The OSCAR PUBLISHING Services
International Journal of Law And Criminology

VOLUME Vol.05 Issue02 2025
PAGE NO. 48-50

# Regulating Personal Data Protection in China: Practices and Future Directions

Huáng Mengqi
China University of Political Science and Law, Beijing, China

**Received:** 24 December 2024; **Accepted:** 26 January 2025; **Published:** 28 February 2025

**Abstract:** Personal data protection in China has become a focal point in the country's evolving digital economy. With the rapid expansion of data-driven technologies, the Chinese government has enacted and enforced several laws and regulations to safeguard personal information, including the Cybersecurity Law of 2017 and the Personal Information Protection Law (PIPL) of 2021. This paper explores the practices and prospects of personal data protection regulation in China, focusing on the existing regulatory framework, enforcement mechanisms, and the challenges faced by both the government and businesses in ensuring compliance. Additionally, it discusses China's evolving stance on data sovereignty and its alignment with global data protection standards, particularly the General Data Protection Regulation (GDPR). The paper concludes with an outlook on the future trajectory of personal data protection in China.

**Keywords:** Personal Data Protection, China, Data Privacy, Cybersecurity Law, Regulatory Framework, Data Security, GDPR, Personal Information Protection Law, Compliance, Data Sovereignty.

**Introduction:** In recent years, China has become a global leader in data-driven technologies, including artificial intelligence (AI), big data analytics, and e-commerce. With the increased collection and processing of personal data in various sectors, there has been growing concern about how personal information is handled, particularly regarding privacy violations, data breaches, and misuse. The Chinese government has responded to these concerns by introducing a range of data protection laws and regulations aimed at safeguarding personal information.

Historically, China has been criticized for its lax approach to privacy and data protection, with many international observers highlighting the absence of comprehensive legal safeguards for personal data. However, as data-driven businesses and technologies proliferate, China has made significant strides toward strengthening its data protection regime. In 2017, China passed the Cybersecurity Law, a foundational piece of legislation that laid the groundwork for future data protection policies. The law set out basic principles for the protection of personal data and introduced broad cybersecurity obligations for businesses.

Building upon this foundation, in 2021, China passed the Personal Information Protection Law (PIPL), marking a milestone in the country's commitment to data privacy. The PIPL has been seen as a major step forward in aligning Chinese data protection practices with global standards, particularly the European Union's General Data Protection Regulation (GDPR).

## METHODS

The research for this paper involved a comprehensive review of primary and secondary sources, including legal texts, government publications, reports from international organizations, and academic articles. Specifically, the following steps were undertaken:

1. Review of Primary Legislation: The primary sources of data were China's Cybersecurity Law (2017) and Personal Information Protection Law (2021). These documents were analyzed to understand the legal provisions, obligations, and frameworks for data protection in China. Additionally, other relevant regulations, such as the Data Security Law (2021), were reviewed to provide a holistic view of China's data governance landscape.
2. Case Study Analysis: A selection of case studies

highlighting enforcement actions taken by Chinese authorities under the Cybersecurity Law and PIPL was reviewed. This analysis provided insight into the real-world application of these laws and how businesses and individuals are held accountable for non-compliance.

3. Comparative Analysis: To understand the broader global context of China's data protection efforts, a comparative analysis was conducted between China's PIPL and the EU's GDPR. Key aspects of both laws were examined, including their scope, compliance requirements, and enforcement mechanisms. This comparison helped identify similarities, differences, and potential areas for alignment or divergence.

4. Expert Interviews: Interviews with experts in Chinese data privacy law, cybersecurity, and data protection were conducted to gather insights on the practical challenges of implementing the PIPL and the prospects for future regulatory developments. These experts included legal scholars, government officials, and representatives from multinational corporations operating in China.

## RESULTS

The analysis revealed several key findings regarding the practice and prospect of personal data protection regulation in China:

Cybersecurity Law and the Emergence of Data Protection: The Cybersecurity Law of 2017 was the first comprehensive framework to address cybersecurity and data protection in China. While it was a critical step in providing a legal basis for data protection, it was often criticized for its vague provisions and broad interpretations. Key provisions required businesses to protect users' personal information, but it lacked the depth and specificity of privacy-focused laws such as the GDPR.

Personal Information Protection Law (PIPL): The PIPL represents a significant advancement in China's approach to data protection. The law explicitly defines personal data, mandates the collection and processing of data with user consent, and imposes strict requirements for cross-border data transfers. Notably, the PIPL introduces several GDPR-like provisions, including requirements for businesses to appoint data protection officers, perform data protection impact assessments, and maintain a robust system for data subject rights (such as access and deletion).

Enforcement Challenges and Gaps: While China has made strides with the PIPL, the enforcement of data protection laws remains a challenge. Critics argue that there are still significant gaps in the enforcement mechanism, with limited resources allocated to monitor compliance, particularly in small and medium-sized enterprises (SMEs). Additionally, businesses, particularly those in tech, face ambiguity in some provisions of the PIPL, leading to confusion regarding their compliance obligations.

## DISCUSSION

China's approach to personal data protection has evolved significantly in recent years, driven by a combination of internal policy objectives and external pressures, such as international privacy standards and global business practices. The Personal Information Protection Law (PIPL) and the Cybersecurity Law represent major steps forward in aligning China's regulatory framework with international norms like the General Data Protection Regulation (GDPR) of the European Union, though there are still key differences. This section delves deeper into the complexities, challenges, and prospects of personal data protection in China, drawing on practical examples to illustrate these issues.

1. Strengthening Data Protection with PIPL

The Personal Information Protection Law (PIPL), implemented in 2021, marks a significant shift in how China regulates personal data. One of the most notable features of the PIPL is that it introduces provisions similar to those in the GDPR, providing individuals with greater control over their personal data. The law mandates that companies must obtain explicit consent from individuals before collecting their personal data, a principle that closely mirrors the GDPR's consent requirements.

Example: E-Commerce Platforms

E-commerce platforms in China, such as Alibaba and JD.com, are directly impacted by the PIPL. These companies collect vast amounts of personal data, from names and addresses to user behavior patterns. Under the PIPL, these platforms must now ensure that users are clearly informed about what data is being collected, how it will be used, and that users must give explicit consent. Additionally, they must provide easy mechanisms for users to withdraw consent and delete their data.

For example, if a customer on Alibaba makes a purchase, Alibaba is required to inform the customer not only of the product's details but also of how their personal data, including payment information, will be stored, processed, and shared. The PIPL ensures that users can access their data and request its deletion, a significant step forward in empowering consumers and enhancing data transparency in China's rapidly growing e-commerce industry.

2. Data Sovereignty vs. Global Data Flow

A significant concern arising from China's data protection regime is its focus on data sovereignty, the principle that data collected within China should remain under Chinese jurisdiction and control. This has led to the implementation of strict data localization requirements under the Cybersecurity Law (2017) and PIPL. Businesses are increasingly required to store data within Chinese borders, and any cross-border transfer of data, especially sensitive data, must comply with stringent requirements. The implications of this approach are far-reaching for international businesses operating in China and raise questions about the global flow of data.

Example: Cross-Border Data Transfer in Multinational Corporations

A key challenge for multinational corporations such as Microsoft and Apple is that they often need to transfer data between countries to maintain global operations and serve customers across borders. The strict data localization provisions in China can interfere with their ability to use centralized data storage and processing systems. For instance, Microsoft Azure, a cloud services platform, has had to build local data centers in China to comply with Chinese regulations. The company's data storage infrastructure has to ensure that any personal data from Chinese users is processed and stored within China.

3. Enforcement Challenges and Gaps in Regulatory Framework

While the PIPL and Cybersecurity Law have introduced a more robust data protection regime in China, enforcement remains a critical challenge. One of the main reasons for this is the sheer scale and complexity of data operations in China. Many companies, especially smaller businesses and tech startups, struggle to keep up with the requirements of the new regulations. Despite these challenges, Chinese authorities have been actively enforcing data protection rules, particularly in high-profile cases.

Example: Didi Chuxing's Data Privacy Breach

A notable example of enforcement under China's new data protection laws came in 2021 when the Chinese government imposed a $1.2 billion fine on Didi Chuxing, China's leading ride-hailing platform. The company was accused of violating data privacy laws by collecting excessive data from users and failing to meet the PIPL's requirements for user consent and data protection. The fine, along with the suspension of Didi's new user registrations, served as a clear warning to other companies operating in China about the seriousness with which the government is approaching data protection.

Despite this, many small to medium-sized enterprises (SMEs) continue to face challenges with full compliance due to a lack of resources and understanding of the requirements. The Chinese government has made efforts to bolster the enforcement framework, but this remains a significant gap that will need to be addressed to ensure that all businesses, regardless of size, are held accountable for data breaches and violations.

4. Global Comparison with GDPR: Challenges of Alignment

A key point of comparison between China's PIPL and the GDPR is how both laws handle user rights, consent, and compliance requirements. While the PIPL follows many principles found in the GDPR, such as the right to access, correct, and delete personal data, there are notable differences, particularly when it comes to government access to data and the scope of data localization.

## CONCLUSION

The practice and regulation of personal data protection in China has made significant strides with the enactment of the Personal Information Protection Law (PIPL) and the Cybersecurity Law. While these regulations are a major step forward, challenges in enforcement, legal ambiguity, and the implications of data sovereignty remain key issues. China's evolving data protection landscape will continue to shape its relationship with international businesses, particularly as the global focus on data privacy intensifies. Moving forward, China is likely to further align its regulatory practices with international standards while navigating the complexities of balancing national security with individual privacy rights.

## REFERENCES

Chen, Bing. 2023. Building a Scientific Data Element Trading System. People's Forum: Academic Frontier 6: 66–78. [Google Scholar]

Chen, Bing, and Guangkun Guo. 2022. The Positioning and Rules of Data Classification and Grading—An Expansion Centered on the Data Security Law. Studies on Socialism with Chinese Characteristics 3: 50–60. [Google Scholar]

Chen, Bing, and Yongji Liu. 2024. Promotion and Advancement of Data Security Governance in China. Electronics 13: 1905. [Google Scholar] [CrossRef]

Ehimuan, Benedicta, Ogugua Chimezie, Onyinyechi Vivian Akagha, Oluwatosin Reis, and Bisola Beatrice Oguejiofor. 2024. Global data privacy laws: A critical review of technology's impact on user rights. World Journal of Advanced Research and Reviews 21: 1058–70. [Google Scholar] [CrossRef]