International Law Protection of Cross-Border Transmission of Personal Information Based on Cloud Computing and Big Data

Xu Ziyi
Hebei University of Economics and Business, 050000 Shijiazhuang, China

Correspondence should be addressed to Xu Ziyi; 20150810238@m.scnu.edu.cn

Received 25 May 2022; Revised 16 June 2022; Accepted 21 June 2022; Published 18 August 2022

Academic Editor: Chi Lin

Copyright © 2022 Xu Ziyi. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Cross-border data flow brings new growth and opportunities for the development of digital economy, but disordered cross-border data flow may damage national security, public interests, enterprise interests, and data sovereignty. At present, the unified rules for global regulation of cross-border data flow have not yet been formed. The existing rules are mainly led by developed countries like Europe and the United States. There is huge room for improvement in the international legal protection of cross-border transmission of personal information. This paper introduces the privacy protection mechanism of personal information data under the digital trade environment in China, that is, the privacy protection framework under the background of big data, cloud computing, and the cloud service selection method of data life cycle privacy protection. At the same time, we combined with many problems existing in the cross-border transmission of personal privacy information in China and compared with foreign advanced experience, and this paper puts forward China’s response path to clarify the obligations of data controllers and exporters, improve the responsibilities of regulators, improve the legislation of cross-border data flow, and improve the operability of the law; we vigorously carry out international cooperation and actively participate in the formulation of international rules, so as to further protect the rights and interests of personal privacy information protection.

1. Introduction

In today’s society, with the rapid development of informatization, especially with the support of cloud computing, big data, Internet of Things and other technologies, the era of informatization and big data not only brings convenience to people’s life but also increases the concentration of social data. At present, the collection, storage, processing, and application of personal information have reached an unprecedented level. With the in-depth development and continuous development of cross-border e-commerce and other businesses, and with the more and more extensive collection and processing of personal information, the risks are also higher and higher. For relevant enterprises, how to make natural persons clearly understand the scope of information collection, the location of information storage, and the purpose of information analysis is a very important notification. On the other hand, if the relevant enterprises that control and stand as personal information cannot fully and clearly understand the personal information protection laws, and do not know which information collection or information processing should be clearly authorized by the data subject, it will even produce greater compliance risks. We should pay more attention to the process of data protection in different jurisdictions, especially in the process of cross-border data transmission. Some developed countries have started the legal practice of cross-border data flow, typical examples are the chapter on digital trade in the United States–Mexico-Canada agreement (USMCA) led by the United States, and the EU-U.S. privacy shield agreement reached between the United States and the European Union, and the EU general data protection regulation (GDPR). The rules on cross-border data flow in these three specifications provide an institutional model for cross-border data sharing. China should learn from these mature international mechanisms on the control of cross-border data flow and combine with its own data protection practice, from the establishment of data classification and review system,
strengthening the construction of technical security, improving the rights and responsibilities of data subjects, strengthening international cooperation and other dimensions, build a legal supervision mechanism for the collection, and release of coordinated cross-border data flow, so as to achieve the incentive compatibility between data exit governance and economic growth needs [1].

2. Literature Review

No matter how personal information is stored, and its most important function is to identify the identity of natural persons and reflect the activities, behaviors, and preferences [2]. Moreover, due to the development of big data and cloud computing technology, the fragmented information can also identify the identity of a specific natural person and reflect the activities of the natural person after integration, analysis, and processing. Therefore, some scholars believe that in the context of international law, the so-called "personal information" refers to the information that can identify or have identified the identity of a natural person alone or in combination with other information, or the information that reflects the customary preferences, identity, and status of a specific natural person [3]. In the process of research, the author found that "personal information" and "personal data" are mixed or defined together in bilateral and multilateral international treaties and other normative documents. However, whether personal information or personal data, its connotation emphasizes the identification of identity and the mapping of personal characteristics, habits, and preferences [4].

Domestic research on the international law of personal information protection mostly focuses on specific legal rules, while foreign research mostly starts from regional documents and only studies the role of relevant documents in the protection of personal information in this region, but there are relatively few papers on the international legal rules as a whole. Moreover, the basic principles of international legal protection of personal information are rarely mentioned in the existing research, and the research on the rights of data subjects mostly focuses on the historical evolution, and the research on the cooperation and connection of the rights of data subjects is not clear enough [5]. This paper intends to study the international legal rules of personal information protection as a whole. Combining the privacy protection framework in the context of big data and cloud computing and the cloud service selection method model of privacy protection in the data life cycle, more intuitively finding the problems of international legal protection of personal information, we sort out the principles of international legal protection of personal information in different documents and summarize the basic principles of personal information protection; analyze the rights of data subjects and the obligations of data controllers and data processors, and put forward relevant improvement suggestions for the insufficient provisions; and study the international cooperation on personal information protection, clarify its cooperation mode, analyze the cooperation effect, and clarify that the cross-border flow of personal information should be promoted and guaranteed by signing bilateral or multilateral treaties [6].

3. Privacy Protection of Personal Information in My Country under the Digital Trade Landscape

With the advent of the era of big data, learning and analysis technology has become a new wave to solve international law problems. Through the data model framework, the process of information storage and cross-border transmission can be more intuitively understood, so as to find the existing legal problems. This part introduces the construction of data privacy protection framework and the cloud service selection method of privacy protection through the data life cycle, and understands data privacy security mechanism, which will affect the country's specific design and selection of international cooperation mechanism and international rules. China needs to think prospectively about the global rules of cross-border information flow, and become the creator of international rules.

3.1. Privacy Protection Framework. From the perspective of cloud service scenarios, this section constructs the research framework of data privacy protection in the cloud environment; attributes the data privacy security in the cloud environment to the three links of cloud service selection, access control, and trusted implementation of privacy policies; and tries to ensure the privacy security of users in these three links. This section mainly describes the application scenarios and assumptions of the proposed data privacy protection framework in the cloud environment. For the detailed application scenarios of the research contents of each part in this framework, please refer to the scene description of each chapter [7]. The cloud application scenario is shown in Figure 1.

As shown in Figure 1, in the above cloud application scenario, users can interact with cloud service providers indirectly or directly based on trusted third parties. Aiming at the above cloud application scenarios, this paper solves three problems: the choice of cloud services for data privacy protection, the protection of user data and identity attribute information, and the implementation of privacy policies. Due to their different emphases, they have different dependences on trusted third parties in this scenario. Therefore, this data privacy protection framework needs to be built at both ends of the trusted third party and the cloud service party. Its framework is shown in Figure 2.

As shown in Figure 2, in this framework, the left side is the deployment scheme of the cloud service selection method for data life cycle privacy protection proposed for the service selection problem for data privacy protection in this framework, and its components are deployed in a trusted third party. In the middle, it is the problem of protecting the privacy of user data, identity, and attributes [8].

3.2. Cloud Service Selection Method for Data Life cycle Privacy Protection

3.2.1. Scene Description. The cloud service selection scenario in this article is shown in Figure 3.
As shown in Figure 3, in the cloud service selection application scenario based on a trusted third party, the user’s selection of cloud service providers is completed by the trusted third party. This third party is responsible for supervising the status of cloud services. For example, TapInSystems, TechOut, and Hyperic can test the availability, response time, throughput, and other information of cloud services provided by Amazon. This paper studies such

![Figure 1: Schematic diagram of cloud application scenario.](image)

![Figure 2: Data privacy protection framework in cloud computing environment.](image)
third-party scenarios [9]. Specifically, in the above scenario, the trusted third party needs to regularly send performance query requests to each service and accept the performance parameters returned by each service to sort out and maintain a service library. After that, when the user submits the cloud service selection request, the trusted third party queries the service library according to the user’s request and gives the cloud service recommendation list for the user to choose. For the above cloud application scenarios, this paper presents a cloud services selection method for data lifecycle privacy protection [10]. This method extracts and quantifies the data privacy protection capability (CoPP) index of each target cloud service from the perspective of data lifecycle in the cloud. On this basis, it calculates the data privacy protection capability (CoPP) and gives the cloud service recommendation list for data privacy protection.

3.2.2. Evaluation Index System. The cloud service selection evaluation index system, as the standard to measure and detect cloud services, mainly takes each stage of the data lifecycle in the cloud environment as the index of data privacy protection capability (CoPP), including seven stages of data generation, transmission, storage, access, derivation, archiving, and destruction, as well as the data privacy security mechanism under each stage, as shown in Table 1.

Next, this paper analyzes the influencing factors of the privacy protection ability of the privacy security mechanism in each stage. Due to space reasons, we take each privacy security mechanism in the data generation stage as an example, including identity authentication, access control, and authorization mechanisms, which need to be analyzed and evaluated from the following aspects, as shown in Figure 4.

Identity authentication is an effective means to verify the identity of users, mainly in several ways in Figure 4. In cloud services, one or more ways are often used at the same time [10]. Generally speaking, it is generally believed that the security of the above authentication methods increases from top to bottom, and the security of multiple authentications is higher than that of single authentication [11]. Authorization mechanism is a method to grant permissions to reliable users. As shown in Figure 4, its security judgment mainly includes authorized environmental monitoring and judging whether it is authorized in real time. Among them, environmental monitoring includes supplier and client detection. At present, cloud computing providers generally use environmental monitoring to ensure the security of authorization in the authorization process. Access control is an important guarantee for users to safely operate cloud data and prevent privacy disclosure. Its principles and types are mainly shown in Figure 4. The integrated access control strategy integrates the technical advantages of a variety of mainstream access control and more effectively ensures the integrity and privacy of data. Therefore, the evaluation of access control should be comprehensively considered from two aspects: the satisfaction of principles and the security of policy types [12].

4. Current Situation and Deficiencies of Cross-Border Transmission and Protection of Personal Information in China under the Background of Digital Trade

4.1. Lack of Integration with the International Protection Model. The concepts of digital trade have been clearly defined, and cross-border transfer of personal information has also been clarified [13–15]. The protection and free flow of personal information must not be neglected. Secondly, it is necessary to protect the cross-border transmission of
personal information at the level of international law. On the one hand, digital trade, as an emerging economic momentum, is in the process of enhancing the vitality of the global economy. On the other hand, the frequent cross-border flow of personal information puts forward requirements for international law; secondly [16], it poses a threat to the security of personal information, and the necessity of international legal protection of personal information is evident [17, 18]. From the analysis of the international legal protection of cross-border transmission of personal

<table>
<thead>
<tr>
<th>Evaluation index system</th>
<th>Life cycle data</th>
<th>Privacy security mechanism at all stages</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data generation G</td>
<td>Access control protocol selection (P1)</td>
<td></td>
</tr>
<tr>
<td>Data transmission T</td>
<td>Autonomous access control (P2)</td>
<td></td>
</tr>
<tr>
<td>Data storage S</td>
<td>Anonymous access control (P3)</td>
<td></td>
</tr>
<tr>
<td>Privacy protection capability (CoPP)</td>
<td>Digital certificate (P4)</td>
<td>Transmission encryption (P5)</td>
</tr>
<tr>
<td>Data access Ac</td>
<td>Virtual machine isolation (P6)</td>
<td></td>
</tr>
<tr>
<td>Data derivation reuse R</td>
<td>Legal storage (P7)</td>
<td></td>
</tr>
<tr>
<td>Data archiving Ar</td>
<td>Storage encryption (P8)</td>
<td></td>
</tr>
<tr>
<td>Data destruction D</td>
<td>Identity authentication (P9)</td>
<td></td>
</tr>
</tbody>
</table>

| Table 1: Evaluation index system of cloud service selection. |

<table>
<thead>
<tr>
<th>Identity P1</th>
<th>Static password</th>
<th>The smart card</th>
<th>SMS password</th>
<th>Dynamic password</th>
<th>A digital signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access Control P2</td>
<td>The strategy principle</td>
<td>Principle of least privilege</td>
<td>Principle of least leakage</td>
<td>Multi-level security principle</td>
<td></td>
</tr>
<tr>
<td>Authorized Environment Detection</td>
<td>Supply-side detection</td>
<td>Client detection</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Real-time detection type</td>
<td>Real-time authorization</td>
<td>Non-real-time authorization</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure 4: Evaluation of privacy security mechanisms in data generation stage.
the WTO and the UN Norms is the most representative, providing a framework and model for national legislation [19, 21]. There are many deficiencies in the existing international protection methods for personal information. The scope of application of bilateral agreements is too narrow, the process of negotiating and negotiating with different countries one by one is relatively complicated, and the existing bilateral protection methods are relatively simple as shown in Figure 5.

The cross-border transmission of personal information has been paid more and more attention; firstly, China’s efforts in cross-border information protection cannot be ignored. In recent years, China has used the Boao Forum, the Asian infrastructure open bank, the BRICs countries, and the Belt and Road initiative to carry out regional cooperation or rule negotiation on cross-border information flow, so as to enhance China’s voice in this field [21]. But compared with other digital trading countries in the world, China lacks cooperation in cross-border information protection, unable to integrate with the international protection model.

There are two reasons for the lack of international cooperation in personal information protection: firstly, in China, the regulation of cross-border data flow is distributed in various laws, regulations, and departmental rules, which are relatively scattered. In general, the existing regulations severely restrict the transfer of domestic data to overseas. China tries to avoid the possible national security risks and personal privacy risks of cross-border data through data localization and retention. But in an environment where cross-border data flows act as an economic engine, the protection measures may aggravate the information asymmetry phenomenon, thus affecting the competitiveness of our country, and there is a lack of confidence in international negotiations on personal information protection. Harsh cross-border data flow restrictions may make a market isolated or limited, it is difficult for the domestic-related enterprises to participate in the international competition, and consumers cannot enjoy the benefits of global scale, which bring negative impact to economic development [22]. Secondly, although China’s digital trade has developed rapidly in recent years, it is still in the exploration and initial stage, and many digital enterprises are still in the stage of “going out.” There is still a large gap compared with the level of personal information protection in developed countries; once China joins regional or international information protection organizations or platforms, digital enterprises are bound to be constrained in the protection of cross-border transmission of personal information, which will increase the operating costs of enterprises and is not conducive to China’s digital enterprises to open the international market in a short time [20, 22].

4.2. Imperfect Legal Provisions on Personal Information Protection in China. The role of the development of big data in promoting global economic growth should not be underestimated. As one of the countries with the best development momentum of digital trade, China is still not in place in protecting the personal information transferred across borders, which is mainly manifested in the imperfect legal provisions. China has not formulated a special personal information protection law, the relevant legal norms and systems are not perfect, and the data commissioner system and information authentication system have not been established. The lack of personal information protection law makes it difficult to get relief when the interests of information subjects are infringed, and it is also unable to connect with the protection mode of other countries. China’s special laws are under preparation, which also gives the public a shot in the arm. The special laws will be able to protect the legitimate information rights of individuals to a greater extent, and the contents on the protection of cross-border transmission of personal information will also be stipulated [23, 24]. The national security law also deals with the cross-border flow of personal information data; that is, important data should be stored locally and other data should be evaluated before cross-border transfer [25].

Firstly, important data are not clearly defined, and the scope of important data cannot be known; secondly, only before the cross-border transfer of data is determined, the supervision during and after the event is difficult to reflect, and the existing supervision system is difficult to implement in place. The essence of security assessment is to serve the exit of data. We should promote the cross-border flow of data on the premise of ensuring security. Only using security assessment as a supervision means in a single way may not meet the needs of real massive data transfer [26] as shown in Figure 6.

5. Legal Protection Countermeasures for Cross-Border Transmission of Personal Information in China

5.1. Actively Participate in International Cooperation on the Protection of Cross-Border Transmission of Personal Information. In an era of connectivity, collaboration, openness, and sharing as themes, cooperation at the international level on cross-border data flow regulation is inevitable. Despite the active regulation of cross-border data flows by regions or countries such as the EU, on a global scale, unified international rules and treaty norms have not yet been formed. In this window period, China needs to make forward-thinking about the global rules of cross-border data flow, deploy research in advance, and strive to be
the builder of international rule making, rather than becoming a passive recipient of the rules.

Due to the need for the development of digital trade and expanding market influence, it is difficult to shake the leading position of Europe and the United States in rule making. In concrete practice, on the one hand, China should actively participate in the discussion on cross-border data flow rules on international platforms and issue China’s voice on behalf of the interests of Chinese enterprises; on the other hand, regional negotiation platforms such as the Regional Comprehensive Economic Partnership (RCEP) and Free Trade Area of the Asia-Pacific (FTAAP) provide favorable conditions for China to actively participate in rule making, and promote the construction of regional rules for cross-border transmission of personal information with the help of regional comprehensive economic partnership [25]. As China’s status in international affairs improves, China can make better use of changes such as the Boao Forum, the Asian Infrastructure, the Open Bank, and the BRICS Belt and Road strategy to carry out regional cooperation agreements or rule negotiations on cross-border data flow, so as to enhance China’s voice in this field. In short, China’s data power image through the negotiation of multilevel international rules or the construction rate that matches China’s international status is not only the need to safeguard domestic interests but also a requirement for ensuring cross-border data flow, the healthy development, and sustainable development of international cooperation.

In addition, compared with China, developed countries have higher requirements on domestic personal information protection standards and information transfer conditions. Therefore, China should also strengthen cooperation with trading partners in mutual legal assistance and information law enforcement, keep up with the high standards of personal information protection, and share personal information governance experience. We need to keep close contact with international professional privacy protection organizations, learn advanced experience, reflect China’s determination and confidence in personal information governance, enhance China’s influence and voice in the field of personal information protection, and win opportunities for China’s digital enterprises to enter overseas markets.

5.2. Effectively Learn from International Experience in Cross-Border Protection and Governance of Personal Information. As the two digital trade giants, the EU and the United States have different legal paths for personal information protection, and there are obvious differences in the protection modes between the two countries, which are closely related to the long-standing values and tradition of the rule of law. Many scholars believe that the United States does not pay attention to the protection of personal information, and personal privacy is vulnerable to infringement. The EU’s general data protection regulations are too strict and complicated, which is not conducive to the development of digital trade. It is considered that privacy protection and trade need not be combined. In short, it is difficult to strike a balance between the development of big data and personal information protection. Economies are also exploring the path of both. The EU and the United States are also facing challenges and urgently need to find better solutions. Latecomers should also seek the development of personal information protection from the experience and training of Europe and the United States. As the saying goes, China should learn from others’ strong points, draw on their essence, and learn from the beneficial experience of European and American information protection models to serve the improvement of China’s rules. Both European and American models have advantages and common laws to follow. In order to achieve the expected protection results, we must follow the way of incentive compatibility. If they are incompatible, it is difficult to implement, and we cannot ignore one and lose the other. Otherwise, it will hinder economic development and personal information protection [26].

Therefore, it is necessary to analyze the advantages and disadvantages of each personal information protection mode and whether the system design of personal information governance is scientific. To improve the degree of personal information protection in China, on the basis of summarizing the experience and lessons of personal information governance in developed countries, we should draw useful experience from the two models, not only see the differences between the two but also summarize the common laws. The EU’s cross-border protection model of personal information is characterized by a strict legal system, including the setting of personal information supervision institutions and data protection commissioners. It is worth learning from China’s specific practice of personal information protection to review the cross-border transmission of personal information before, during, and after the event, and clarify the main responsibilities of all parties. China is a civil law country. It is a good choice to learn from the advanced experience of the EU in the formulation of legal norms. Secondly, the personal information protection system of the United States...
combines departmental decentralized legislation with industry self-discipline system, although the effect of departmental decentralized legislation is far less than that of formulating a unified personal information protection law. However, the relatively perfect industry self-discipline system in the United States is still worthy of reference in the practice of personal information protection in China. The industry norms are more flexible. The formulation of self-discipline norms in line with the industry development characteristics and economic development trend in various industries and assisting the government in relevant law enforcement work will be an important direction of personal information protection in the future.

5.3. Vigorously Improve the Laws and Regulations on the Protection of Cross-Border Transmission of Personal Information. In terms of cross-border flow of personal information, China should apply the hierarchical and classified management systems of different cross-border flow management mechanisms to the personal information and important data, general personal information, and business data of network operators, and establish an international data flow circle in line with its own security standards and the needs of industrial interests on this basis. Specifically, first is dual supervision of local data storage and cross-border data flow. China can encourage localized data storage and processing for the reasons of promoting data aggregation and protecting national security. For the flow of cross-border data, China can set a regulatory threshold. For the normal cross-border flow of data, there are no obstacles, but only the cross-border flow of data reaches the corresponding threshold [27].

Second is dual track supervision of personal information and important data. Personal information is essentially different from important data. Personal information mainly protects the private rights of data subjects, while important data focus on the protection of national interests and national security. Due to the significant differences between personal information and important data in regulatory objectives, scope of application, and evaluation procedure indicators, China can formulate regulatory norms applicable to personal information and important data, respectively. The cross-border flow of personal information can be solved based on civil means such as evaluation, agreement, express consent, and certification, while the cross-border flow of important data should mainly rely on administrative supervision [28].

Third, the legal reasons for the cross-border flow of personal information are diversified. Looking at the legitimacy of the cross-border flow of personal information all over the world, it roughly includes the adequacy identification of the information receiving country, the adoption of adequate safeguard measures, authentication mechanism, and interstate peer-to-peer agreement. China can learn from the content above and add legal reasons such as authentication mechanism and adequacy safeguard measures to make the flow of personal information more convenient [29].

6. Conclusion

Digital trade with the Internet as the carrier has greatly promoted the growth of the global economy. At present, Internet users have exceeded 3/4 of the global population. At the same time, it is also accompanied by the transnational transfer of massive information. How to coordinate the contradiction between cross-border transmission of personal information and personal information protection has become an urgent practical problem to be solved. Firstly, there are huge differences in the level of digital technology between countries, and digital trade protectionism still exists; secondly, digital trade lacks a universal global rule system and exists fragmentation of digital trade rules; finally, China lacks perfect legislation on cross-border data flow and cannot integrate with the protection mode of other countries.

To solve these problems, firstly, each country’s norms in the field of personal information protection are not similar, which leads to huge differences in national legal norms. If a country imposes domestic norms on its international dealings with other countries, it is bound to cause conflicts. It is the general consensus of the international community to oppose the implementation of hegemonism and protectionism, so it is necessary in the process of cross-border information transfer countries should carry out cooperation and consultation on this issue, which can effectively reduce the occurrence of conflicts. Whether within the European Union or between the European Union and the United States, data cross-border flow has been realized under a certain legal framework or relevant norms, which provides a reference for China to realize the protection of data cross-border flow. At the same time, China should actively participate in the discussion of cross-border data flow rules on international platforms and make a Chinese voice on behalf of the interests of Chinese enterprises. We learn from RCEP, FTAAP, and other regional negotiations to seek to establish cross-border data flow rules in line with China’s interests. This can enhance the trust of the international market in Chinese enterprises, strive for opportunities for enterprises to participate in global competition, cultivate industry self-discipline in this process, and promote the improvement of China’s data protection level and the sustainable development of related industries [30].

Secondly, China’s personal information protection legal system is gradually improving, but it is still a certain distance from the high level of personal information protection, and little attention is paid to the protection of cross-border transmission of personal information. As an important member of APEC and a new force in the development of global digital trade, China should actively participate in the formulation of international rules for cross-border information transmission, draw on the strengths of others, absorb useful foreign experience, actively connect with international rules, accelerate the process of digital trade globalization, improve China’s information protection level, and play a more important role in the process of digital trade globalization.
References


