Science of Law Journal (2024)
Clausius Scientific Press, Canada

DOI: 10.23977/law.2024.030414
ISSN 2616-2296 Vol. 3 Num. 4

Legal Dilemmas and Paths to Relief in Cross-Border Transfers of Personal Data by Multinational Corporations

Yuxuan Xie

Beijing Technology and Business University, Beijing, 102488, China
2410933890@qq.com

Keywords: Transnational corporations, cross-border transfer of personal data, data legislation, conflict of laws, international co-operation

Abstract: Multinational corporations (MNCs) face multiple legal dilemmas when transferring personal data across borders, mainly including the lack of uniform international law standards globally, the inconsistency of data legislation and the lack of clarity of the rules of extraterritorial application of domestic laws, which have led to MNCs facing great challenges in cross-border transfers of personal data. The insufficient role of international organisations in global data governance, irreconcilable differences in data legislations deeply influenced by conditions, and unclear rules of extraterritorial application prone to jurisdictional conflicts are all important reasons for the legal dilemma of cross-border data transfer. The solution to the current dilemma requires the tripartite cooperation of international organisations, governments and enterprises, through the promotion of international cooperation and coordination, the improvement of domestic laws and policies, the provision of technical support and other measures, in order to achieve the gradual improvement of global data protection standards.

1. Formulation of the problem

Cross-border transfers of personal information of multinational corporations have become an important legal issue due to the complexity of international and domestic regulations, the tightening of national policies, and the significant impact of data transfers on privacy and national security. With the trend of globalisation, it has become the norm for companies to conduct business in multiple countries and for data to be transferred globally. At the same time, governments recognise the importance of data sovereignty and are concerned that cross-border transfers of data by multinational corporations may lead to the leakage of sensitive data, which in turn affects national security. Therefore, they have introduced new data protection regulations. For example, China's Cybersecurity Law and Personal Information Protection Law set stricter conditions and security assessment requirements for cross-border transfers of personal information, emphasising compliance by critical information infrastructure operators and large-scale data processing companies. The EU's General Data Protection Regulation (GDPR) has global reach because it not only regulates EU member states, but also has extraterritorial applicability to any business that processes the data of EU citizens. It explicitly requires the use of standard contractual clauses, adequacy decisions, and other safeguard mechanisms when transferring data across borders. The

Asia-Pacific Economic Cooperation's (APEC) Cross-Border Privacy Rules System (CBPR) and other international policy frameworks are promoting legal compliance regulation of cross-border transfers of data, aiming to balance data flows with privacy protection. The policy coordination of these international organisations has made data transfers increasingly important in the global economy.

Strict scrutiny enhances the security of cross-border transfers of data, but is bound to lead to significant challenges for multinational companies when transferring personal data across borders.In 2019, the US Federal Trade Commission (FTC) fined Facebook $5 billion for misleading users about its data privacy policies, which led to unauthorised access to user data by third parties.[1]In 2020, H&M was fined €35 million by the Hamburg Office for Data Protection and Freedom of Information. The reason was that H&M violated the privacy rights of its employees by over-collecting their data in its German service centres.[2] These cases show the stringent regulation and enforcement of regulators on data privacy and cross-border transfers, and multinational companies need to develop well-thought-out data management strategies to prevent high fines and reputational damage.

Because of the problems under the current situation of cross-border transfer of personal information of multinational corporations, the academic community has also conducted in-depth discussions. Presently, domestic and foreign scholars' research mainly focuses on two aspects: research on the legal frameworks and policies of various countries and international coordination and cooperation. In terms of research on legal frameworks and policies of various countries, Paul M. Schwartz has studied in detail the conflict between the EU and the US in terms of data protection laws. He points out that legislation such as the EU's GDPR and the U.S.'s CCPA present distinctly different concepts that are difficult to reconcile and have become major legal barriers to cross-border data transfers.[3] In his book, Graham Greenleaf analyses the development of data privacy laws in Asian countries and their role in international trade. He argues that data protection laws in Asian countries have had a diverse impact on trade, which has led to significant uncertainty in cross-border data transfers.[4] In the area of international coordination and cooperation, Chinese scholar Liu Jinrui explored the main legal issues and challenges facing global data flows, particularly regarding personal information protection, national data security and jurisdiction. He argues that the current global data regulatory system is insufficient to meet these challenges, and proposes that China should play a more active role in global data governance and provide Chinese solutions to promote the construction of a global regulatory framework.[5] .On the other hand, scholars such as Veronica Arroyo, Karin Hess and other scholars propose measures for modification and change of cross-border flow of data from an international perspective, and emphasise the role of international organisations in formulating rules for cross-border data transfer. [6]

Although there has been extensive research focusing on the legal aspects of cross-border data transmission, there are still several research gaps. Firstly, scholars' studies have mainly focused on the legislation and policies of the region or specific countries, while the global perspective and international legal comparative studies are slightly insufficient. Although some scholars have put forward proposals for coordinating international data protection, there is a lack of concrete strategies on how to practically implement global coordination. Second, there are significant differences in the data transfer needs and legal frameworks of different regions, and current research on the development and implementation of data protection laws in emerging markets and developing countries is relatively scarce, failing to adequately take into account the unique challenges and interests of developing countries, which in fact play an increasingly important role in the global data ecosystem. Finally, there is a lack of research on how to find a balance between protecting individuals' right to privacy while promoting data-driven economic development and safeguarding the legitimate interests of multinational corporations.

Therefore, it is indispensable to further expand the research on the legal issues of cross-border transfer of personal data of transnational corporations. The current legal problems of cross-border transfer of personal data of multinational corporations are mainly due to the lack of uniform international law standards and the different domestic data legislation of different countries, which makes it difficult for multinational corporations to follow the consistent standards. This paper will analyse the above problems and propose feasible solutions in order to build a more complete legal framework for cross-border transfer of personal information.

2. Legal dilemmas in the cross-border transfer of personal data by transnational corporations

There are a number of legal challenges and dilemmas associated with the cross-border transfer of personal data of transnational corporations. First, despite the unprecedented exchange and sharing of data brought about by the digital age, there is still a glaring gap in uniform international law standards, which creates a lot of uncertainty in cross-border data flows and management. Secondly, there are significant inconsistencies in the legislative concepts of data legislation across countries, resulting in a fluid situation for multinational corporations and individuals in terms of data processing. To complicate matters even further, even if a country has developed a relatively sound legal framework for data, the question of whether these laws can play a role in cross-border data flows, as well as their extraterritorial applicability in the international context, remains ambiguous and uncertain in nature. These are important issues that need to be addressed by the international community at this time.

2.1 Vacancy in the harmonisation of international law standards

Currently, there is a lack of uniform international legal standards on the regulation of cross-border data transfers globally, which makes multinational corporations face a number of challenges in formulating data management policies. Firstly, there are only a few voluntary international agreements or initiatives, such as the Guidelines on Privacy Protection and Transborder Flows of Personal Data developed by the Organisation for Economic Co-operation and Development (hereinafter referred to as the OECD) and the Asia-Pacific Economic Co-operation (hereinafter referred to as the APEC) Privacy Framework. Moreover, the limited number of countries participating in these agreements has prevented them from forming a global consensus and developing into legally binding global standards. Secondly, national and regional legislation tends to be autonomous and localised. Countries formulate data legislation and policies based on their interests, resulting in very different requirements for data protection in different jurisdictions. Some countries enact strict data protection laws and impose severe penalties for violations. Others, on the other hand, have more relaxed data protection legislation and value the commercial freedom and development of enterprises. This lack of uniform standards not only affects the operational efficiency of enterprises, but is also highly susceptible to potential legal risks.

2.2 Inconsistencies in national data legislation

In the absence of harmonised international law standards, multinational corporations need to follow the data legislation of different countries and regions, yet there are significant inconsistencies in the content and requirements of such legislation. Definitions of data protection, compliance requirements and penalties vary from country to country. For example, the EU General Data Protection Regulation (GDPR), which is representative of the common law system, and the US California Consumer Privacy Act (CCPA) are both dedicated to the protection of consumer privacy and the security of personal data, but they have very different legal requirements.[7]The GDPR

favours comprehensive protection of personal data, providing data subjects with rights of access, erasure and data portability.[8]Whereas the CCPA focuses primarily on control and transparency for consumers, giving them the right to object to the sale of their data.[9] Civil law in China and Russia are different, with the Personal Information Protection Law (PIPL) and the Russian Federation's Law on Personal Data focusing more on data localisation and national security, with an emphasis on strict data regulation. This legal inconsistency means that multinationals must have different data transfer policies for each region in which they have operations to ensure compliance.[10] In addition, due to the ever-changing legislation in each region, companies also need to continually monitor and adjust their policies to ensure that they meet the legal requirements of each location at all times. This adds administrative complexity and exacerbates the risks and costs for companies operating in multiple jurisdictions

2.3 Ambiguity and uncertainty in the extraterritorial application of data legislation

The extraterritorial application of data legislation refers to the application of national data legislation by the State with respect to persons, things, or acts located or occurring outside its field of jurisdiction.[11] This phenomenon has certain inevitabilities, but it is also bound to create legal problems. For example, the rules and scope of some domestic data protection laws' extraterritorial application are unclear, leaving businesses uncertain when transferring data across borders..Taking Article 3 of the GDPR as an example, it provides. for the extraterritorial application of the GDPR to non-EU businesses, i.e., those that are involved in the provision of goods or services to data subjects in the EU, or in the monitoring of the data subjects' activities within the EU must comply with the GDPR.However,these rules lack detailed explanations in several instances. For example, the circumstances in which a data subject is considered to be "providing services for the EU market" or "activities in the EU" are not clearly defined. The extraterritorial application of Chinese Personal Information Protection Act is also problematic. The regulation's extraterritorial application focuses on foreign enterprises that provide goods or services in China. However, how to define these enterprises and how to regulate them remains a challenge in practice.

3. Causes of the Dilemma of Cross-Border Transfers of Personal Information by TNCs

Before exploring solutions to the dilemmas, it is essential to recognise the causes of these dilemmas. The dilemma of cross-border transfer of personal data of multinational corporations is the result of a combination of factors. First, the role of international institutions in data governance has not yet been brought into full play, leading to a lack of uniform laws and norms in the process of data transfer. Second, the data legislation of various countries is influenced by their respective national conditions, and the difficulty of coordinating legal differences is high, which brings many legal risks to the global operation of enterprises. Furthermore, due to the importance countries attach to data sovereignty, the phenomenon of extraterritorial application of data legislation has become increasingly prominent, and multinational corporations face more complex challenges in data compliance. Together, these factors are the main reasons for the difficulties faced by multinational corporations in the cross-border transfer of personal information.

3.1 Inadequate role of international agencies in data governance

The shortcomings of international institutions in global data governance are twofold. On the one hand, existing agreements that have been developed lack legally binding force when it comes to monitoring and enforcement. First, most of the existing international agreements are guiding principles or recommendatory frameworks, and lack mechanisms that are mandatorily binding on

countries, such as the Guidelines on Privacy Protection and Transborder Flows of Personal Data of the Organisation for Economic Co-operation and Development, and the Asia-Pacific Economic Co-operation's (APEC) Privacy Framework.[12] Such agreements usually fail to meet the special needs of all member countries, and due to their voluntary nature, countries can choose the degree of compliance at will according to their own interests, resulting in international standards not being fully implemented. Secondly, international law has always followed the principle of state sovereignty, and states have the highest jurisdiction over affairs within their borders. Therefore, when international institutions set global standards, member states usually retain priority over domestic laws.[12]For example, despite the OECD's proposed guidelines for cross-border data flows, member states can still enact stricter or looser regulations according to their own national realities. This situation is particularly evident in the extraterritorial application of the EU GDPR and the formulation of the US CCPA, where each country emphasises the priority of its own regulations. Again, there is a lack of independent international enforcement agencies. Most international institutions do not have the power to directly enforce international agreements and can only rely on the voluntary fulfilment of member states. The UN's International Court of Justice (ICJ), although it has the power to adjudicate international disputes, requires the initiative of member states to submit cases. International organisations often lack enforcement bodies to ensure that countries comply with global standards. Even under the framework of international standardisation organisations such as ISO, companies are free to choose whether or not to follow their standards. Finally, unlike other physical products, online data is intangible and can easily bypass traditional customs and border controls through virtual channels, making it difficult for countries to accurately track the path of data flows across borders. The cross-border nature of data storage also makes it difficult for States to determine the scope of their jurisdiction, leading to difficulties in holding them accountable for data breaches and violations.

On the other hand, the willingness of member States to participate in agreements developed by regional organisations is low. Regional organisations face the problem of low willingness of some member states to participate in developing cross-border privacy rule systems. This is mainly caused by differences in national interests and policies. For one thing, there are differences in the needs and priorities of member states in terms of data privacy protection and cross-border data transfers. Some countries may focus more on opening up data flows to facilitate cross-border trade and scientific and technological co-operation. In contrast, others may prioritise data privacy and sovereignty, emphasising the protection of citizens' privacy and restricting the exit of data. That is why it is difficult to find a balance between member states involved in rule-making, leading to a lack of enthusiasm in the establishment and implementation of rules in some member states. Secondly, it is difficult to implement unified rules due to the huge differences in the legal systems, cultural backgrounds and political structures of different countries. Some countries have backward legal systems that are unable to meet the requirements of international standards, while others have mature regulatory systems and are unwilling to lower their standards. So some member countries may think that the cost of joining the regional rule system is higher than the benefit, and then lack the motivation to participate. Third, the issue of data sovereignty is a sensitive topic for cross-border privacy rules. Countries are worried about losing control of their own data in the process of implementing a regional rule system, resulting in the impairment of data sovereignty. Developing countries, in particular, are concerned that their data will be misused by developed countries as a result of cross-border transmission and lack the corresponding legal and technical means to protect against it. This concern has led some member states to have reservations about the regional rules system, preferring to enact stricter domestic regulations to protect data privacy.

3.2 Data legislation is influenced by national circumstances and differences are difficult to reconcile

3.2.1 Overview of Data Legislation and Comparison of Differences by Region

Differences in data legislation are widespread across the globe, with multinational corporations facing the complexities of different regulatory regimes for data transfer and protection. This paper chooses the EU, the US, China and Russia as representative regions for the study, mainly based on their respective unique data protection legislative systems, economic scale and global influence. These countries and regions not only have large economic markets, but also their legislative policies directly influence the direction of global data protection rules. The General Data Protection Regulation (GDPR) in the EU, the California Consumer Privacy Act (CCPA) in the U.S., the Personal Information Protection Law (PIPL) in China, and the Russian Federation's Law on Personal Data in Russia are each representative of their own, reflecting the values and regulatory models regarding privacy and data protection in different economies.

The EU's GDPR is considered to be the most comprehensive and stringent privacy regulation in the world today. Its strict regulations are reflected in several aspects: first, the broad scope of application, even if a business is not located in the EU, as long as it provides products or services to EU residents or monitors their behaviour, it must comply with the GDPR. Second, the protection of the rights of data subjects, such as the right of access to data, the right to rectification, the right to erasure and the right to data portability.[13]Third, there are compliance requirements for data processors and controllers, including the designation of a data protection officer, the conduct of data protection impact assessments, and the timely reporting of data breaches. In addition, the GDPR sets fines of up to 4 percent of global turnover or 20 million euros as a powerful enforcement tool to ensure that regulations are strictly enforced.

In contrast to the EU's harmonised regulations, privacy legislation in the US is relatively decentralised, with states enacting their own data privacy laws, while regulations at the federal level are usually specific to particular data types or industries. The CCPA, a state-level statute, is considered the benchmark for privacy protection in the U.S. and is intended to provide California consumers with greater control over their personal information, including knowing, deleting, and restricting businesses from selling or sharing their personal information. However, the CCPA is limited to California residents and lacks a binding effect on businesses nationwide or globally. Meanwhile, U.S. federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA) and the Children's Online Privacy Protection Act (COPPA) set specific protection requirements for medical and children's online data, respectively. This fragmented legislation has resulted in fragmented and geographically specific data privacy protections in the US, lacking a unified national standard.

China and Russia, as emerging markets, place a higher value on national security and data sovereignty in their data legislation than the EU or the US. China's Personal Information Protection Law requires that when transferring personal information outside of China, the controller or processor of the personal information needs to apply to the relevant Chinese regulatory authorities and undergo a review and approval process to ensure that the outbound transfer of personal data complies with laws and regulations.[14] The strengthening of this procedure reflects China's strict control over outbound transfers of personal data to protect national security and public interests. Russia's Law on Personal Data of the Russian Federation stipulates that personal data of Russian citizens must be stored and processed in the country, and that cross-border transfers need to ensure that privacy protections in the destination country are in line with Russian standards.[15] At the same time, there is a specialised regulator responsible for monitoring and enforcing data protection regulations and has the power to mandate compliance by businesses. The bill highlights Russia's

emphasis on state control and regulation in the data sphere, particularly in relation to national security.

It can be seen that the EU focuses on individual privacy and strict regulation, the US focuses on market-driven and industry self-regulation, and China and Russia strengthen data sovereignty and national security. Inconsistencies in the legal standards of different regions have led to difficulties for enterprises in cross-border data transfer and processing. For example, under the EU's GDPR rules, businesses need to obtain users' explicit consent to process their personal data and must take strict technical and organisational measures to safeguard data security. However, the US CCPA allows businesses to share user data without explicit consent, as long as the user has the right to opt out. In such cases, where companies are involved in both EU and US operations, it is difficult to determine which country's legal requirements should be followed.

3.2.2 Main causes of legislative differences between regions

3.2.2.1 Differences in legislative values

Differences in legislative value propositions reflect the different views of States on the balance between personal privacy and commercial interests. Such differences stem mainly from differences in cultural traditions and social perceptions. European society attaches great importance to individual privacy and regards it as an inviolable basic human right. Influenced by this concept, the EU's cross-border data governance is premised on the protection of personal privacy, while focusing on the construction of the internal market, presenting a "strict external and loose internal" regulatory thinking: internally, it encourages the free flow and sharing of data, and establishes a single data market to promote the development of the EU's digital economy; externally, it embodies the strict protection of personal data, and is based on the general principles of data transfer, adequacy and transparency. The external regulation reflects the strict protection of personal data, with the general principles of data transfer, adequacy determination, and standard data protection clauses as the three-pronged means to build a normative system for cross-border data transfer, [16] and set strong compliance requirements and high fines. The U.S. concept of privacy protection, on the other hand, is influenced by market liberalism, which emphasises the freedom of individuals and business, and believes that privacy protection needs to be balanced with economic interests.[17] As a result, federal regulations have been more industry-specific in setting standards for privacy protection, rather than creating comprehensive state-level regulations. State legislation also reflects local economic, political and social needs. Chinese and Russian values reflect an emphasis on national security and sovereignty in data legislation. China's PIPL, as well as Russia's Law on Personal Data of the Russian Federation, reflect the state's will to safeguard national interests and data sovereignty through strict regulatory means. They set extensive national censorship and data localisation requirements to ensure that sensitive data is subject to strict state regulation. This line of thinking stems from both countries' high value on national sovereignty and stability.

3.2.2.2 Differences in the level of development of countries

Differences in the level of development of countries have a similar impact on data legislation. For one thing, in terms of the maturity of the digital economy, developed economies usually have more mature digital economies and information infrastructures, and have higher requirements for data protection. For example, the European Union and the United States have more mature digital markets, and the need to regulate privacy protection is more pressing. Second, in terms of resource allocation and regulatory capacity, developed countries usually have more regulatory resources and technical support, and are able to formulate more complex privacy protection regulations and enforce them effectively. Developed countries and regions, such as the EU GDPR, require

companies to set up data protection officers, conduct data protection impact assessments, etc., and have higher regulatory and compliance requirements. In contrast, in developing countries, the lack of adequate technical and financial support makes it more difficult to enforce data protection regulations.

3.2.2.3 Differences in Legal Culture and Tradition

Differences in legal cultures and traditions have also profoundly impacted the data legislation regime. In terms of the influence of legal systems, the main countries in the EU belong to the civil law system, which focuses on statutory law and provides uniform legislative standards, and the GDPR, as an EU-level regulation, provides a consistent privacy protection framework for all member states. The U.S., on the other hand, mainly belongs to the common law system, which emphasises case law and the separation of powers, and states have a high degree of legislative autonomy. As a result, privacy protection in the U.S. is characterised by fragmentation and territoriality, and lacks national standards. From the perspective of regulatory tradition, the EU countries are more accustomed to the central government to set uniform regulatory standards, and member states have a certain degree of flexibility in implementation. The United States, on the other hand, tends to promote privacy protection through market self-regulation and industry norms, with the government acting more as a watchdog than a direct regulator. China and Russia, on the other hand, have regulatory traditions that favour direct administrative intervention in data flows and use to ensure that the will of the state is carried out.

These differences, stemming from regional political systems, legal traditions, economic interests and national security needs, make it difficult to develop globally harmonised standards for personal data protection and create complex challenges for multinational corporations with regard to data transfers.

3.3 Lack of clarity on the rules applicable extraterritorially

3.3.1 Reasons for the establishment of the rule of extraterritorial application

In the context of globalisation, cross-border flow of data has become an irreversible trend. States have enacted data protection laws with the aim of protecting the security of citizens' personal information and their right to privacy. However, due to the borderless nature of data flows, the traditional theory of national jurisdiction has been challenged, and countries have adopted data protection laws to impose jurisdiction over the data processing activities of enterprises outside their borders, which raises the issue of the extraterritorial application of data protection laws.

First, the rules on extraterritorial application have their roots in the importance that States attach to data sovereignty. Data sovereignty means that a State has sovereign jurisdiction over data generated within its territory and is able to determine the way in which data are stored, processed and transmitted. With the development of the Internet and information technology, data has become an important part of a country's economy and security, and data sovereignty has become an important manifestation of national sovereignty. Therefore, countries have passed legislation to give extraterritorial effect to data protection laws in order to safeguard the country's data sovereignty and citizens' right to privacy. For example, the EU's GDPR explicitly provides for jurisdiction over companies that are outside the EU but process data of EU residents, which reflects the EU's emphasis on data sovereignty.[18]

Second, globalisation and the development of the digital economy have also contributed to the creation of rules on the extraterritorial application of data protection law. Multinational enterprises operate globally, and the cross-border transmission and data processing has become part of their

daily business. In order to protect the personal data of their citizens, legislators in various countries have realised that it is not enough to regulate the conduct of domestic enterprises, and that they must also impose jurisdiction over the relevant conduct of enterprises outside their borders in order to ensure that the data of their citizens are protected globally.[19] Such considerations have led countries to introduce rules of extraterritorial application in their data protection legislation.

3.3.2 Conflict of laws arising from the extraterritorial application of data legislation

While the extraterritorial application of data protection laws has positive significance in protecting citizens' data security and privacy rights, it has also given rise to many legal conflicts. These conflicts are mainly reflected in the following aspects:

First, the rules of extraterritorial application are uncertain in terms of the scope of application of the law. Different countries define the scope of extraterritorial application of data protection laws differently, making it difficult for multinational enterprises to determine which laws they need to comply with in a given situation. The EU's GDPR requires businesses to comply with the GDPR even if they are located outside of the EU, as long as they process the data of EU residents.[20]But this provision can cause problems in practice. If a U.S. company collects data on EU residents through its website, it would need to comply with the strict requirements of the GDPR. However, if the company is not actively orientated towards the EU market, then its need to comply with the GDPR may be disputed in practice. This uncertainty about the scope of the law's application increases legal risk and policymaking costs for companies.

Second, the extraterritorial application of the rules may give rise to conflicts of law such as jurisdiction.[21]A U.S. company processing data of EU residents has to comply with both the provisions of the GDPR and the relevant U.S. laws. However, when these two sets of laws are in conflict in certain aspects, the company will be in a dilemma. For example, the GDPR requires companies to obtain explicit user consent to process personal data, and they need to notify regulators within 72 hours of a data breach[22]. In the U.S., specific notification and user consent requirements vary from state to state, with Virginia's Data Security Act, for example, requiring companies to notify affected individuals "within a reasonable time," usually no more than 45 days.[23] This conflict of multiple jurisdictions makes it difficult for companies to meet the legal requirements of each country at the same time, thereby exposing them to the risk of legal penalties.

4. The way out of cross-border transfers of personal information by transnational corporations

The cross-border transfer of personal information has become a global proposition, so it requires the cooperation of every international entity, including international organisations, governments and multinational enterprises, in order to gradually solve the current dilemma of cross-border transfer of personal information.

4.1 International organisations: regional cooperation and harmonisation of standards

International agencies need to work closely with governments, businesses and technical experts to address the challenges of transnational data protection through measures such as promoting regional cooperation, progressively facilitating the development and implementation of globally harmonised data standards, and establishing a global regulator.

First, regional cooperation should be promoted to facilitate global harmonisation. As regional organisations have advantages in coordinating regional interests, regional cooperation should be used to promote the development of unified data standards. For example, APEC can increase the

transparency of the system, show enterprises and member states the advantages and protection mechanisms of the system, and enhance trust. It can also streamline the compliance process for cross-border data transfers by introducing a multinational certification body to review the privacy practices of enterprises. International agencies need to promote mutual recognition of the CBPR system with other regional data standards to achieve broader regional harmonisation.

Secondly, the development of implementable international standards. In the process of developing global data standards, international agencies should develop a step-by-step implementation strategy. Firstly, an independent committee composed of technical and legal experts should be set up to study data legislation on a global scale and formulate a set of fundamental principles. The basic principles need to broadly cover data privacy, data security, and data sovereignty, and have a high degree of acceptance globally. Under the guidance of the basic principles, countries gradually integrate the basic principles into their national legislation and make appropriate adjustments to them to meet their own special needs, expanding the basic principles into regulatory requirements with practical operation. In the process of standard-setting, international institutions should pay attention to maintaining flexibility and make timely adjustments and optimisation according to the feedback from member countries. A multi-level rule system should be formulated in conjunction with the actual needs of member countries to ensure that cross-border data flows can be facilitated while safeguarding the privacy and data sovereignty of each country.

Thirdly, a global data regulator should be established. International agencies should establish a global independent data regulator. First, it should have a regulatory function. It is responsible for supervising the fulfilment of cross-border data protection agreements by member states and ensuring their compliance with international data protection standards. Second, it should have a dispute resolution function. International organisations should establish a global data arbitration body to handle disputes in cross-border data transfers and provide fair arbitration results. At the same time, regulators should be given investigative and punitive powers to ensure that non-compliant companies and countries bear due responsibility. Finally, technical and policy assistance should also be provided. Provide technical support to countries with low levels of data protection and assist them in formulating and implementing data protection policies. International agencies need to provide references for countries in the formulation of legislation and policies on data protection and cross-border data transfer, and help them improve relevant regulations.

4.2 Governments: legal improvements and technical support

Governments should take measures mainly in the areas of international cooperation, legal frameworks and technical support.

First, in terms of international cooperation, the Government should, like international organisations, actively promote global cooperation to fill the gap of uniform standards in international law. Through participation in international organisations or multilateral conferences such as the United Nations, the Organisation for Economic Co-operation and Development, the International Telecommunication Union, etc., the government can promote the formulation of international data protection agreements with the ability to gain consensus. At the same time, the government can also reduce the inconvenience caused by legal differences by signing bilateral or multilateral data protection agreements. For example, the EU has promoted the adoption of similar high-standard data protection regulations in other countries by signing agreements with other countries on the application of the GDPR. In the process of international co-operation, the government should maintain an open and inclusive attitude, and actively consult with the regulatory bodies of various countries to jointly address the challenges in the field of data protection.

Secondly, in terms of legal framework, governments should establish and improve their domestic

data protection legal system to ensure the transparency and clarity of laws and regulations. Governments can draw on the provisions of advanced international laws and regulations, combine them with the actual situation of their own countries, and formulate data protection laws and regulations in line with national conditions, so as to promote the improvement of relevant domestic rules. Through the construction and output of the domestic rule system, the state's right to participate in the governance of cross-border data flow and influence can be strengthened, so as to provide practical protection for enterprise data cross-border.[24] At the same time, it should also further refine the legal provisions by issuing implementation rules and guidelines, clarifying the scope of application of the law and specific operational requirements, strengthening the operability of data regulations, and reducing uncertainties in the implementation of the law. In addition, the government should strengthen publicity and education on data protection laws to raise the legal awareness of the public and enterprises to ensure the smooth implementation of the laws.

Thirdly, in terms of technical support, the Government should enhance the overall level of data protection by providing technical support and guidance. The government can support the research and development and application of data protection technologies and enhance the level of data protection by setting up special funds and technology research and development projects to subsidise research institutes and enterprises to develop advanced technologies such as data encryption, anonymisation and de-identification. The government can also provide technical counselling and services to help enterprises solve data protection technical problems by establishing national-level data protection laboratories and technical platforms. In addition, the government should strengthen the standardisation of data protection technologies, formulate unified technical standards and specifications, and promote the standardisation and universal application of the technologies. For example, China has regulated the application of data protection technology and gradually improved the overall level of data protection through the release of national standards such as the Personal Information Security Specification for Information Security Technology. Through government technical support and guidance, the capacity of domestic data protection can be effectively enhanced.

4.3 Transnational corporations: internal compliance and external coordination

Multinational corporations should address the obstacles encountered in the cross-border transmission of personal data mainly in three areas: legal compliance, technical safeguards and international cooperation.

First, in terms of legal compliance, companies should establish a comprehensive global compliance system, component a specialised global compliance team that is responsible for tracking the dynamics of data protection laws in each country and adjusting the company's data management policies according to the latest regulations. The compliance team should include legal, technical and business experts to ensure that the company's global operations are in compliance with local data protection laws, and develop a multi-level compliance strategy based on data protection laws in different countries and regions. In addition, transnational corporations should provide clear guidelines on the division of labour, responsibilities and specific business practices of relevant personnel involved in data cross-border processes within the company, refine the authority approval and management control of data usage, or establish a regular data compliance self-assessment system and conduct regular self-reviews of data compliance risks to guarantee the effective implementation of the data compliance work system.[24]

Second, in terms of technical protection, enterprises should improve their own data protection technology. Enterprises can adopt data encryption, anonymisation, de-identification and other technical means to protect user data privacy, reduce the risk of data leakage, and ensure that their

operations in different countries and regions comply with local data protection laws. Enterprises should also establish a sound data management system, including a full-process protection mechanism for data storage, transmission and processing, to ensure data security and compliance in all aspects. In addition, enterprises can also improve the automation level of data protection by introducing artificial intelligence and machine learning technologies to achieve real-time monitoring and rapid response to data leakage and violations. Through continuous innovation and enhancement of technological means, enterprises can effectively respond to the lack of international data protection standards and the inconsistency of national data legislation.

Thirdly, in terms of international cooperation, enterprises should pay close attention to data protection agreements and guidelines promoted by international organisations such as the United Nations and the Organisation for Economic Co-operation and Development, actively participate in the process of formulating international standards, put forward constructive comments and suggestions, and work together to formulate more reasonable and feasible international standards. Data protection agreements can also be signed with partners in other countries or regions to clarify the responsibilities and obligations of both parties in data protection and transmission, and to ensure that data meets the legal requirements of both parties during cross-border transmission. In addition, enterprises should strengthen communication with data protection regulators in various countries to understand the latest legal developments and regulatory requirements, and adjust their data management policies in a timely manner.[25] Through international cooperation and regional coordination, enterprises can gradually achieve standardisation and consistency in data protection on a global scale.

5. Conclusion

Under the wave of globalisation and digitisation, the legal dilemmas faced by multinational corporations in conducting cross-border transfers of personal information have become increasingly prominent. Solving those problems required the concerted efforts of many parties. International organisations are responsible for promoting regional cooperation, setting global standards and establishing regulatory bodies to ensure the regulation of cross-border data transfers; governments should strengthen international cooperation, improve domestic legal frameworks and provide technical support to ensure the security of data transfers. Multinational corporations, for their part, should focus on legal compliance, technological safeguards and international cooperation to meet the ever-changing challenges of data protection. These comprehensive measures will help ensure the secure transmission of personal data, achieve a balance between data flow and privacy protection, and promote the sustainable development of the global digital economy. We have reason to believe that in the near future, the legal dilemmas of cross-border data transfers will gradually be eased and multinational companies will be able to conduct cross-border transfers of personal data more efficiently and securely.

References

[1] Information on: https://www.ftc.gov/news-events/news/press-releases/ 2019/07/ftc-imposes-5-billion -penalty-sweeping - new-privacy-restrictions- facebook

[2] Information on: https://www.bbc.com/news/technology-54418936

[3] Schwartz P M. The EU-US Privacy Collision: A Turn to Institutions and Procedures[J]. Harvard law review, 2013, 126(7): 1966-2009.

[4] Greenleaf G. Asian data privacy laws: trade & human rights perspectives[M]. OUP Oxford, 2014.

[5] Liu Jinrui. Towards global regulation of cross-border data flows: Basic concerns and Chinese solutions [J]. Administrative Law Studies, 2022,(04):73-88.

[6] Information on: https://www.sciencespo.fr/public/chaire-numerique/ wp-content/uploads/ 2023/09/policy-brief

-data- flows.pdf
[7] Zhang Shouwen. Legal Development and comprehensive Protection of consumer Information Right [J]. Law Journal, 2021,(12):149-161.
[8] See EU General Data Protection Regulation, Article 5.
[9] See California Civil Code Section 1798.100 - Consumer rights.
[10] Liang Yanni. Corporate Data Compliance Governance: From Personal data protection to cross-border data flow [J]. Social Scientist, 2023,(12):81-85.
[11] Wen Shu. Conflict of Laws caused by extraterritorial application of data legislation and China's solution [J]. Journal of Yunnan Normal University (Philosophy and Social Sciences Edition), 2019,55(06):96-108.
[12] Ao Haijing. Data protection way of international soft law [J]. Journal of local research, 2022, 33 (02) 6:158-172.
[13] Wang Qian, Gu Xueying. Employee Personal Data compliance management in European companies under GDPR [J]. German Research, 2019,36(02):117-131+136. (in Chinese)
[14] See Article 37 of the Personal Information Protection Act.
[15] See Article 5 of the Personal Data Act of the Russian Federation.
[16] Mei Ao. Data the new development of cross-border transport rules and coping [J]. China local research, 2023, 40 (04): 58-71. DOI: 10.16390 / j.carol carroll nki issn1672-0393.2023.04.008.
[17] Ye Chuanxing, Yan Wenguang. Data on China cross-border system present situation, problems and rescue path [J]. Journal of Beijing university of aeronautics and astronautics (social science edition), 2024 ((01): 57-71. DOI: 10.13766 / j.b HSK. 1008-2204.2023.2035.
[18] Guo Chunzhen, God send. The dilemma of defining the cross-border flow of personal information and its judgment framework [J]. China Law Review,2022,(06):86-106.
[19] Si Weipan. Evolution, paradigm and Mirror of the governance of cross-border Personal Data Transfer in EU [J]. Science and Technology Management Research, 2019,43(20):205-213.
[20] Wang Qian, Gu Xueying. Employee Personal Data compliance management in European companies under GDPR [J]. German Research, 2019,36(02):117-131+136. (in Chinese)
[21] Wen Shu. Conflict of Laws caused by extraterritorial application of data legislation and China's solution [J]. Journal of Yunnan Normal University (Philosophy and Social Sciences Edition), 2019,55(06):96-108.
[22] See EU General Data Protection Regulation, Article 33.
[23] See Virginia General Assembly. "Virginia Data Breach Notification Law." Virginia Code, §18.2-186.6.
[24] Chen Bing. Digital enterprise data across borders compliance governance approach [J]. Journal of rule by law the rule of law research, 2023, (02): 34-44, DOI: 10.16224 / j.carol carroll nki cn33-1343 / d. 20230224.006.
[25] Mei Ao, Pan Zijun. Governance model, problem review and compliance approach of enterprise cross-border data compliance [J/OL]. Intelligence, theory and practice of 1-9 [2024-05-22]. http://kns.cnki.net/kcms/detail/11. 1762.G3. 20240112. 1248.002.html.