Proceedings of ICGPSH 2026 Symposium: EdTech & AI in Learning: Large Language Models in Business, Politics, and Humanities
DOI: 10.54254/2753-7048/2026.LD32786

Risks and Regulation of Cross-Border Personal Data Flows in the Digital Age

Ruojin Tong

International Law School, East China University of Political Science and Law, Shanghai, China
3156989939@qq.com

Abstract. In this time of internet, we have the cross border flow of person information, although it develop our economy, many urgent problems occur by those flow. Key situations are digital consumption and platform service; global corporate operation and management; international cooperation. The process of cross border flow of personal information during development period is actually the process of advancement for digital economy, it's from free-flowing to regulation- based circulation. Risk of cross-border flow of personal data in digital age contains infringement on individuals rights, country data security and company's operation conforming to rule. Enhance in three dimensions simultaneously to turn on the corresponding regulation paths: empower data subjects, establish a state-guided evaluation system for data exports, and upgrade corporate compliance services. Provide useful references for this research to promote the secure, efficient and order cross-border flow of personal information worldwide.

Keywords: Cross-border personal data, Data security, Empowerment mechanisms

1. Introduction

With the further develop progressment of digital globalization,cross-border flow for individuals' information has become an indispensable parts in digital economy growing process. At the same time, they bring multiple challenges to national data security and personal data rights protection, and have become a focus of academic attention. Some experts think that cross-border transmission of personal information is restricted due to different laws and enforcement mechanisms between countries, which should be solved through multiple agreements [1]. Some people believe that data rights should be protected by setting rules for cross-border flow of data [2]; Academy is worried about regulation model over cross-border going around of personal data, and different conclusions comparing international frame work. Research on risk classification and regulatory paths for cross-border personal data flows in the digital age is also lacking. Therefore, this paper explores cross-border personal data flow in the digital age and sequentially discusses its actual situation, identifies risk types, and builds a risk regulation system. To provide theoretical references for other countries in the process of balancing data freedom and security, and refining the governance rules for cross-border data flow.

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2026.LD32786

2. The contemporary landscape of cross-border personal data flows in the digital age

Data has inherent fluidity, the healthy development of the Internet industry and the dissemination and update of information and knowledge are all based on the free movement of data [3]. In the digital age, like "new currency", become more and more valuable resources for drive world social-economy progress. With the progress in global development and info revolution, for the digital economic we cannot avoid cross-border data flow. Personal data due to the personal nature of itself is important for economic development, social governance, national security and other field [4]. As a result, cross-border transmission of personal data has become a common occurrence in the global economy and society.

2.1. Primary scenarios for cross-border personal data flow in the digital age

In this digital era, there are cross-border flow of personal data everywhere in society and economy. Mainly refers to the data collection, processing , use and trade. Such simple situations can be summarized as follows:

First, digital consumption and platform service. This is the most direct link of people in the digital era, and also the most common scenario of personal data flow. That is, cross-border e-commerce, international social networking sites and search engines. These organizations take users' Identity Information, payment data, browsing data and so on, and then transfer them across borders, and analyze them in their own data centers. This can make personalized recommendation, targeted service etc. [5] Second Global corporate operation and management. In the process of data globalizing, cross-border data flow is now more important for the global economy than traditional cross-border trade and investment. In the context of this situation, multinational corporation, global industrial chain and supply chain trade form has developed rapidly. Multinational corporations, for example, integrate and convey personal data such as employees' information and customers' contracts from different subsidiaries to the headquarters for global analysis and management of human resources, finance and customer information. Therefore, personal data flows worldwide with commercial activities and industrial chains. Third International Cooperation. The actions of governments and public institutions within international cooperation are also important scenarios of cross-border personal data flow. International Cooperation: use of personal information in various contexts like International Health care, fighting transnational crimes, dealing with immigration etc. It assists in managing & working alongside government/public agencies such that the intl. Order stays stable [6].

By reviewing the above scenarios, the main occasions for cross-border personal data flow are to facilitate certain functions of users' services or circulate with the architecture of globalized business models, penetrating every corner of life.

2.2. Developmental characteristics and trends in cross-border personal data flows

As stated above, cross-border flow of personal data is not a fixed state. Their development is inherently related to the progress of the digital economy, and they have shown a path of free flow - regulation - control.

The first one is the scaling up of flows. With the development of digital economy, the quantity of transferred data have become more and more large scale compared with scattered transmission in early days. And it is all over the world, which provides basic support for global digital services. Second, there is a fragmented regulation. Currently, no unified global framework exists. EU's strict

DOI: 10.54254/2753-7048/2026.LD32786

regulations about personal data that can be cross-border compete, compromise and converge with USA's bilateral or multilateral agreements which strengthen cross-border regulation of data form the fundamental structure of international regulatory landscapes of cross-border flow of personal data [7].

The course of cross-border personal data flow should not longer strive for absolute freedom or control, but rather keep a steady stream of personal data crossing borders according to common rules. Although there are already some patterns formed by developed countries, countries need to work together through economics and law in the complex international situation to explore and build a new order of cross-border personal data management. And the new order will promote cooperative innovation, be more in line with national interests that each country is pursuing at present. Promoting the safe, efficient and orderlies movement of personal data across borders is to meet develope ment requirem ents of digital age.

3. Types of risks in cross-border personal data flows in the digital age

Cross-border flow of personal data involves national interest, industrial interest and risk control. Personal data has the attributes of personality rights and great property value [1]. Cross-border data flow across national borders, the data collection processing chain all over the world supervision is difficult. Technologies are susceptible to theft and misuse, heightening associated risks to trade security.As a result, in the digital age era, the risk of cross border personal data flow has evolved from just one person's privacy violation to a major problem for both people's right and national security as well as business operation.

3.1. Risks to individual rights

In the digital age, with the large-scale generation and transmission of information, people are becoming more and more transparent, and the demarcation line of data rights is also gradually blurring,making personal data easily infringed. If the collection and transmission of personal information go beyond the original intention of use, there is a risk that sensitive information will be disclosed or that the personal data will be abused, invading people's privacy and rights to their person. Cross-border e-commerce, when consumers place orders online, personal data such as order details, Delivery Address, Phone Numbers etc. will be sent to overseas e-commerce platforms. If these platform fails to take effective protection measure towards personal data, or use the obtained personal information for illegal activities, it is considered as violation of people's privacy [2]. At the same time, with personal data flow across country, all links of cross-border transmission may be involved different countries and regions. Putting the victim in a predicament that there is no remedy for violation of rights. International court cooperation: all sorts of issues what law it is, how you get the evidence and then there's enforcement of judgment. A single data infringement may trigger jurisdictional claims by more than one jurisdiction, e.g., the data subject's location or the place of business of the data controller. Rights holders are often in the predicament of how to determine which country's law should be applied and where to sue. In terms of personal experience, the high cost and inconvenience of litigation make this way of redress actually unachievable.

3.2. National data security risks

The 'PRISM' incident confirmed that the United States had penetrated into the network system abroad to illegally obtain data in other countries and transfer it across borders, thus invading and

DOI: 10.54254/2753-7048/2026.LD32786

threatening the national security of other countries. Although personal information is usually scattered, the foreign institution can gather large scale , system x cross border flow in order to understand the domestic social condition,analyze polit and military situation . It's big trouble of our country sovereignty , major national interest. Taking Didi Chuxing as an example. As a commonly used domestic ride-hailing application, it contains sensitive user information such as frequently used addresses, travel paths and geographical Information. Company went to list on the New York Stock Exchange without Chinese regulatory authorities' approval. This move was accused of possibly involving sensitive data leakage and threatening national security. Subsequently, some relevant Chinese government departments carried out a cybersecurity inspection and ultimately punished the company for illegal collection of users' data and threatening national security. In addition, cross-border leakage of personal data may also cause damage to the national sovereignty of data. Data sovereignty is the external representation of a country's highest power in the field of data. When a country is unable to manage and protect the storage, use and flow of personal data after it crosses borders, this means that the country has lost effective control over these data. Parties overseas can deal with and inspect freely such data which violates straightly China's data sovereignty [3]. The losing data sovereignty will generally have an impact on a nation's economy and technology progress, which limits their ability in world digital economies.

3.3. Operational compliance risks for enterprises

It was mentioned before that different countries' Regulations on cross border transmission of personal data are not consistent. Different countries' Data protection measures and circulation regulations may lead to conflicts of legal applicability. Enterprises with international business and data transmission involve multiple jurisdictions' data regulation requirements, resulting in a series of operational compliance risks. The most typical one is that there will usually be problems regarding the enforcement jurisdiction over overseas operating enterprises. In such cases, with different governments having a potential interest in the same dataset according to its own nations' laws. For instance, according to GDPR if any company which provides goods or services to the EU residents then it should follow GDPR even if they are not based in the EU or use domestic machinery/equipment. Wherever there is a processing of personal data by the data subject on behalf of an enterprise, it has to follow this regulation [4]. The passage of the US Congress' Clarifying the Law on the Use of Foreign Data Act, which allows U.S. law enforcement to get access to user data that is kept in foreign servers by American companies, from traditional territorial rules [8]. Enterprises therefore have to deal with different regions and reduce their risk mitigation power and operational efficiency.

4. Risk regulation for cross-border personal data flows in the digital age

In view of the personal data right infringement risk, national data security risk, and enterprise compliance dilemma caused by it, we promote the relevant regulation paths in coordination at 3 levels: empowering individual, state leading cross border data transfers assessment system forming and enterprise complying optimization service. And thus makes a cross-border personal data flow regulation plan as per the nations' situation.

DOI: 10.54254/2753-7048/2026.LD32786

4.1. Strengthening data subject empowerment mechanisms

Personal data essentially relates to people, and any regulation lacking the protection of individual rights lacks legitimacy. As mentioned above, increased openness in the digital era has resulted in a severe deficit of people's right to know, control and seek compensation for cross-border data, thus losing the dominant power over their own data. The following ways can be used to empower data subjects.

On the one hand, we need to build up a major information consent system. Users encounter lengthy and obscure private policy in the regular "notice & consent", which they don't fully understand but have no insight on the risks of data transmitted across borders. They have no choice but to click "agree", losing all power to decide where their data goes and what is done with it. Under the substantive informed consent mechanism, platforms should separately and prominently give pop-up notices when involving the risk of data transfer abroad. Users need to know the destination country or region of their personal information, the application scenario, and the possible risk in order to maximize their right to know and control of cross-border data flow.

At the same time, enhance the rights of data subjects for relief, reducing the difficulty for people to exercise their rights. In the scenario of cross-border data flow, due to the involved countries or regions, people often find that there is no place to seek protection. To this end, the state can make jurisdiction rules favorable to individuals and clearly affirm that domestic courts have jurisdiction over foreign-related personal data cases. This way, it won't be necessary for people to sue abroad, reducing the threshold for judicial remedy. At the same time, empower the Procuratorate to bring public interest litigation for personal data protection. In the case of large-scale cross-border data breaches, such litigation can become an efficient path for accountability to protect people's right to remedy in terms of cross-border data flow.

4.2. Establishing a state-led cross-border data transfer assessment mechanism

The cross-border flow of personal data involves the interests of individuals, as well as national security and public interest. Being the highest sovereignty, the state should establish a data security review mechanism to carry out preemptive evaluation and supervision on high-risk cross-border transfer of personal data. Ensure the secure and stable circulation of personal data, guard national data security, and advance the construction of the state-led cross-border data transfer evaluation mechanism.

Top priority in the state-led cross-border data transfer review mechanism should be giving way to establishing the cross-border personal data security review framework. This mechanism needs to clearly specify standards for judging risks of cross-border data transmission, assess the necessity of regulatory actions on cross-border data flow, effectively strengthen the security barrier for cross-border personal information, and ensure that such data transfer serves the basic purpose of achieving "legitimate public policy objectives" [9]. This check shouldn't go for a formality, but rather to see if the handing over of person data is safe. For example, whether to transfer personal data at all: Is the transfer really necessary for the needs of corporate or individual business? Are there other methods that can be done domestically? Through analysis of the purpose of transfer and foreign environment, strengthen the national competent department's control over the cross-border personal data transfer to guarantee the legal, reasonable and necessary of such transfer operation, protecting nation date security. And at same time it's not a static assessment for outbound personal data, it can change on the go along with market condition and national situations etc. The validity of assessd personal info must be created. Should national legal changes occur, significant data breaches arise, or the purpose

DOI: 10.54254/2753-7048/2026.LD32786

of data transfer change during this period, reassessment must be sought. Also the State should set up related supervising department to do supervision and random inspect on the outbound data to be evaluated whether by enterprises or individual, so as to keep our evaluation system going well and let our assessment result open and just.

4.3. Optimizing cross-border data compliance services for enterprises

In the messy international rules of cross-border data flow, there are contradictions between the compliance regulations of different areas. Frequent constraints of enterprises during operation reduce the efficiency of operation and increase cross-border compliance cost. Thus, the regulatory system needs to provide enterprises with executable compliance tools, improve the cross-border data compliance service, and create a good compliance environment.

Establish and improve the industry self-regulation framework for cross-border flow of personal data. Under the legal framework, promote proactively to achieve data security and free flow at the same time. For example, the United States Data regulatory system places more emphasis on self-regulation by industry bodies and ex-post accountability. Binding obligations usually come into effect by signing contract, corporate members in the association means accepting the self-regulatory rules. This is done using precisely crafted contractual and transactional means for the liberalisation of cross-border flow of personal data and growth of international digital markets [10].

Secondly, to promote the marketization of compliance services and offer professional services to enterprises. Developing third-party service providers in terms of data compliance consultation and security evaluation to promote professional cross-border data compliance services for enterprises. At the same time, governments should also add online service function on relevant data entry/exit management web pages such as adding assessment application, contract filing, policy inquiry service etc., so that enterprises can file their data more effectively.

Finally, due to its distinct multi-disciplinarity and cross-dimensionality, digital enterprises need both lawyers to enhance risk-oriented measures and reduce legal risks, as well as technical personnel to participate in data compliance technology R & D to improve the intelligence level of data compliance systems. Therefore, constructing a composite team of data compliance personnel is especially important. Digital Enterprises require to employ specialist personnel in Data Complying aspect and also frame a complying system through multi-professional linkage. On the other hand,they need to step up regular data security compliance training and assessment of their compliance team to raise professionalism level [8].

5. Conclusion

In the digital age, personal information has become a coveted resource sought after by various parties, and cross-border flow of information is everywhere in people's lives. Setting up such risk regulatory systems as countries have to deal with cross-border data flows risks on top of compliance demands and feasibility regarding individuals, states and enterprises. Breaking through the traditional single angle in the traditional National Security - personal Rights - enterprise Operation frame work to expose the system and multi angle characteristics of cross-border personal data flow risk. And propose individual consideration in the risk regulation of cross-border personal data flow, provide reference for balancing data freedom, rights protection and compliance supervision. With the advancement of digital technology, there are always new kinds and forms of cross-border personal data flowing. More targeted research is needed on personal data protection rules and cross-border regulatory cooperation mechanisms in the new context of artificial intelligence, cross-border

DOI: 10.54254/2753-7048/2026.LD32786

data platforms and other fields to provide continuous theoretical support for improving the national governance system for cross-border personal data flow.

References

[1] Zhang Jihong. Restrictions on Cross-Border Transfer of Personal Data and Their Solutions [J]. East China Journal of Jurisprudence, 2018, (6): 37-48.
[2] Ma Qijia, Li Xiaonan. On the Construction of China's Cross-Border Data Flow Regulatory Framework [J]. Rule of Law Research, 2021, (1): 91-101.
[3] Wu, Shenkuo. "Research on Cross-Border Data Flow and Data Sovereignty." Journal of Xinjiang Normal University (Philosophy and Social Sciences Edition), 2016, (5): 112-119.
[4] Ye Kairu. "Extraterritorial Jurisdiction in Cross-Border Data Flow Regulation: An Originalist Examination of the EU's GDPR" [J]. Law Review, 2020, (1): 106-117.
[5] Zhang Zhengzhang, Chen Shuting. Application Dilemmas and Countermeasures for Liability for Data Product Infringement [J]. Journal of Tongji University (Social Sciences Edition), 2025, 36(6): 107-119.
[6] Ma Zhongfa. International Regulation of Cross-Border Data Flow and China's Response [J]. Journal of Political Science and Law, 2026, (1): 3-18.
[7] Xu Duoqi.The International Framework for Cross-Border Data Flows and China's Response [J]. Law Forum, 2018, (3): 130-137.
[8] Chen Bing. A Legal Approach to Compliance Governance for Cross-Border Data Flow in Digital Enterprises [J]. Rule of Law Research, 2023, (2): 34-44.
[9] Chen Si, Ma Qijia. China's Approach to Coordinating Cross-Border Data Flow Regulation [J]. China Circulation Economy, 2022, (9): 116-126.
[10] Xu Duoqi. Legal Safeguards for Bilateral Compliance of Enterprises in Cross-Border Data Flow Regulation [J]. East Asian Law Review, 2020, (2): 185-197.