

Legal Protection of Data Property Rights: A Comparative Study of International Experience and Chinese Practice

Maoyi Cai

School of Law, Hunan University of Technology, Zhuzhou City, Hunan 412000, China;

ABSTRACT

This study explores the legal protection of data property rights, comparing international experiences with practices in China. Data property rights concern ownership and control over personal information, business secrets, and other digital content, which are vital for privacy, security, and fair use. Internationally, regulations such as the GDPR in the EU and a mix of federal and state laws in the USA shape the landscape of data rights. In China, the Cybersecurity Law and Data Security Law have been implemented, but inconsistencies remain. A comparison reveals differences in legal frameworks, implementation, and enforcement between international examples and China. The analysis identifies areas for improvement in China's approach to data property rights and suggests lessons learned from global practices.

KEYWORDS

Data property rights; Legal protection; International experience; Chinese practice; Comparative study

1 Introduction

The rapid development of digital technology has led to the emergence of data as a new form of property, which has significant value and potential. Data property rights refer to the ownership, control, and use of data assets, which include personal information, business secrets, and other forms of digital content. The protection of these rights is crucial for ensuring the privacy, security, and fair use of data in both global and domestic contexts. Internationally, various legal frameworks and regulations have been established to safeguard data property rights. For instance, the European Union's General Data Protection Regulation (GDPR) imposes strict rules on the collection, storage, and processing of personal data, while the United States relies on a combination of federal and state laws to protect data privacy and security. These international experiences provide valuable insights into the challenges and opportunities of legal protection for data property rights [1]. In China, the issue of data property rights has gained increasing attention in recent years. The country has introduced a series of laws and policies to regulate the use and management of data, such as the Cybersecurity Law and the Data Security Law. However, there are still gaps and inconsistencies in the current legal framework, which raise questions about the effectiveness and enforcement of data property rights in practice.

Given the global nature of data flows and the varying legal approaches across countries, it is essential to conduct a comparative study between international experience and China's practice in the legal protection of data property rights. This comparison can help identify best practices, address challenges, and promote international cooperation in this field [2]. By examining the similarities and differences in legal frameworks, implementation, and enforcement, we can gain a

better understanding of how to improve the legal protection of data property rights in China and contribute to the global dialogue on data governance.

2 Legal Protection of Data Property Rights in International Experience

2.1 Overview of International Practices and Regulations

International practices and regulations pertaining to data property rights reflect a diverse range of legal philosophies and technological environments. Broadly, these can be categorized into regulatory frameworks that lean towards privacy protection and those that balance privacy with other concerns such as national security and business interests. The European Union leads with its comprehensive GDPR, which harmonizes data protection laws across member states. The GDPR emphasizes individual rights, including the right to erasure and data portability, and imposes strict obligations on data controllers and processors. Enforcement is robust, with hefty fines serving as a deterrent for non-compliance. In contrast, the United States adopts a sector-specific approach, combining federal mandates like the Health Insurance Portability and Accountability Act (HIPAA) for sensitive data and sector-specific regulations like the Gramm-Leach-Bliley Act for financial institutions. Additionally, state laws, such as the California Consumer Privacy Act (CCPA), introduce further complexity by varying from state to state, necessitating compliance strategies that accommodate multiple jurisdictions [3]. Beyond these jurisdictions, other nations have developed their unique frameworks in response to local contexts and values. For instance, Brazil's General Data Protection Law (LGPD) aligns with the GDPR in many respects but adapts to fit Brazil's informational landscape. Similarly, India's Information Technology Act of 2000, amended in 2011 to include a privacy rule, reflects its status as both a developing nation and a digital hub. Common challenges among these international practices include adapting to technological advancements, balancing individual privacy rights with free speech and business innovation, and ensuring that laws are not so onerous as to stifle growth in the digital economy.

2.2 Case studies of specific countries or regions

The European Union, through its GDPR, established a stringent and unified legal framework for data protection across all member states. The GDPR not only mandates high standards for personal data processing but also empowers individuals with rights to access, rectify, and erase their data. Fines for non-compliance are substantial, serving as a deterrent and leading to a culture of compliance among businesses operating in the EU.

In the United States, the approach is more decentralized, with a mix of federal and state laws. For instance, while the HIPAA protects healthcare information, CCPA grants consumers more control over their personal information and applies to a range of industries. This patchwork of laws presents challenges for national companies and multinational corporations navigating multiple jurisdictions. The GDPR has been largely effective in raising data protection standards and promoting dialogue on privacy issues. However, it faces challenges such as adapting to new technologies and maintaining a balance between privacy rights and technological innovation [4]. Additionally, the uniform application of the GDPR across diverse member states can be challenging due to local contexts and legal traditions. In the United States, the diversity of laws across states like the CCPA fosters a competitive environment for data protection, encouraging businesses to adopt best practices to remain competitive. However, this fragmented approach can also lead to confusion and increased administrative burdens for businesses operating in multiple states. Balancing state-level innovations with national coherence remains a challenge for US lawmakers.

3 Legal Protection of Data Property Rights in China's Practice

3.1 Overview of China's current legal framework and policies

China's approach to data property rights has progressively evolved, reflecting the nation's unique developmental context and digital economy. The legal framework is multi-layered, encompassing constitutions, laws, administrative regulations, and national standards. Notably, the Cybersecurity Law of 2016 marks a significant milestone, establishing foundational principles for data protection and cybersecurity. Additionally, the Data Security Law, effective from September 2021, mandates data security management responsibilities for organizations handling large amounts of personal information and important data. This law emphasizes risk assessments and categorizes data into different protection levels based on sensitivity and potential impact on national security. Furthermore, the Personal Information Protection Law (PIPL), implemented in 2021, strengthens individual privacy rights and places stringent requirements on businesses, especially regarding consent and processing of personal information. This law represents a substantial step towards structuring data governance and enhancing individual rights in China. Administrative guidance and standards complement these laws, providing more specific directions for implementation. For instance, the National Standard for Personal Information Security Specification (GB/T 35273-2020) offers detailed security measures for personal information processing [5].

3.2 Case studies of specific industries or sectors

In China, the rapid development of the internet economy has led to the emergence of large-scale internet companies such as Alibaba, Tencent, and Baidu. These companies handle vast amounts of user data, making data property rights a critical issue. The Personal Information Protection Law (PIPL) significantly impacts these firms by requiring explicit user consent for data collection and strictly limiting data transfers. For instance, internet platforms now allow users to opt-out of personal data sharing with affiliates and third parties, reducing the potential for data misuse but also affecting business models reliant on data monetization. Financial institutions in China, including banks and fintech companies like Ant Financial, face similar challenges. The Data Security Law mandates that financial data, often classified as "important data," undergo strict security management. Compliance requires significant investments in technology and procedure upgrades, from encrypting sensitive transactions to implementing robust access controls. These measures enhance data security but also increase operational costs and complexity.

The enforcement of these laws has heightened data protection awareness among Chinese businesses. Internet companies and financial institutions have had to revise their data strategies, prioritizing user consent and transparency. However, adapting to these new legal requirements presents challenges, particularly for small and medium-sized enterprises with limited resources. The cost of compliance, especially for widespread encryption and data management systems, can be substantial. Moreover, as the laws are relatively new, there is an ongoing process of interpretation and clarification by regulatory bodies, leading to a degree of uncertainty in implementation. Businesses face challenges in staying updated with the latest legal interpretations and adapting their operations accordingly.

The effectiveness of these policies in safeguarding data property rights is increasingly evident in raising standards and user trust [6].

However, the challenge lies in maintaining a balance that promotes innovation and economic growth while ensuring stringent data protection. As China continues to refine its approach, it is essential to foster an environment where compliance is feasible and where legal frameworks keep pace with technological advancements and market dynamics.

4 Comparison between International Experience and China's Practice

4.1 Similarities and differences in legal frameworks and policies

Both international experience and China's practice emphasize the importance of data property rights and recognize the need for legal protections. Countries like the EU and the USA, as well as China, have established comprehensive legal frameworks to regulate data handling and protect individual privacy. These frameworks share common ground in their focus on consent, data minimization, and security requirements. The EU's GDPR and China's Personal Information Protection Law (PIPL) both prioritize individual control over personal data. They mandate explicit user consent for data collection and set stringent rules for data processing. Furthermore, both regulations emphasize the importance of data minimization, requiring that only necessary data be collected for specified purposes. However, there are significant differences in the approach and scope of these laws. The GDPR applies broadly to all personal data of EU citizens, regardless of where the data is processed, reflecting a regional and extraterritorial focus. In contrast, Chinese laws, while increasingly stringent, primarily target domestic organizations and have a more territorial application.

Another difference lies in the enforcement mechanisms and penalties. The GDPR is known for its strict enforcement and hefty fines, acting as a strong deterrent against non-compliance. On the other hand, while China's laws also impose penalties, the enforcement has been more variable, with a mix of administrative guidance and regulatory oversight. There are also elements where China can draw lessons from international experiences. For instance, the GDPR's emphasis on individual rights and its pan-European consistency could inspire further harmonization and clarity in China's legal implementation. Conversely, China's rapid adaptation to changing technologies and market conditions offers insights into flexible regulatory approaches that balance innovation with protection.

4.2 Similarities and differences in implementation and enforcement

Implementation and enforcement of data property rights differ significantly between international frameworks like the EU's GDPR and China's approach. The GDPR relies on a combination of technological solutions, such as data encryption and pseudonymization, and administrative procedures to enhance compliance. This law emphasizes the role of data protection officers (DPOs) within organizations and places a strong emphasis on individual rights, including the right to erasure and data portability. Enforcement is stringent, with the possibility of fines up to 4% of global annual revenue for non-compliance. In contrast, China's enforcement of data property rights has been more administrative, focusing on regulatory guidance and government oversight. While laws like the Cybersecurity Law and the Personal Information Protection Law (PIPL) establish clear norms, their enforcement relies heavily on administrative actions rather than private enforcement mechanisms. Chinese regulators often issue guidelines and conduct inspections to ensure compliance, and there is a growing trend toward imposing substantial fines for violations.

One notable difference is the involvement of private actors in enforcement. In the EU, individuals have more power to enforce their data rights through legal action, whereas in China, regulatory bodies play a more dominant role. Additionally, China's approach includes more direct government intervention in cases of non-compliance, often involving temporary suspension of services until issues are resolved, which is less common in the EU. Regarding implementation, both systems face challenges. The GDPR's far-reaching extraterritorial application can create complexity for global businesses, while China's rapidly evolving legal landscape requires constant adaptation by companies operating within its jurisdiction [7]. The GDPR has been criticized for potentially stifling

innovation due to its broad requirements, whereas China's approach is still evolving in lockstep with its rapidly growing digital economy, seeking to balance innovation with regulation.

5 Lessons that China can learn from international experience

While China has made substantial strides in data property rights protection, there remains room for improvement by learning from international successes and challenges. By integrating lessons on individual rights, extraterritoriality, sector-specific regulation, independent enforcement, and public awareness, China can further refine its approach to protect data property rights effectively. Also, China's rapid digitalization has led to a critical need for robust data property rights protection. International experiences, such as those of the EU and the USA, offer valuable lessons that China can incorporate to enhance its legal framework and enforcement mechanisms.

Firstly, the EU's GDPR emphasizes individual control over personal data, including explicit consent requirements and rights to erasure and data portability. China can further strengthen individual rights by clarifying and enhancing these aspects within its existing laws, ensuring that individuals have greater agency in how their data is used. Secondly, the GDPR's extraterritorial reach demonstrates that data regulation can effectively apply to international businesses operating within the EU. While China's laws primarily focus on domestic organizations, considering a more expansive application could better protect Chinese citizens' data rights globally. Moreover, the USA's approach to sector-specific regulation, such as in finance and healthcare, shows the importance of tailored regulations for specific industries. China might benefit from similar industry-specific guidelines that consider the unique data handling practices and sensitivity of different sectors. Another lesson from international practices is the role of independent supervisory authorities and judicial enforcement. The GDPR assigns significant power to data protection authorities and allows for private right of action, enhancing enforcement. China could explore establishing more independent supervisory bodies and clearer pathways for individual legal actions to bolster enforcement. Lastly, both the EU and USA have placed significant emphasis on raising public awareness and promoting data literacy. Integrating data protection into education and public discourse can empower individuals to make informed decisions about their data and hold processors accountable.

6 Conclusion

The comparative study between international experiences and China's practice in legal protection of data property rights reveals both similarities and differences. International frameworks, such as the EU's GDPR, emphasize individual rights and employ comprehensive enforcement mechanisms, including significant fines and direct individual involvement in enforcement. In contrast, China's approach is characterized by rapid development, focusing on administrative guidance and government oversight to ensure compliance. Despite these differences, there are opportunities for China to learn from international successes. Lessons include enhancing individual control over personal data, considering extraterritorial application of laws, developing industry-specific regulations, establishing independent supervisory authorities, and promoting data literacy. By integrating these lessons into its existing legal framework, China can further refine its approach to protect data property rights effectively. Additionally, international practices can benefit from China's experience in balancing innovation and regulation within a rapidly evolving digital economy. Cross-learning and continuous improvement are essential in the global effort to protect data rights, ensuring that legal frameworks remain relevant and effective in the face of technological advancements.

About the Author

Maoyi Cai, Sichuan Province in 1999, graduated from Shantou University with a bachelor's degree in law, and is currently studying law (law) at Hunan University of Technology.

References

- [1] Cui S., & Qi P. (2021). The legal construction of personal information protection and privacy under the Chinese Civil Code. *Computer Law & Security Review*, 41, 105560.
- [2] Yan L. (2024). Research on the legal issues of network privacy right and personal information protection. *International Journal of Frontiers in Sociology*, 6(5).
- [3] Berrell M., & Wrathall J. (2006). Between Chinese culture and the rule of law: What foreign managers in China should know about intellectual property rights. *Management Research News*, 30(1), 57-76.
- [4] Feng Y. (2019). The future of China's personal data protection law: challenges and prospects. *Asia Pacific Law Review*, 27(1), 62-82.
- [5] Yu X., & Zhao Y. (2019). Dualism in data protection: Balancing the right to personal data and the data property right. *Computer Law & Security Review*, 35(5), 105318.
- [6] Weber P. A., Zhang N., & Wu H. (2020). A comparative analysis of personal data protection regulations between the EU and China. *Electronic Commerce Research*, 20, 565-587.
- [7] Sharma A. K., & Sharma R. (2024). Comparative Analysis of Data Protection Laws and ai Privacy Risks in brics Nations: A Comprehensive Examination. *Global Journal of Comparative Law*, 13(1), 56-85.