International Journal of Social Sciences and Public Administration
ISSN: 3005-9836 (Print), ISSN: 3005-9585 (Online) | Volume 10, Number 4, Year 2026
DOI: https://doi.org/10.62051/ijsspa.v10n4.05
Journal homepage: https://ijsspa.org

The Dilemmas and Improvement Paths of Civil Protection of Personal Information in the Context of Data and Platform Compliance

Yimin Lei

Faculty of Law, University of Malaya, Kuala Lumpur, Malaysia

ABSTRACT

From the perspective of data compliance and platform governance, this paper adopts empirical research and normative analysis to conduct a systematic study on the civil protection of personal information in China. An examination of current institutional practices reveals prominent dilemmas in key areas such as legislative coordination, judicial application, platform liability enforcement, and individual rights remedies. These dilemmas mainly include insufficient adaptability of legal rules, unbalanced allocation of the burden of proof, ineffective implementation of platform compliance, and high costs for individual rights relief. Based on China's existing legal framework and judicial practice, this paper proposes a systematic improvement path for the civil protection of personal information from five aspects: refining legislation, unifying adjudication standards, improving platform internal control mechanisms, optimizing remedy channels, and establishing a multi-stakeholder collaborative regulatory system. This can provide practical reference for the protection of personal information civil rights and the standardized operation of platforms. This article only focuses on the analysis of civil remedies and does not delve into the mechanism of civil execution connection. The empirical materials mainly consist of public judgments made by some courts, which restricts the research scope to a certain extent. In the future, we can combine new application scenarios such as algorithm recommendation and cross-border data transmission to further improve the rules for civil compensation and liability determination, promote the collaborative efforts of multiple governance mechanisms, and achieve a dynamic balance between personal information protection and platform compliance in the context of sustainable development of the digital economy.

KEYWORDS

Personal Information; Platform Compliance; Civil Protection; Judicial Practice; Rights Protection Paths.

1. INTRODUCTION

The deep popularization of digital technology has made personal information the core production factor driving the development of the digital economy. As the core entity of personal information collection, storage, use and circulation, the compliance operation level of network platforms directly affects the judicial protection and actual realization of personal information civil rights and interests. According to the official report of the Fourth Intermediate People's Court of Beijing Municipality, from 2022 to 2024, the court heard and concluded 66 civil appellate cases involving personal information rights, with the number of cases increasing year by year, and internet platforms are the main litigation subjects. This judicial feature not only confirms the improvement of public awareness of personal information protection, but also highlights the practical needs and pain points in this field [1]. By 2025, the National Cyberspace Administration's Reporting Center had received and disposed of 223 million reports involving illegal and harmful online information nationwide. including vague

Content from this work may be used under the terms of CC BY-NC 4.0 licence (https://creativecommons.org/licenses/by-nc/4.0/).
Published by Warwick Evans Publishing.

connection in the application of law, imbalanced allocation of the burden of proof, inconsistent compensation standards and high costs of personal rights protection. Contradictions remain prominent between the inadequate fulfillment of platform compliance obligations and the ineffectiveness of civil accountability mechanisms. Based on this, this article takes the perspective of data and platform compliance to systematically analyze the practical difficulties in the civil protection of personal information and explore targeted improvement paths, aiming to provide a reference for judicial practice and institutional improvement in this field. This study holds both theoretical explanatory value and guiding significance for judicial practice.

2. THE LEGISLATIVE DILEMMA OF CIVIL PROTECTION OF PERSONAL INFORMATION IN DATA AND PLATFORM COMPLIANCE

In the context of the digital economy, China has established a basic legislative framework for the civil protection of personal information, with the Civil Code and the Personal Information Protection Law as the core. However, considering the actual compliance scenarios of platform large-scale data processing and full-process information circulation, the current legislation still has such problems as vague definition of core provisions, poor alignment of legal norms and insufficient scenario adaptability [2], making it difficult to effectively respond to the practical demands for the civil protection of personal information.

Firstly, legal provisions are overly principled and lack operability. The core rule of "notice and consent" established by the Personal Information Protection Law does not clearly define the "reasonable scope" and "necessary limits", and there is a lack of specific identification rules for "separate consent" and "express consent". Many platforms adopt standard form clauses to blur the boundaries of information authorization, making platform compliance operations lose clear legal guidance. The trial practice research of the Guangzhou Internet Court in January 2026 confirmed this problem. The study reviewed and sorted out 240 relevant civil disputes heard by Guangzhou's people's courts at two levels from 2019 to June 2024, and nearly 80% of the disputes were concentrated in the judicial review of the terms of authorization in the Privacy Policies and User Agreements. This research is an excellent research achievement for the key research project of provincial-level courts, and was published in the judicial journal of the Higher People's Court of Guangdong Province.

Secondly, there are multiple loopholes in the application and connection of different laws. The Civil Code and the Personal Information Protection Law not only contain inconsistent provisions on the delimitation of the boundary between personal information and privacy rights, as well as the elements of infringement liability, but also have significant differences in defining the scope of compensation for damages. The former only regulates compensation for property losses, while the latter includes compensation for moral damage. According to a special survey conducted by the China Court News Network in 2024, the unclear application relationship between the two laws is the most prominent legal application problem in judicial practice of such cases.

Thirdly, legislation in emerging scenarios lags behind the development of digital technology. In response to new processing behaviors such as algorithmic decision-making, cross-border data transmission, algorithm recommendation and data aggregation and sharing, existing legislation lacks supporting civil protection rules and fails to clarify infringement liability and damage compensation standards [3]. It is difficult to cope with the covert and cross-regional infringement risks posed by technological development, and cannot provide comprehensive legal protection for personal information civil rights and interests.

3. THE JUDICIAL IMPLEMENTATION DILEMMA OF CIVIL PROTECTION OF PERSONAL INFORMATION IN DATA AND PLATFORM COMPLIANCE

Judicial practice is a core guarantee for the relief of personal information civil rights and interests. However, in the actual scenario of data and platform compliance, judicial implementation has faced various practical obstacles, making it difficult for the institutional design of personal information civil protection to truly be implemented and effective. The practical obstacles in the evidentiary process are particularly prominent, as individuals are inherently in an information-disadvantaged position in evidence collection. The core data of the entire personal information processing process are solely controlled by the platform, making it difficult for ordinary people to obtain direct evidence of the platform's illegal processing of information. The special research conducted by the two courts in Guangzhou from 2019 to June 2024 shows that 37.08% of personal information civil infringement disputes involve mainstream online platforms such as WeChat and Douyin, among which more than 60% of cases are due to the platform's refusal to cooperate in providing user information related to infringement, which directly leaves individuals in an evidentiary deadlock [4], and the causal relationship between personal information leakage and subsequent fraud, reputation damage and other damages also makes it difficult for individuals to provide evidence. At the same time, the principle of presumption of fault, which is clearly defined in the Personal Information Protection Law, has not been uniformly applied in judicial practice. Some courts still insist on requiring individuals to provide evidence to prove that the platform has subjective fault. In current judicial practice, no unified standards have been established for damage determination and adjudication. Personal information infringement usually constitutes non-pecuniary damage, and the amount of moral damage compensation lacks a clear quantitative basis.Court decisions vary considerably: some cases only uphold several hundred yuan in reasonable rights-protection costs, while others award tens of thousands of yuan in moral damages.Research data from Guangzhou courts show that the judicial support rate for such cases over the past five years is merely 17.5%. Even where rights holders successfully adduce evidence, their property losses frequently cannot be fully compensated because causation is difficult to establish. Low litigation efficiency and high rights-protection costs have further undermined the practical effect of judicial relief. Most personal information infringement cases are small claims, yet they require complex litigation procedures and lengthy trial cycles, with a low application rate of summary procedures for small claims. Most right holders choose to abandon litigation as the costs of rights protection far outweigh the expected benefits [5], ultimately resulting in the judicial relief mechanism for the civil protection of personal information being reduced to a mere formality, which fails to perform its practical functions.

4. THE PLATFORM LIABILITY DILEMMA OF CIVIL PROTECTION OF PERSONAL INFORMATION IN DATA AND PLATFORM COMPLIANCE

As the core responsible entity for personal information processing, the platform's compliance awareness cultivation and the actual effectiveness of fulfilling legal obligations are directly related to the practical effect of protecting personal information civil rights and interests. However, there are still significant deficiencies in the compliance construction of current online platforms, which have not fully played the role of the first line of defense for personal information protection.

Firstly, the platforms have weak compliance awareness, and illegal processing of personal information remains rife despite repeated crackdowns. Some platforms, guided by the maximization of commercial interests, indirectly force the collection of users' personal information through blanket authorization and subsequent mandatory updates of user agreements [6]. According to data from the Ministry of Industry and Information Technology's 2025 APP Infringement of User Rights Special Rectification, over 2 million APPs were inspected nationwide in the year, and over 10,000 non-

compliant APPs were ordered to conduct rectification. Multiple educational and lifestyle APPs were ordered to rectify within a specified period of time for forcibly requesting non-essential personal information during the login process. Such behavior has constituted a direct infringement on users' personal information rights and interests.

Secondly, there are obvious deficiencies in the construction of the platform's internal compliance system. Most platforms have not appointed a full-time person responsible for personal information protection in accordance with the Personal Information Protection Law, have not established a sound control mechanism for the entire process of personal information processing, and neglected to conduct regular compliance audits and professional training for relevant staff. This makes it difficult to effectively supervise personal information processing behavior within the platform, thereby significantly increasing the potential risks of personal information leakage and illegal use.

Thirdly, an inter-platform collaborative compliance supervision mechanism has not yet been effectively established. There is a lack of data security linkage and compliance information sharing mechanisms between different online platforms [7]. Some platforms conceal or delay the disposal of personal information leakage incidents. The typical case released by the Shanghai Cyberspace Administration in 2025 shows that such acts not only result in the further aggravation of damages caused by personal information infringement, but also set multiple obstacles for infringement source tracing, significantly increasing the practical difficulty of protecting personal information civil rights and interests.

5. THE DILEMMA OF PERSONAL RIGHTS PROTECTION IN CIVIL PROTECTION OF PERSONAL INFORMATION IN DATA AND PLATFORM COMPLIANCE

As the subject of personal information rights, individuals' awareness and practical ability to protect their rights directly affect the effectiveness of the civil protection system for personal information. However, in the context of data and platform compliance, individuals always face multiple obstacles to protecting their rights and interests, making it difficult to achieve effective remedies.

Firstly, individuals' awareness of safeguarding their rights varies greatly, and their ability to preserve evidence is generally poor. According to a special survey on personal information protection conducted by the Suzhou Municipal Council for the Protection of Consumers' Rights and Interests in 2025, nearly 60% of respondents reported having experienced personal information leakage to varying degrees, but over 30% of the public have a vague understanding of the legal protection boundaries of personal information rights and interests. They have not actively consulted the platform's privacy policy and information collection authorization scope, nor have they timely preserved key evidence through screenshots, notarization and other means after their rights and interests have been infringed upon [8]. Ultimately, due to insufficient evidentiary materials, their claims for rights protection cannot be advanced.

Secondly, the operation of individual rights protection channels is not smooth, and the platform has not effectively fulfilled its legal response obligations. Although the Personal Information Protection Law explicitly grants individuals the legal rights to access, copy, and delete personal information, the aforementioned survey shows that over 50% of respondents have reported that the platform has not established a convenient mechanism for exercising their rights, and the entry points for rights protection complaints are obscure and the efficiency of manual response is low [9]. Some platforms even directly reject reasonable rights protection requests without furnishing legitimate reasons, making it difficult for individuals to realize their rights protection demands through non-litigation channels such as negotiation and complaints.

Finally, the high costs of rights protection, coupled with the difficulty in evidence collection and a high case dismissal rate, create a double barrier to rights protection. In cases of personal information

infringement, individuals need to bear their own attorney's fees, evidentiation costs, notarization fees and other rights protection costs, and the litigation cycle of the case is long and the trial process is complex. The analysis of trial practice released by the Guangzhou Internet Court in January 2026 shows that 37.08% of the 240 related civil disputes accepted by the Guangzhou two-level courts from 2019 to June 2024 occurred on the mainstream network platform. The platforms control the core data but refuse to cooperate in providing evidence, which is the main reason why there is no way for individuals to provide evidence; In typical cases involving claimants Xie and Zhong, the claims were dismissed due to insufficient evidence to prove the source of personal information leakage, and the amount of compensation awarded in such cases is generally low. The cost of personal rights protection often far exceeds the actual amount of compensation received, which ultimately discourages most individuals from taking legal action against such infringements.

6. THE WAY OUT AND IMPROVEMENT PATH OF CIVIL PROTECTION OF PERSONAL INFORMATION IN DATA AND PLATFORM COMPLIANCE

In response to the practical difficulties of legislation, judiciary, platform responsibility, and individual rights protection in the context of data and platform compliance, it is necessary to coordinate measures from five aspects and build a systematic personal information civil protection system.

Firstly, improve the legislative system and enhance the operability of the relevant provisions. Refine the relevant provisions of the Personal Information Protection Law, clarify the definition of "necessary limits" and "reasonable scope", ascertain the logical alignment between the Civil Code and the Personal Information Protection Law, supplement special civil protection rules for new data processing scenarios such as platform algorithmic decision-making and cross-border data transmission, and fill legislative gaps [10].

Secondly, optimize the judicial implementation mechanism and lower the threshold for individual rights protection. Unify the rules for allocating the burden of proof, clarifying that platforms bear the burden of proof for their own compliant conduct, and reducing the burden of proof for individuals; Promote the expedited small claims procedure for personal information infringement cases, simplify the trial process, and improve judicial efficiency; Establish a unified standard for determining compensation for infringement damages, refine the calculation basis for compensation for moral damage, and standardize judicial adjudication criteria.

Thirdly, strengthen the primary liability of platforms and improve their internal compliance systems. Require platforms to establish and improve internal management systems for personal information processing, designate dedicated personal information protection personnel in accordance with regulations, and regularly conduct compliance audits and professional training for practitioners; Embed personal information rights protection functions in the product design phase, and strictly regulate the implementation of the "notice and consent" rule, and achieve compliance control throughout the entire process of personal information processing.

Fourthly, enhance individual rights protection capabilities and strengthen awareness of rights protection. Popularize legal knowledge on personal information protection through various forms such as media publicity and community lectures, and guide the public to clarify channels and operational procedures for safeguarding rights [11]; Expand the coverage of public legal aid, provide free legal services for economically disadvantaged individuals seeking rights protection, and effectively reduce the economic cost of individual rights protection.

Fifth, strengthen cross-departmental regulatory coordination and tighten source governance. Establish a regular joint law enforcement mechanism among departments such as the cyberspace administration, industry and information technology, public security, and market supervision, and consolidate platform compliance responsibilities through special law enforcement inspections and

daily supervision; Establish a platform information protection compliance credit evaluation system, incorporate compliance into the platform credit file, and impose severe legal penalties on illegal and non-compliant platforms in accordance with the law; Promote the formation of a diversified collaborative protection pattern with government supervision, platform self-discipline, individual participation, and social supervision.

7. CONCLUSION

In the context of data and platform compliance, civil protection of personal information carries the dual value of safeguarding citizens' civil rights and promoting the high-quality development of the digital economy. This study focuses on analyzing the practical issues in this field, clarifying that China has formed a legislative framework for the civil protection of personal information with the Civil Code and the Personal Information Protection Law as the core, and has accumulated practical experience in judicial adjudication and platform supervision. However, in the practical scenarios of large-scale data processing and platform compliance operation, systemic problems still emerge in this field, which are mainly manifested in the poor connectivity mechanism of legislative provisions, practical obstacles to judicial implementation, the inadequate fulfillment of platform compliance responsibilities, and multiple constraints on individual rights protection. Such problems do not exist in isolation, but are interrelated and deeply intertwined. Measures taken by a single governance entity or institutional improvements from a single dimension cannot fundamentally solve this practical predicament. It is urgent for legislative, judicial, regulatory agencies, platforms and individuals to work together to forge a synergy of multi-stakeholder governance.

By improving the legislative system, optimizing the judicial implementation process, consolidating the compliance responsibilities of platform entities, enhancing individual rights protection capabilities, and strengthening cross-departmental supervision and coordination, targeted governance can be advanced from five dimensions. This can effectively address practical difficulties in the field and drive the protection of personal information rights and interests, platform compliance development, and the healthy progress of the digital economy to form a positive interaction. The continuous iteration and upgrading of digital technology have brought about new scenarios and governance challenges for personal information protection. Future institutional construction in this field needs to align with technological trends and practical demands, continuously optimize rule design, improve a comprehensive and multi-tiered protection mechanism, and promote the standardization and normalization of work in this field. Only by building a practice-adaptive legal system can we lay a solid legal foundation and provide solid institutional guarantees for the high-quality development of China's digital economy.

REFERENCES

[1] Romanosky, S., Hoffman, D., & Acquisti, A. (2014). Empirical analysis of data breach litigation. Journal of Empirical Legal Studies, 11(1), 74-104.

[2] Zuboff, S. (2015). Big other: Surveillance capitalism and the prospects of an information civilization. Journal of information technology, 30(1), 75-89.

[3] Wachter, S., Mittelstadt, B., & Floridi, L. (2017). Why a right to explanation of automated decision-making does not exist in the general data protection regulation. International data privacy law, 7(2), 76-99.

[4] Hylton, K. N. (2002). An asymmetric-information model of litigation. International Review of Law and Economics, 22(2), 153-175.

[5] Acquisti, A., Taylor, C., & Wagman, L. (2016). The economics of privacy. Journal of economic Literature, 54(2), 442-492.

[6] Koch, S., Altpeter, B., & Johns, M. (2023). The {OK} is not enough: A large scale study of consent dialogs in smartphone applications. In 32nd USENIX Security Symposium (USENIX Security 23) (pp. 5467-5484).

[7] McMahon, A., Buyx, A., & Prainsack, B. (2020). Big data governance needs more collective responsibility: the role of harm mitigation in the governance of data use in medicine and beyond. Medical law review, 28(1), 155-182.

[8] Barth, A., Datta, A., Mitchell, J. C., & Nissenbaum, H. (2006, May). Privacy and contextual integrity: Framework and applications. In 2006 IEEE symposium on security and privacy (S&P'06) (pp. 15-pp). IEEE.

[9] Citron, D. K. (2016). The privacy policymaking of state attorneys general. Notre Dame L. Rev., 92, 747.

[10] Calo, R. (2017). Artificial intelligence policy: a primer and roadmap. UCDL Rev., 51, 399.

[11] Ausloos, J., & Dewitte, P. (2018). Shattering one-way mirrors–data subject access rights in practice. International Data Privacy Law, 8(1), 4-28.