10.18686/frim.v2i3.4235

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

Hao Ren

Henan University of Economics and Law, Zhengzhou, Henan 450000

Abstract: Cross-border data is crucial for the digital economy's growth, but uncontrolled transfers risk national security, public interests, corporate interests, and data sovereignty. Currently, cross-border data regulation lacks unified global rules, with existing ones dominated by Europe and the U.S. China needs to improve its international legal protection for cross-border personal information transfer. This paper examines China's mechanisms for personal data privacy protection in digital trade, including frameworks for big data, cloud computing, and cloud service selection for data lifecycle privacy protection. It suggests clarifying data controllers' and exporters' obligations, strengthening regulatory responsibilities, improving cross-border data legislation, enhancing law operability, and advocating for stronger international cooperation and participation in global rule-making to protect personal privacy information rights.

Keywords: Cross-border data; Regulation; International law; Information protection

1. Introduction

In today's fast-paced information technology society, driven by cloud computing, big data, and the Internet, the concentration of data has increased significantly. This growth, especially in cross-border e-commerce, has elevated risks associated with personal information. Ensuring individuals understand the scope, storage, and purpose of information collection is crucial. Businesses must comprehend personal information protection laws and obtain proper authorization from data subjects to mitigate compliance risks. Special attention is needed for data protection processes in different jurisdictions, particularly regarding cross-border data transfers.

2. Status of research

The primary function of personal information is to identify individuals and reflect their activities, behaviors, and preferences. Advances in big data and cloud computing allow even fragmented data to identify individuals[1, 2]. Scholars suggest that "personal information" in international law includes data that identifies or reflects a person's habits and identity. This paper examines international legal rules for personal information protection, combining privacy protection frameworks in big data and cloud computing with models for choosing cloud services. It analyzes principles from various documents, the rights of data subjects, and the obligations of data controllers and processors, offering improvement suggestions. The study also explores international cooperation in personal information protection, proposing the promotion of cross-border data flow through bilateral or multilateral treaties.

3. Privacy protection of China's personal information in the digital trade environment

With the advent of the era of big data, learning and analytical techniques have become the new trend in solving international law problems. By building a fine-grained data modeling framework, the process of storing and transmitting information across borders can be understood more intuitively, thus revealing existing legal issues. This paper partly introduces the construction of a data privacy protection framework across the data lifecycle and the selection of privacy-protecting cloud services [3, 4], and delves into the impact of data privacy security mechanisms on the development of international cooperation mechanisms and the selection of international rules by countries. China needs to think prospectively about the rules of global cross-border information flow and actively participate in the development of international rules [5].

3.1 Privacy protection framework

This section constructs a framework for data privacy protection in cloud environments, focusing on three segments: cloud service selection, access control, and the trustworthy implementation of privacy policies. It aims to ensure user privacy in these areas. The framework addresses application scenarios, including direct or indirect interactions between users and cloud service providers through trusted third parties.

The main issues are cloud service selection for data privacy, protection of user data and identity attributes, and implementation of privacy policies. Due to different focuses, the reliance on trusted third parties varies. The framework, depicted in Fig. 2, includes components deployed at both trusted third parties and cloud service providers, addressing data lifecycle privacy protection and user data privacy.

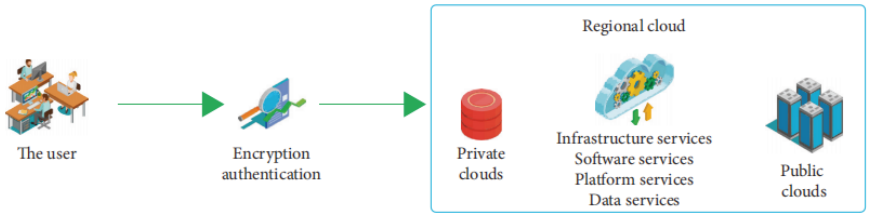

Figure 1 Schematic diagram of cloud application scenarios

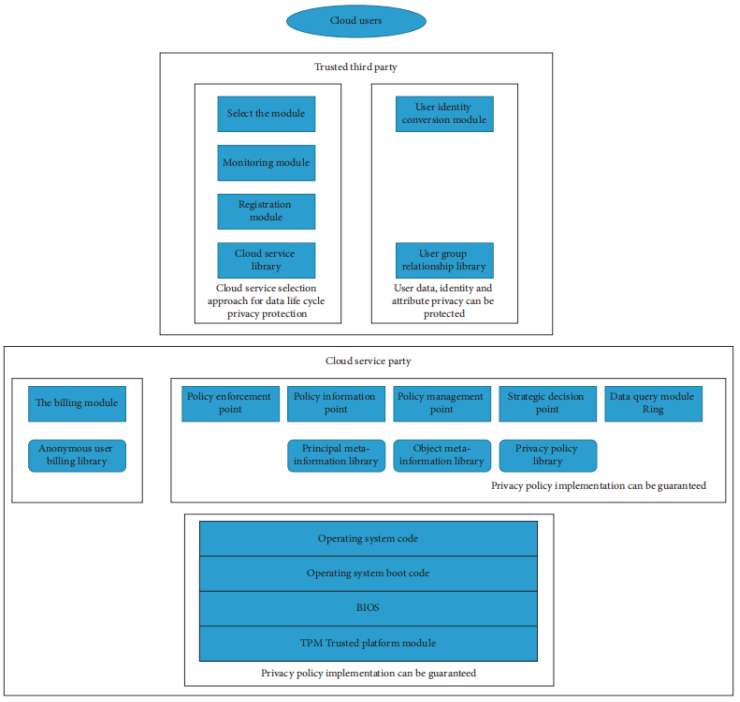

Fig. 2 Data privacy protection framework in cloud computing environment

3.2 Cloud service selection approach for data lifecycle privacy protection

3.2.1 Scenario Description

The cloud service selection scenario in this paper is shown in Figure 3.

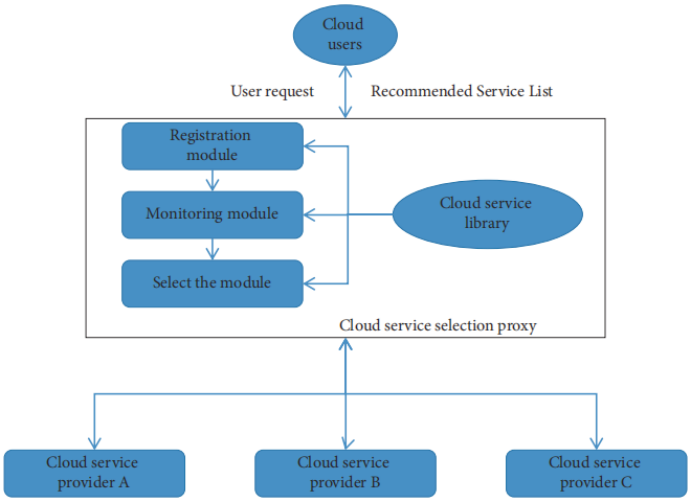

Figure 3 Cloud application scenario based on trusted third party

Third-party scenario. Specifically, in the above scenario, the trusted third party needs to periodically send performance query requests to each service and accept the performance parameters returned by each service to organize and maintain a service library. Later, when the user submits a cloud service selection request, the trusted third party queries the service library based on the user's request and gives a list of recommended cloud services for the user to select. For the above cloud application scenarios, this paper proposes a cloud service selection method for data lifecycle privacy protection. It is an approach that extracts and quantifies the data privacy protection capability (CoPP) metrics of each target cloud service from the perspective of data lifecycle in the cloud. Based on this, the data privacy protection capability (CoPP) is calculated and a recommended list of cloud services for data privacy protection is given.

4. Status quo and deficiencies of cross-border transmission and personal information protection in China in the context of digital trade

4.1 Lack of integration with international protection organizations

The concept of model digital trade has been defined, clarifying the cross-border transfer of personal information, emphasizing both protection and free flow. It is crucial to safeguard China Telecom's personal information at the international law level. Digital trade, as an economic driver, boosts the global economy but also increases the need for international legal protection of personal information due to its frequent cross-border flow.

Internationally, bilateral privacy agreements like those between the US and Europe, and regional norms by the EU and APEC, set high standards for personal information protection. Despite China's rapid digital trade growth, it remains in the early stages, with digital enterprises exploring international markets. However, China's personal information protection lags behind developed countries, and joining international protection organizations may impose stricter requirements, raising costs and potentially limiting market expansion.

5. Conclusion

Digital trade has significantly boosted the global economy, with over a third of the global population now online. However, this growth has led to extensive cross-border transmission of personal information, raising urgent issues of coordination and protection. Differences in digital technology levels among countries, lack of universal global trade rules, and China's imperfect legislation on cross-border data flow exacerbate these challenges. Legal norms for personal information protection vary widely, causing regulatory conflicts. International cooperation is essential, as seen in the EU-US data flow agreements. China should engage in international discussions and regional negotiations like RCEP and FTAAP to establish favorable cross-border data flow rules, enhance information protection, and promote sustainable digital industry development, thereby boosting global trust in Chinese enterprises and advancing digital trade globalization.

References

[1] Q. Ma, “Li Xiaonan on the construction of supervision rules for cross-border data flow in China, ” Research on the rule of law, vol. 1, pp. 91–101, 2021.

[2] D. Guo, Open the Rudder Research on Legal Regulation of Cross-Border Data Flow, University of international business and economics, Beijing, China, 2018.

[3] M. Xiaying, “Legal attribute of data and its civil law positioning, ” Chinese Social Sciences, vol. 40, no. 9, pp. 164–183+209, 2016.

[4] M. Ferracane, “Restrictions on Cross-Border data flows: a taxonomy, ” ECIPE Working Paper No. 1/2017, 2017.

[5] S. A. Aaronson, “Data is different, and that’s why the world needs a new approach to governing cross-border data flows, ” Digital Policy, Regulation and Governance, vol. 3, 2019.

[6] R. Pepper, J. Garrity, and C. LaSalle, “Cross-border data flows, digital innovation, and economic growth, ” Global Inf. Technol. Rep, vol. 2016, pp. 39–47, 2016.

[7] D. W. Trabay, I. El-Henawy, and W. Gharibi, “A trust framework utilization in cloud computing environment based on multi-criteria decision-making methods, ”:e Computer Journal, vol. 65, no. 4, pp. 997–1005, 2021.

About the author: Hao Ren (2004.02-) male, Han Nationality, Xinyang, Henan province, Undergraduate, Henan University of Economics and Law, Research direction: Law