



Personal information protection in the context of cross-border e-commerce: challenges and systematization

OPEN ACCESS

SUBMITTED 22 April 2025

ACCEPTED 18 May 2025

PUBLISHED 20 June 2025

VOLUME Vol.07 Issue06 2025

CITATION

Wang Cong. (2025). Personal information protection in the context of cross-border e-commerce: challenges and systematization. *The American Journal of Political Science Law and Criminology*, 7(06), 49-52.

<https://doi.org/10.37547/tajpslc/Volume07Issue06-09>

COPYRIGHT

© 2025 Original content from this work may be used under the terms of the creative commons attributes 4.0 License.

Wang Cong

Doctoral Student at the University of World Economy and Diplomacy, Tashkent 100174, Uzbekistan

Suqian University, Suqian 223800, China

Abstract: In the context of globalization and digitalization, the rapid development of cross-border e-commerce has promoted the cross-border flow of personal information, but also brought challenges to data security and privacy protection. The cross-border transmission of personal information involves complex legal jurisdiction conflicts, and the regulatory systems of various countries vary significantly. The lack of unified international rules leads to high compliance costs for enterprises. China's "Personal Information Protection Law" and other laws and regulations have established a framework for personal information protection, but there are still problems such as insufficient legal connection and weak industry self-discipline mechanism. In order to optimize the governance system, we can learn from Singapore's "regulatory sandbox" model, promote technological innovation, and strengthen regional cooperation. In the future, it is necessary to balance security and development, establish a hierarchical and classified protection system, and form a governance network of government, enterprise, technology, and international collaboration to protect citizens' rights and promote the sustainable development of cross-border e-commerce.

Keywords: Cross-border e-commerce; personal information; protection system.

Introduction: In an era where globalization and digitalization are intertwined, cross-border e-commerce has become an important engine for international

trade. According to data from the Ministry of Commerce of China, the scale of China's cross-border e-commerce imports and exports will reach 2.38 trillion yuan in 2023, a year-on-year increase of 15.6%. [1] In 2024, the scale of China's cross-border e-commerce market will exceed 17 trillion yuan, with exports accounting for more than 70%. In 2024, the scale of the cross-border e-commerce market will exceed 17 trillion yuan, and exports will account for more than 70%. [2] Behind this prosperous scene is the cross-border flow of massive personal information - from consumers' delivery addresses, payment information to corporate user portrait data. While promoting business efficiency, this information also faces unprecedented security challenges. Personal information protection is not only related to citizens' basic rights, but also involves the balance between national data sovereignty and the development of the digital economy. When a Beijing consumer buys German goods through a cross-border e-commerce platform, his personal information may pass through a Singapore server and eventually be processed by a US data analysis company. This complex cross-border scenario makes the traditional legal framework seem stretched, and it is urgent to build a new governance system that takes into account both security and mobility.

RESULTS

1. Re-understanding the legal attributes of personal information

In the era of big data, data is no longer a simple information carrier, but data itself is specific information. The object of personal information protection discussed in this article is the personality and property interests carried by information or data. It is just that the emphasis of personal information and personal data in different application scenarios is different, but from the perspective of legal protection, the two are almost equivalent. The legal definition of personal information has evolved from "privacy right accessory" to "independent right object". [3] China's "Personal Information Protection Law" adopts "identifiability" as the core standard, which contrasts with the "identification theory" of the EU GDPR and the "association theory" of California CCPA. This difference in definition reflects the value orientation of different legal jurisdictions. Europe emphasizes the protection of personal dignity, the United States focuses on information freedom, and China tries to find a balance between the two.

In practice, the value of personal information presents dual characteristics. For enterprises, user behavior data can increase marketing conversion rates by 10%-

15%; for individuals, a data leak on an e-commerce platform in 2018 caused millions of users to suffer from precision fraud. This value conflict is particularly prominent in cross-border e-commerce. For example, in 2022, an international logistics company was fined 2 million euros by the European Union and investigated by the State Administration for Market Regulation of China for illegally transmitting customer information.

2. Governance difficulties caused by cross-border e-commerce

Regulatory systems in different countries are different and there is no unified law and practice internationally. Many countries have enacted personal information protection legislation, but the regulatory systems and strictness of each country are different. In particular, cross-border e-commerce, as a form of international trade, involves politics, administration, customs and other aspects. Different value orientations and regulatory systems may have an impact on the rights and interests of personal information subjects, national data sovereignty, and the development of digital trade in the country. Different countries and regions have different provisions and strictness for cross-border transmission of personal information, and there is currently no unified law and international practice to regulate it, which makes cross-border personal information protection difficult. The conflict of legal jurisdiction is the primary problem. The "server location principle" in traditional international private law has gradually become invalid in the era of cloud computing. [4] The 2023 Alibaba Cloud case shows that the European user data served by its Singapore data center triggers the compliance requirements of China's "Data Outbound Security Assessment Measures" and GDPR at the same time. This overlapping jurisdiction increases the compliance costs of enterprises by more than 30%. Another deep contradiction lies in the fragmentation of international rules. There is a fundamental difference between the APEC CBPR system and the EU adequacy recognition standard. The former adopts an industry self-discipline model, while the latter requires equal protection at the legislative level. This difference leads to the need for Chinese companies to establish multiple compliance systems when exporting to different regions. The annual report of a listed cross-border e-commerce company disclosed that its annual expenditure on data compliance in various countries exceeds 5% of its revenue.

3. Assessment of the current status of China's protection mechanism

China's personal information protection legal system presents a "pyramid structure". The "Personal Information Protection Law" is the top-level design, and

supporting regulations such as the "Data Outbound Security Assessment Measures" constitute the execution layer, and various industry standards provide technical support. However, this structure has connection problems. [5] For example, the cross-border transmission conditions stipulated in Article 38 of the Personal Information Protection Law conflict with the interpretation of Article 37 of the Cybersecurity Law.

Cross-border e-commerce companies have gradually strengthened internal policy construction in terms of data compliance, but actual implementation still faces bottlenecks. Although some companies have formulated data management specifications, there are problems of copying legal provisions and insufficient operability. Especially in the cross-border data transmission scenario, there is still a gap between corporate compliance capabilities and regulatory requirements. [6]

In addition, the professional capabilities of third-party certification agencies need to be improved. According to the latest developments of the National Technical Committee for Cybersecurity Standardization (TC260) in 2025, standards related to data security and cross-border compliance are still being improved, but there are still relatively limited professional assessment agencies for cross-border e-commerce scenarios. [7]

4. Path exploration for systematic improvement.

4.1 At the regulatory level, we can learn from Singapore's "regulatory sandbox" experience. The country's Personal Data Protection Committee (PDPC) allows companies to test cross-border data transfer solutions in limited scenarios, which not only controls risks but also encourages innovation. my country can pilot similar mechanisms in areas such as Hainan Free Trade Port and gradually establish a "white list + negative list" management system.

4.2 Technological innovation is also critical. The application of block chain technology in the field of cross-border payments proves that distributed ledgers can both ensure data traceability and avoid single node control risks. Ant Chain's "Trusple" platform has achieved security verification of cross-border trade data between China and Europe, and this model can be extended to the field of personal information protection.

4.3 International cooperation requires new ideas. Compared with directly joining the CBPR system, China can take the lead in promoting the construction of the "ASEAN + China, Japan and South Korea" regional data circulation circle. The Regional Comprehensive Economic Partnership Agreement (RCEP), which will take effect in 2024, has established a special chapter

on e-commerce to provide an institutional basis for such cooperation. At the same time, multinational companies such as Huawei and ByteDance should be supported to participate in the formulation of international standards and enhance their voice in rules.

CONCLUSION

Balance is the kingly way, and the dialectical relationship between security and development should be handled well.

Personal information protection is not the opposite of the digital economy, but the cornerstone of its healthy development. The experience of the European Union shows that the strict GDPR has instead spawned a data compliance industry, and the global market size is expected to reach US\$130 billion by 2025. For China, the key is to build a "tiered and classified" protection system: absolute protection of core data such as ID numbers, and flexible management of general information such as shopping preferences.

In the next five years, with the application of new technologies such as digital twins and metaverse, personal information protection will face more complex scenarios. Only by establishing a three-dimensional governance network led by the government, participated by enterprises, supported by technology, and coordinated internationally can we release the global value of cross-border e-commerce while protecting citizens' rights. Although this road is full of challenges, it is the only way to go in the era of digital civilization.

REFERENCES

"2023 China E-commerce Market Data Report", <https://imgs-b2b.100ec.cn/zt/2023dzswscbg/>, June 6, 2025.

In 2024, the cross-border e-commerce market will exceed 17 trillion yuan, with exports accounting for more than 70%, <https://www.100ec.cn/detail-6649720.html>, June 6, 2025.

Liu Lianjun. Distinguishing between personal information and personal data [J]. Quest, 2022 (5): 151-159.

Gong Yongqin. Research on personal information protection issues in cross-border e-commerce [D]. Beijing: University of International Business and Economics, 2016.

Wang Qinghua. Systematic interpretation of personal information rights —— Discussing the public law attributes of the "Personal Information Protection Law" [J]. Global Legal Review, 2022, 1: 69-78.

The current status and future prospects of cross-border e-commerce development in 2025,

The American Journal of Political Science Law and Criminology

<https://www.chwang.com/article/188236385935>,
June 6, 2025.

"Network Security Standardization Monthly Report"
2025 Issue 3,
<https://www.tc260.org.cn/front/postDetail.html?id=20250512153400>, June 6, 2025.