Literature, Language and Cultural Studies
ISSN Print: 3079-5095
ISSN Online: 3079-5109
https://doi.org/10.63313/LLCS.9013

Cross-border data flow rules are in line with Chinese law

Xu Wang
School of Law, Anhui University of Finance and Economics, Bengbu 233030, China
Email: 1207825148@qq.com

How to cite this paper: Wang, X. (2025). Cross-border data flow rules are in line with Chinese law. Literature, Language and Cultural Studies, 1(1), 75–82. ISSN 3079-5095 (Print), ISSN 3079-5109 (Online).
https://doi.org/10.63313/LLCS.9013
Published: 2025-04-17

Abstract

Cross-border data flow, as a new product of the Internet era, plays a pivotal role in global economic development. In the Internet era, countries pay more and more attention to cross-border data flow rules. In the international community, the cross-border rules of data include the mode of data free flow, the mode of data rights protection and the mode of data localization. Starting from the legis-lative path of data localization in China, combined with the cross-border data flow rules in the United States and Europe, from the aspects of studying and im-proving the multiple paths of Chinese data outbound, adopting refined data out-bound management policies, vigorously carrying out international cooperation, and actively participating in the formulation of international rules, in order to promote the development of domestic data and enhance the voice of interna-tional data cross-border rules.

Keywords

Data localization; Data cross-border flow; Data security

1. Definition of cross-border data flow

The concept of "cross-border data flows" was first proposed in the 1970s by the Working Group on Computer Applica-tions under the Committee on Science and Technology Poli-cy (CSTP) of the OECD.The existing literature describes cross-border data flows in a variety of ways. The most au-thoritative definition comes from the 1980 OECD Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (hereinafter referred to as the "Guide-lines").Article 1, paragraph 3, of the Guidelines defines "Transborder flows of personal data" as "movement of per-sonal data across national borders," and paragraph 2 defines "personal data" as "any information relating to an identified or identifiable individual (data subject)."In fact, because the cross-border movement of personal data is the most critical and controversial aspect of international data flows, the vast majority of current studies replace the term "Transborder data flows" with "Transborder personal data flows".11111111In addition, in this re-

search, "data" is often confused with "information" and "data", and there is no sub-stantial difference in meaning.

2. Cross-border data rules in the United States and Europe

There is a serious conflict of values on cross-border data rules in Europe and the United States, resulting in different cross-border data flow rules led by their value level. In the European Union's "rights-based" concept, individual users are regarded as the subject of information data rights, while in the United States' "market-based" concept, individual us-ers are simply regarded as "consumers". The difference is that the United States considers the privacy protection of personal information in the "market environment" and only considers the "prevention of commercial fraud or improper transactions", while European countries have a set of data rights that can be actively exercised. The fundamental reason is the inherent differences be-tween the two sides in terms of the protection and development of personal rights and data. The essence of the several changes in the cross-border data flow of Europe and America is the battle between the "right standard" of the EU and the "market standard" of the United States.

2.1. The United States - market standard

The United States adopts the model of free flow of data. The United States regards the free flow of data across borders as part of free trade, and believes that data should flow around the world without restrictions.It also believes that the pro-tection measures taken by countries around the world to protect their own data resources are serious obstacles to data flow.At a hearing held by the US House of Representatives in 1980, the chairman of the Subcommittee on Government In-formation and Individual Rights pointed out that US compa-nies often "have to meet various requirements of laws and regulations in different countries", which would pose a major threat to the data transmission and free trade of US com-pa-nies.In 1980, the OECD issued the Guidelines to focus on harmonizing the incon-sistent levels of privacy and personal information protection laws in various coun-tries. The aim was to reduce the strength of data protection measures adopted by various countries for data security, so as to im-prove the level of data openness in various countries.Prior to this, the United States Department of Health, Education, and Human Services issued the far-reaching Fair Information Practice Principles. These principles call for the prohibition of the secret storage of personal records, the protection of an individual's right to know, the use of personal information based on an individual's authorization, the right to correct personal records, and in-formation security.222222The OECD has infused these principles into the Guide-lines to provide a framework for the free flow of data that does not have the force of formal law, but has the characteristics of "soft law". [3]The guidelines stress that OECD members should "take all reasonable and appropriate steps to ensure the cross-border data flow of personal data, including through uninterrupted and se-

cure transfers between member states." [4]Among oth-er things, it advises countries to avoid excessive privacy protections and to avoid "developing laws, policies and prac-tices in the name of protecting privacy and personal freedom that create barriers to the cross-border flow of personal data that exceed the requirements for such protection." [5]The United States does not take protective measures to enhance the security level of the right to privacy and personal infor-mation, but its actual purpose is to meet the needs of data collectors for their own privacy protection, so as to ease the conflicts between data flows and data collectors, reduce the resistance of data collectors to the generation of data, and promote the further improvement of the level of data flow.

2.2. Europe-rights-based

Europe has a long tradition of attaching importance to the protection of human rights, especially in the protection of privacy legislation. [6]Hence the data-rights model. For a long time, data protection in Europe has been based on the right to privacy. It is generally believed that data right is part of the right to privacy, and the so-called protection of per-sonal data and information is only an interpretation of the right to privacy from the "information perspective". [7]The EU's regulations on the cross-border flow of data are mainly reflected in the General Data Protection Act (GDPR) and the Digital Services Act (DSA). Described as "the most stringent Personal data protection regulation in history", the GDPR emphasizes the protection and privacy of personal data, and imposes strict conditions on the exit of data flowing to non-EU countries, ensuring that these countries can provide the same level of data protection as the EU. For example, by establishing mechanisms for comparable levels of data pro-tection, or using tools such as standard contractual clauses, to maintain compliance with data flows across borders. Compared to GDPR, the DSA focuses more on regulating the behavior of digital platforms, protecting the fundamental rights of users, and improving the transparency, fluidity, and security of data flows. The above shows that EU policies promote the free flow of data, but place a higher priority on citizens' fundamental rights and freedoms. This rights-based concept reflects the EU's legislative thinking and priorities in dealing with data development and individual rights protec-tion in the Internet era, that is, while promoting data devel-opment and economic development, it prioritizes the pro-tection of personal data security and privacy rights.

3. China's data cross-border rules and legislative path

The data localization model refers to the country's adoption of laws or rules to restrict the flow of domestic data abroad. In some important information security sectors, data locali-zation model is often used. For example, the United States has clearly required that the data of important departments such as defense, tax and medical services must be stored lo-cally and subject to export control. Based on the complex social situation in China and the fierce international situa-tion, China

chooses a relatively sound data localization model.

3.1. Personal information and important data are stored in China

According to the requirements of the Cyber Security Law, personal information and important data collected and gen-erated by operators of critical information infrastructure involving public communications, energy, transportation and finance should be stored in China. China's Cyber security Law has clear requirements for this,especially in key areas related to national security, public interest and social or-der-including public communications, energy, transporta-tion and finance. Operators in these sectors, when operating in China, are obliged to ensure that the personal information and important data they collect are stored in our territory. Such regulations help protect national security and prevent leaks of sensitive information, while also safeguarding citi-zens' right to privacy. China has offered more lenient policies to operators of non-critical information infrastructure. These operators do not have to make it mandatory to store data within the country, but can decide based on their own business needs and international cooperation. Such an ap-proach, while giving operators more flexibility, equally stresses the importance of "promoting the secure and free flow of data across borders".

3.2. Security assessment of data leaving the coun-try

The Guidelines for the Protection of Personal Information in Information Security Technology Public and Commercial Service Information Systems put forward restrictive re-quirements for the departure of personal information, that is, personal information can only be sent out of the country with the explicit consent of the information subject or with the approval of the relevant department. In China, due to the gradual improvement of the classification and hierarchical management of data by law, the domestic data exit security evaluation system adopts the same dual structure as the do-mestic storage. First, in accordance with the "Information Security Technical Data Exit Security Assessment Guidelines (Draft)" and the "Personal Information Protection Law", the security of personal information and important data pro-duced and collected in China is evaluated. Outbound security risks are determined from the aspects of the data's exit plan, exit quantity, exit scope, exit type, exit sensitivity, exit tech-nical means, and exit target information. The Law on In-ternational Criminal Judicial Assistance introduced a new provision in 2018 that no foreign institution, organization or individual can obtain information from China on the basis of the requirement for mutual legal assistance without the approval of the relevant authorities of the People's Republic of China. Second, for non-critical information infrastructure operators, a more relaxed data exit mechanism should be adopted to promote the free flow of data, taking into account its application value in industrial development, scientific and technological innovation and international trade, as well as the exit security risks of such data itself.

3.3. Some data is prohibited from leaving the country

Under the framework of China's overall security concept, the prohibition of leaving the country is the most stringent situ-ation for "local storage and evaluation of exit" as stipulated in the "Network Security Law" for the cross-border flow of personal information and important data. The qualified do-mestic data is locked locally, and the data controller can on-ly store and process the data in the country, and pro-hibit its cross-border flow. According to Article 21, paragraph 2, of the Data Security Law, such data includes core national data that is "related to national security, the lifeblood of the na-tional economy, important people's livelihood and major public interests." The Measures for the Security Assessment of Personal Information and Important Data Leaving the Country (Draft for Comment and revised draft) further de-tails it as follows: without the consent of the personal data subject, or it may harm the interests of the individual; The departure of data may affect national secu-rity and social public interests;And other circumstances in which the com-petent authorities do not allow exit.

4. Implications for China

In its current phase, "the commodification of personal data has made it one of the most valuable resources on the plan-et". [8]At the same time, international norms on cross-border data flows have also entered an important stage of negotiation and formation, and international digital trade rules centered on cross-border data flows will be de-veloped in a higher and stricter direction. How China re-sponds to and adjusts rules such as the cross-border flow of data is related to whether it can gain a greater advantage in the game of international digital trade rules. In the context of cross-border data flow as an economic driving force, the adoption of localized data flow patterns will make infor-mation asymmetry more serious, which in turn will affect the international competitiveness of our country. Because of strict restrictions on cross-border data flow, a certain mar-ket may be isolated or restricted, it is dif-ficult for domestic enterprises to participate in international competition, and consumers are unable to enjoy the benefits of global scale, which will have a nega-tive impact on economic development. [9]

4.1. To study and improve multiple paths for Chinese data to leave the country

In the past few years, the European Union has also under-gone major legislative re-forms, and despite its extremely strict approach to data protection, it has provided more flex-ible, diverse and legal channels for cross-border data transfer. In this way, businesses are not only able to meet their de-mand for data to flow across borders, but at the same time meet the regulatory objectives of promoting industry de-velopment and ensuring data security. From China's per-spective, with the continuous improvement of network and data security technology and industrial capabilities, under the current legal framework, there are already a series of strict security assessment processes, authentication mechanisms for personal infor-

mation, and standardized contract management provisions for data outbound activi-ties. However, as the data security situation becomes in-creasingly severe and users' awareness of privacy protection increases, the existing measures may not be enough to fully meet the regulatory needs. Therefore, we can begin to ex-plore whether it is necessary to include the concept of "equal protection" in the consideration of the legality of data leaving the country. In today's era, the protection of person-al information rights has become particularly important. For those countries and regions that have established a relatively mature personal information protection system, especially some economic powers, such as the European Union, Singa-pore, etc., it is necessary for us to carry out in-depth evalua-tion and analysis. These countries not only have advanced laws and systems in place to ensure data security and privacy, but they have also become indispensable partners in global digital trade. To this end, an integrated evaluation methodology that combines the "principle of reciprocity" and the "practical needs of national governance" can be used. In other words, on the basis of confirming that the data protection level of these countries and regions has reached a certain standard, while taking into account the actual situ-ation of their management capacity and technical level, a determination method can reflect the advanced level of data protection and has a certain flexibility. In this way, after careful assessment, these regions can be included in a special "white list" in order to reduce or eliminate unnecessary ob-stacles and burdens that may be encountered in the transfer of data to these countries and regions.

4.2. On the basis of hierarchical and classified data management, a more refined data exit management policy will be adopted

On the one hand, formulate and introduce data classification guidelines or standards at the national level as soon as pos-sible, and clarify the scope of important data as soon as pos-sible to clarify the "negative list" of China's data exit. When formulating relevant policies and rules, it is necessary to clearly define the connotation and extension of data, espe-cially the definition of "important data", and avoid its scope being arbitrarily expanded. [10]The purpose of this is to en-sure that, in international negotiations,China can justify and justify restrictions on cross-border flows based on the im-portance of each type of data. At the same time, definitions of critical information infrastructure and important data should not be generalized. On the other hand, in accordance with the requirements of the cross-border data flow system established by the Cyber Security Law, the Data Security Law and the Personal Information Protection Law, it is proposed to revise the provisions of the previously issued and imple-mented administrative regulations and departmental rules such as the Map Management Regulations and the Measures for the Management of Population Health Information (Tri-al), which have inconsistent provisions on cross-border data flow in industrial fields. For example, it can be consistent with the Personal Information Protection Law and other upper laws, and add the path for security as-

sessment, certifi-cation and other data to leave the country legally; It could also provide for technical convergence in legislation, and add exceptions such as "laws and administrative regulations have other provisions on cross-border data provision, and follow those provisions" to the existing provisions.

4.3. We should vigorously carry out international cooperation and take an active part in the formula-tion of international rules

In today's information explosion and data-driven era, the rapid development of the Internet and continuous progress in digital technology have deeply rooted the words "connectivi-ty,collaboration,openness and sharing" in our lives.In this context, cross-border data flow, as a new phenomenon, has not only had a profound impact on business operations and economic activities, but also put forward higher requirements for the protection of personal privacy.Therefore, regulatory cooperation on cross-border data flows at the international level has become an urgent issue to be solved, whether for the sake of national security or to promote international trade.

At present, although some regions such as the European Union have begun to implement positive regulatory measures to reg-ulate cross-border data flows, looking at the world, we still lack a uniform system of international rules or international treaty framework. This situation undoubtedly poses chal-lenges for countries and regions seeking legal ways to carry out cross-border data flows. During this critical window, China must reflect on how to address this global challenge and lay the foundation for the international consensus that may emerge in the future.

The country should have a forward-looking mindset, conduct in-depth studies on global rules for cross-border data flows, and lay out relevant research work in advance. In this way, we can actively participate in the process of building international rules, instead of passively accepting existing rules and per-haps even becoming pawns used by other countries and re-gions. In today's globalized world, it is necessary for China to stand at the height of history, focus on the long term, and ac-tively promote the establishment of a new global data govern-ance order that can guarantee the free flow of data while safe-guarding national interests and users' rights and interests. Only in this way can we hold a favorable position in the increasing-ly fierce international competition and ensure the healthy and sustainable development of our country's digital economy.

References

[1] Huang N, Li Y. "The Evolution and Causes of Cross-border Data Flow Regulation under the 'Triple Dilemma' Choice"[J]. Journal of Tsinghua University(Philosophy and Social Sciences), 2017(05): 172-182.

[2] Ding X D. Legal Reflections and Institutional Restructuring of Cross-border Data Flows —— With a Commentary on the Data Export Security Assessment Measures[J]. Administrative Law Review, 2023(01): 62-77.

[3] Guzman A T, Meyer T L. International Soft Law[J]. Journal of Legal Analysis, 2010(01): 171-225.

[4] OECD Guidelines, §16.

[5] OECD Guidelines, §18.

[6] Gao H Z. The legal logic and optimization path of tripartite governance of privacy, personal information, and data[J]. Law and Social Development, 2022(02): 207-224.

[7] Gonzalez Fuster G. The Emergence of Personal Data Protection as a Fundamental Right of the EU[J]. Springer, 2014(02): 214.

[8] Shan W H, Zheng N. From the perspective of the "Data Privacy Framework," the rules game of cross-border data flows between Europe and the United States[J]. Pacific Journal, 2024(04): 73-88.

[9] Gao S X, Liu W Q. Data Cross-border Flow Regulation and Its Countermeasures - A Discussion on Article 37 of the Cybersecurity Law[J]. Journal of Xi'an Jiaotong University(Social Sciences), 2017(02): 85-91.

[10] Liu J R. Towards Global Regulation of Cross-Border Data Flows: Fundamental Concerns and the Chinese Approach[J]. Administrative Law Review, 2022(04): 73-88.