing) Strategic Connectivity Demonstration Project, 2021). The construction of this facility will be a new addition to the cooperation area between China and Singapore for information and communication. At the same time, this localised cooperation model organically integrates the three core experiences to provide a replicable and scalable practical template for bilateral data cooperation between China and the countries of the Belt and Road Initiative. On

the one hand, a whitelist for cross-border data flow is established, and according to the classification and tiering of data sensitivity, general data are designated as the primary focus within the whitelist for easy flow. At the same time, it will recognise the whitelisted enterprise qualifications and cross-border data security assessment results provided by the other party to establish a cross-border mutual recognition system for data protection evaluation results. Whitelisted enterprises will be exempt from repeated security audits and reduce the cost of compliance for data export.

4. Pathway for Constructing China's International Data Jurisdiction Coordination Mechanism

4.1. Adhering to Three Core Principles

First, the basic requirement for international cooperation and the objective of the UN Charter are aligned with the principle of data sovereignty equality. In accordance with the principles of data sovereignty and equality, fully respect the regulatory requirements established by other countries under their national conditions, keep core data in China within Chinese jurisdiction, firmly reject the abuse of “data hegemony” and “long-arm jurisdiction”, and in terms of legal theory, this principle is consistent with the fundamental norm of sovereign equality in international law, as well as the legislative objectives of China's Data Security Law and Personal Information Protection Law. In practice, it can be connected to the systems of “classified and tiered governance” and “data export security assessment” established by the two laws. On the other hand, the United States has used its national security rationale to extend its long-arm jurisdiction over Chinese enterprises, employing tools such as the *CLOUD Act* and the Foreign Investment Risk Review *Modernization Act*, and even mandated that companies provide core data stored in China (Xu, 2022). Thus, it will violate the rule of equal data sovereignty and contradict China's governance position of opposing hegemony and promoting a multilateral order. Therefore, we should advocate for this idea in our cooperation abroad to protect China's data sovereignty and promote the construction of an all-weather fair global data governance system.

Second, the conflict between the requirements for security and development is also a problem in data governance. It will meet the demands for national data security and help the company reduce compliance costs and improve the convenience of data sharing. Data classification and tiered management are generally used to realise this goal, and different rules apply to jurisdiction and cross-border transfer. At the national level, specify the scope of the core data, essential data and general data more clearly (Tang, 2025). Due to security reasons, some data on national defence and critical infrastructure will be subject to strict restrictions on cross-border transfer or may be banned entirely. Some necessary data will be secured beforehand and only exported under supervision. Generally, business data and non-sensitive personal information will be included in the reduced scope of cross-border transfer and thus permitted for transfer. The company can, on its own side, align the compliance plan with different kinds of data more precisely to achieve more efficient cross-border data use in a secure regulatory environment.

Finally, in light of multilateralism, it is proposed that the system of global data governance should be based on multilateral platforms, such as the United Nations and the World Trade Organization, and inclusive and broadly representative rules can be developed through consultation rather than being divided into “rule islands” formed by exclusive regional arrangements. This is in line with China's goal of a world government based on “broad consultation, joint contribution and shared benefits”, and it will also help enhance the participation of developing countries in global data rules. At the level of the state, China should actively participate in discussions on cross-border data flows in multilateral platforms such as

the UN and WTO, take a more proactive role in agenda-setting, and promote an international rule system that better serves the common interests of all countries. Given the new national multilateral strategy, at the enterprise level, they can participate in rule consultation through industry associations and cross-border cooperation channels, and share the practical needs and compliance experience of Chinese companies in cross-border data governance. For instance, at the multilateral forum of the *United Nations Global Digital Compact* consultations and WTO e-commerce negotiations, enterprises can present real-life compliance cases for cross-border data flow and provide empirical support to strengthen and improve the rules of the multilateral system.

4.2. Constructing a Three-Dimensional Coordination Mechanism

Based on the above ideas and integrating the practical experience of multilateral, regional and bilateral coordination, China should build a “multilateral-regional-bilateral” three-dimensional coordination mechanism to construct a complementary and coordinated system at all levels to address the conflict over data jurisdiction.

First of all, at the level of multilateral cooperation, China should take the initiative to promote the implementation of the Global Digital Compact in the UN system, clarify the principles of “data sovereignty relativity” and “necessity testing” (Tang, 2025), confirm that all countries enjoy equal data sovereignty, and require that cross-border data regulatory measures meet the criteria of legitimacy, necessity and proportionality. China can also actively participate in the round table talks at the WTO on the rules for electronic commerce, promote the spirit of non-discrimination and transparency in cross-border data flow through multilateral consultations, and implement the principle of multilateralism. In line with the global Data Security Initiative, China will build a community with a shared future that benefits all and ensures common security. A platform for data governance cooperation among developing countries should be built to coordinate the demands of developing nations and advance the cause of China's rising global status.

Second, at the level of regional coordination, China should be in line with high-standard international rules and strengthen regional economic cooperation; thus, it needs to speed up the alignment of DEPA rules and introduce flexible governance mechanisms, such as modular design and regulatory sandboxes, to promote mutual recognition of data protection certifications among member countries. At the same time, China can use pilot zones such as Shanghai and Hainan to explore the CPTPP's “principles + exceptions” core rules and refine the exceptions for data localisation to provide a solid institutional foundation for China's future full membership in the CPTPP (Bi, 2025).

Finally, a bilateral coordination mechanism will be established to provide high flexibility and strong specificity in handling jurisdictional conflicts in some countries, and thus enterprises can carry out targeted overseas expansions. China should adopt different strategies according to the characteristics of the rules in a partner country. On the one hand, based on the model of China-Singapore cross-border data cooperation, China can sign bilateral data flow agreements with Belt and Road Initiative partner countries to build a bilateral cross-border data regulatory cooperation platform. At the same time, China can hold periodic talks with the United States and the European Union on some of the differences between them, such as data access and privacy protection. Drawing from the U.S.-U.K. Agreement *Data Access Agreement* and the EU-U.S. Data Protection Framework: Build a dual-track conflict resolution system in China that integrates judicial assistance and corporate compliance, offering enterprises an explicit path for conformity.

4.3. Improving Supporting Guarantee Measures

A regular-running three-dimensional coordination system needs a number of supporting institutional arrangements. At this time, China needs to strengthen the construction of its own system and increase its participation in the international mechanism to ensure that the coordination framework can be realised effectively.

First of all, the system of laws in our country provides the institutional basis for participating in overseas data-jurisdiction cooperation. Therefore, China needs to further improve its own legal system to align better with the rules of the international system in this area. For example, in light of the core requirements in the CBPR, DEPA and CPTPP frameworks, revise the *Data Exit Security Assessment Measures* to specify the scope, procedures and standards for assessment more clearly, and add an “international rule alignment clause” to enhance consistency. In accordance with the *Data Security Law*, the relevant authorities will work with sector regulators to establish and continuously update catalogs of important data across different industries and domains, specify identification criteria, responsible regulatory departments, and rules for cross-border transfer to provide enterprises with a clear legal reference for compliance (Li, 2025). At the same time, further strengthen the guarantees for the protection of data subject rights and improve other provisions in the law to enhance its overall international compatibility.

Second, construct an independent early warning mechanism for disputes at home and join efforts to formulate the rules of international commerce, thereby adding another option for risk response and remedy for enterprises. The construction of the cross-border data flow coordination mechanism should be carried out through industry associations and legal service institutions to establish a cross-border data jurisdiction dispute early warning platform covering major outbound markets, monitor law enforcement dynamics and rule changes in real time, and issue risk warnings in advance. Additionally, China can take the initiative to participate in the development of the rules for international dispute settlement, promote multilateral platforms such as the WTO and the UN to establish specialised digital trade and data jurisdiction dispute resolution institutions, and strengthen domestic enterprise remedy channels. A cross-border data compliance legal aid mechanism should be established, and digital trade courts in domestic courts can be used to link domestic and foreign remedies effectively. Finally, the countries that have not signed judicial assistance treaties can send special “judicial assistance letters” to request an expedited response and assistance from the other party (Swire & Hemmings, 2016) to provide a practical path for dispute resolution and ensure the security of the digital economy.

5. Corporate Cross-Border Data Compliance Strategies

As the main subjects of cross-border data flows, enterprises’ compliance practices are necessary to avoid cross-border operational risks and ensure long-term stable development; at the same time, they also provide support for the actual implementation of China’s international data jurisdiction coordination mechanism. Given the above reasons, enterprises should make full use of the international coordination system to reduce compliance costs and provide a practical case study for improvement at the lower level of this system. More specifically, the four directions are as follows: compliance risk assessment, differentiated compliance strategies, effective use of international coordination tools, and strengthening the construction of the internal compliance system..

5.1. Compliance Risk Assessment

First, establish an all-encompassing and scientific model for jurisdiction risk assessment in the company. The categories and tiers of the model include core data, important data, and general

data, specify the destination of the data flow, and differentiate between high-protection and low-protection countries as its main attributes. It can help identify the problem of jurisdiction conflict. For instance, when transferring data to the EU, it is necessary to meet the relevant requirements of the GDPR; for the United States, one must observe the security demands of the *Cybersecurity and Infrastructure Security Agency* (CISA) and any restrictions under the Preventing Foreign Adversaries from Acquiring American Data Act (PADFA) (Tang, 2025). Second, the company can learn from the case of TikTok and face a secondary fine for failing to adapt in time to changes in US and EU regulations. Therefore, the company will add a new rule-tracking mechanism dynamically. Set up a rule-monitoring team in the company to track all multilateral, regional and bilateral agreements under the three-dimensional coordination mechanism, as well as the legislative changes in the host countries; pay particular attention to the enforcement trends of the FTC on children's data protection and updates to the review standards for cross-border data transfers by the Irish Data Protection Commission (DPC). At the same time, the company can work with the industry association to raise problems such as rule misalignment or uneven enforcement of standards at the national regulatory department, and thus provide practical data for improving the system of international cooperation.

5.2. Differentiated Compliance Strategies

Based on the target market and scale of the company, establish differentiated compliance plans to reduce compliance costs and lower compliance risks for the company.

First, in line with China's "security-first + classified jurisdiction" model, enterprises need to meet the requirements for data classification and tiering management. The core data must be stored locally, and after a security assessment of the data exit, standard contract filings and personal information protection certifications should be carried out in accordance with relevant regulations to meet the requirements of domestic regulations (Cyberspace Administration of China, 2026).

Secondly, for the EU's "privacy protection + territorial jurisdiction" adequacy decision system, enterprises can apply for GDPR certification or sign standard contract clauses to ensure that the level of data protection meets the EU's requirements for "adequacy". They should also set up an effective data subject rights response mechanism to handle compliance obligations under the right to erasure and data portability reasonably well.

Finally, the U.S. "free flow + long-arm jurisdiction" model can be used voluntarily to join APEC CBPR certification and employ the multilateral mutual recognition system for cross-border data retrieval risk reduction. At the same time, they should also be in line with the Cloud Act and regulate the storage and cross-border transfer of data. TikTok can use its model of storing US user data on domestic US servers to avoid the compliance risks of long-arm jurisdiction. Apple has announced the construction of a data centre in China to meet the requirements of China's data localisation laws and regulations, and will ensure that this data is subject to Chinese governance. Apple promised not to build a backdoor and still kept possession of the encrypted keys in the US. A year later, Apple moved the iCloud account keys for China to Chinese territory in line with regulations from the Chinese government (Andrew Keane Woods, 2018). ByteDance (TikTok) also released the "Texas Plan" to adapt in the US. Cloud Act and TikTok Act data localisation and security review requirements by establishing a U.S. data security joint venture (USDS), storing U.S. user data on Oracle's U.S.-based servers, and backing up in Singapore. The company introduced US capital and set up a board with a US majority, and prevented Chinese entities from accessing the original US user data. Thus, TikTok was able to meet the requirements of U.S. jurisdiction and was not compelled to sell its U.S. business (Dongfang Caifu, 2025). These foreign-invested enterprise cases show that, in order to enter the market and avoid legal penalties, these enterprises need to meet the data-sovereignty requirements of the destination countries.

6. Conclusion

With the continuous development of the digital economy and the large-scale application of artificial intelligence technology, many problems have gradually appeared in cross-border data compliance for Chinese enterprises. China should follow the three main ideas of data sovereignty, equality and mutual respect; balance security and development; give priority to multilateralism; build a three-dimensional international data jurisdiction coordination mechanism under the leadership of multilateralism, coordinated at the regional level and supplemented by bilateral talks. Participate in building the multilateral rules system, comply with the high-standard regional agreements, strengthen bilateral cooperation, safeguard vital interests, and promote the inclusive development of the global data governance system. Establish an all-encompassing process compliance system to reduce compliance risks and promote the implementation and optimisation of the national-international coordination mechanism; thus, form a virtuous cycle in which both the government and enterprises actively participate in global data governance. China can lead the world in promoting institutional reform and offer an enterprise-compliance-based model of data governance.

References

- [1] Cyberspace Administration of China. (2023, April 28). *Digital China development report (2022)* [Report]. <http://m.toutiao.com/group/7227021026759475764/>
- [2] Bi, D. X. (2025). The challenges and responses to CPTPP cross-border data flow rules for China. *International Trade Issues*, (03), 89–102.
- [3] Tang, Z. (2025). Fragmentation of international rules on cross-border data flow and coordination pathways. *Jiangxi Social Sciences*, 45(6), 112–124, 207, 209.
- [4] Xu, D. G. (2022). On data jurisdiction and localization tendencies in cross-border data flow. *Chinese Yearbook of International Private Law and Comparative Law*, 31(2), 3–20.
- [5] Liu, Y. (2023). EU's technological sovereignty strategy in U.S.-EU cross-border data flow conflicts and its implementation. *International Law Review*, (06), 46–85.
- [6] Ma, Z. F. (2024). Construction of a regulatory sandbox system under the digital economy context. *Legal Studies Journal*, (02), 45–53.
- [7] Ji, Z. T. (2024). The extension and application of the EU-U.S. Data Privacy Framework and its implications. *International Law Review*, (03), 56–72.
- [8] Cyberspace Administration of China. (2019, November 5). Report on the construction of the China-Singapore international internet data dedicated channel [Web page]. http://www.cac.gov.cn/2019-11/05/c_1125195287.htm
- [9] World Bank. (2020, November 1). Key data from regulatory sandboxes across the globe [Brief]. <https://www.worldbank.org/en/topic/fintech/brief/key-data-from-regulatory-sandboxes>
- [10] Caixin. (2022, October 3). Two years after the U.S.-UK data access agreement: 80% improvement in cross-border data retrieval efficiency [Web page]. <https://www.caixin.com/2022-10-03/101960842.html>
- [11] China-Singapore (Chongqing) Strategic Connectivity Demonstration Project Management Bureau. (2021, September 10). *2021 China-Singapore cross-border data flow cooperation white paper* [White paper].
- [12] Li, M., & Qin, J. (2025). Exploring the construction of China's cross-border data flow rules system-A case study of the Hainan Free Trade Port. *International Economic Cooperation*, 41(3), 48–57, 93. <https://doi.org/10.20090/j.cnki.gjjh.2025.3.5>
- [13] Government of the United States of America & Government of the United Kingdom of Great Britain and Northern Ireland. (2019, October 3). Agreement between the Government of the United States of America and the Government of the United Kingdom of Great Britain and Northern Ireland on access to electronic data for the purpose of countering serious crime [Treaty].

- [14] Swire, P., & Hemmings, J. D. (2016). Mutual legal assistance in an era of globalized communications: The analogy to the visa waiver program. *New York University Annual Survey of American Law*, 71(4).
- [15] Cyberspace Administration of China. (2026, February 10). *Regulations on promoting and standardizing cross-border data flow* [Regulation]. https://www.gov.cn/zhengce/202501/content_6997438.htm
- [16] Woods, A. K. (2018). Litigating data sovereignty. *Yale Law Journal*, 128, 328, 362–363.
- [17] 360 Column. (2025, December 25). The “split” strategy of TikTok in the U.S. and its 19.9% stake behind the scenes: Revealing new paradigms for Chinese enterprises expanding overseas [Web page]. <https://caifuhao.eastmoney.com/news/20251225223504010514900>