Scientific and Social Research, 2025, Volume 7, Issue 11
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Research on the Civil Law Protection of Citizens' Personal Information in the Big Data Era

Xinxin Wang*

College of Humanities & Information Changchun University of Technology, Changchun 130012, Jilin, China

**Author to whom correspondence should be addressed.*

Abstract: This paper examines the civil law framework for protecting personal information in China's big data context. It analyzes current legislation, including the Civil Code and Personal Information Protection Law, highlighting persistent challenges such as ambiguous rights attribution and inadequate enforcement mechanisms. The study proposes concrete improvements, including clarifying personal information rights, refining processing principles, establishing differentiated liability systems, and enhancing public interest litigation. These recommendations aim to balance effective protection with the legitimate utilization of data resources.

Keywords: Big data era; Civil law protection; Personal information right; Remedy mechanisms

Online publication: November 14, 2025

1. Characteristics of personal information in the big data era

In the big data era, personal information exhibits distinctive characteristics that challenge traditional legal protections. Firstly, it demonstrates enhanced identifiability. As defined in Article 4 of China's Personal Information Protection Law (PIPL), personal information refers to "various kinds of information, recorded electronically or otherwise, related to an identified or identifiable natural person" [1]. The power of big data analytics means that even non-traditional data fragments can be combined to identify individuals, expanding the concept far beyond direct identifiers like names or ID numbers.

Secondly, personal information possesses strong connectivity and aggregation value. Isolated data points, when aggregated, form comprehensive digital profiles or "personality sketches" of individuals, revealing preferences, habits, and behaviors. This aggregated data holds significantly more commercial and analytical value than discrete pieces of information, making it a prime target for large-scale collection.

Thirdly, its economic and property attributes are markedly accentuated. Personal information has evolved into a crucial factor of production and a tradable commodity within the data-driven economy [2]. Its commercial exploitation drives business models based on targeted advertising and personalized services, but also fuels a black

market for illicit data trade.

Finally, personal information is characterized by ease of replication and dissemination. Digital information can be duplicated and transmitted globally instantaneously at minimal cost, making containment after a breach nearly impossible. This, combined with the often-irreversible nature of privacy invasions once data is public, creates significant and lasting risks for data subjects.

2. Problems facing personal information protection in the big data era

2.1. Diversity of infringing subjects

The landscape of infringers has become highly diversified. Beyond individual hackers or criminals, the primary actors now often include powerful commercial entities such as internet platforms, data brokers, and corporations that collect and process user data on a massive scale as part of their core operations [3]. Furthermore, public authorities and government agencies constitute another significant category, given their extensive data collection for public administration, social security, and other governmental functions. This diversity creates a complex regulatory challenge, as a one-size-fits-all legal approach may not adequately address the differing powers and obligations of these varied actors.

2.2. Concealment of infringing acts

Infringements are increasingly covert and difficult to detect. Data processing operations are often conducted using complex algorithms and backend systems that are opaque to the average individual. Infringements may not cause immediately apparent harm; instead, they involve subtle, cumulative data harvesting and profiling [4]. As noted in academic discussions, the technical expertise and resources required to monitor these activities create a severe information asymmetry between data subjects and processors. Individuals are often completely unaware of when, how, or by whom their information is being collected and utilized, making it exceptionally difficult to discover infringements and initiate legal action in a timely manner.

2.3. Universality of the infringement scope

Personal information infringement has become a pervasive societal issue. Virtually every aspect of modern life—from using social media, shopping online, and navigating with GPS to undergoing facial recognition access control—involves the generation and potential exposure of personal data [5]. This universality means that nearly every individual is a potential victim. Large-scale data breaches affecting millions or even billions of user records have become commonplace, highlighting the systemic vulnerability of personal information in the digital ecosystem. This wide-scale risk undermines general trust in digital services and complicates enforcement efforts due to the sheer scale of the problem.

2.4. Diversification of infringement methods

The methods of infringement have multiplied and evolved. They range from illegal collection—such as covert tracking, hidden data harvesting through SDKs, or obtaining data through deceptive interfaces—to abuse of authorized data. A critical failure point is the operational breakdown of the "informed consent" rule [6]. In practice, "consent" is often obtained through lengthy, complex privacy policies that users do not read or understand, creating a scenario of "consent without real choice." Moreover, a significant problem is the repurposing and secondary use of data beyond the specific purpose for which it was initially collected, directly contravening the

purpose limitation principle stipulated in Article 6 of the PIPL, which mandates that "the handling of personal information shall have a clear and reasonable purpose" and be "directly related to the handling purpose." These diversified methods exploit legal and technical loopholes, making traditional tort law frameworks, which rely on clear, identifiable wrongful acts, less effective.

3. The current state of civil law protection for personal information in China's big data era

3.1. Relevant provisions in the civil code

The Civil Code establishes a foundational framework for personal information protection, marking a significant legislative advancement. Its provisions are characterized by their principled nature, setting the stage for specialized laws [7]. The key contributions of the Civil Code are systematically outlined in **Table 1** below.

Table 1. Key provisions for personal information protection in the Civil Code

Article	Core Content	Legal Function
Article 111 (General Provisions)	Mandates lawful acquisition and security assurance of personal information; prohibits illegal handling.	Establishes a general obligation for all information processors.
Article 1034 (Personality Rights)	Defines personal information and delineates its relationship with privacy rights.	Provides a legal definition and clarifies the application of law.
Article 1035 (Personality Rights)	Articulates the principles of legality, legitimacy, necessity, and requires consent for processing.	Sets the core principles for lawful processing activities.
Article 1037 (Personality Rights)	Grants data subjects the right to access, copy, correct, and delete their information.	Empowers individuals with control over their personal data.

As shown in **Table 1**, the Code's achievement lies in elevating personal information protection to a fundamental civil right within a personality-rights-based model. However, its provisions remain largely foundational, leaving operational details to be fleshed out by subsequent specialized legislation.

3.2. Relevant provisions in the personal information protection law

The Personal Information Protection Law (PIPL) constructs a detailed regulatory regime. It refines the definition of personal information, emphasizing "identifiability." The PIPL elaborates on fundamental principles and reinforces the "informed-consent" mechanism. It creates a distinct category for "sensitive personal information", subjecting its processing to stricter rules. A critical advancement is in Article 69, which establishes a presumption of fault for civil liability, substantially enhancing the legal position of data subjects in litigation.

3.3. Relevant provisions in other legal instruments

China's protection framework is reinforced by other laws. The Cybersecurity Law obliges network operators to adhere to core principles and sets rules for cross-border data transfers. The Data Security Law imposes general security obligations and mandates a classified protection system where personal information is a critical category.

3.4. Deficiencies in the civil law protection of personal information

Despite legislative progress, the current system reveals profound deficiencies in the big data era. The main shortcomings are summarized and analyzed in **Table 2**.

Table 2. Major deficiencies in the current civil law protection framework

Deficiency	Specific Performance	Consequence
Ambiguous Rights Attribute	Use of "rights and interests" rather than a definitive "right" (Legal interest model).	Results in weaker protection and a fragile basis for individual control.
Ineffective Core Principles	"Informed-consent" is illusory; "purpose limitation" conflicts with data analytics.	Undermines the foundational legal mechanisms for regulating processing.
Inadequate Remedial Mechanisms	Difficulty in proving damages; low compensation; underdeveloped public interest litigation.	Fails to provide effective deterrence or meaningful redress for victims.

Table 2 summarizes the primary defects. The ambiguous legal status of personal information weakens its protection fundament. Furthermore, core principles face severe operational challenges, becoming formalistic. Structural obstacles in tort remedies, including difficulties in proof and insufficient compensation, ultimately fail to deter violations effectively, leaving data subjects vulnerable.

4. Recommendations for the civil law protection of personal information in the big data era

4.1. Clarifying the rights attribute of personal information

The foundational step towards robust protection is to unequivocally recognize a subjective "right to personal information" within the civil law framework. The current "legal interest" model provides insufficient doctrinal grounding for individual control. Legislatively, this entails amending the Civil Code's Personality Rights Book to establish "Personal Information Right" as an independent, concrete personality right in a dedicated chapter, distinct from privacy. This right should be explicitly defined as a right of personality with a proprietary character, acknowledging its dual nature. Jurisprudentially, this clarification provides a solid basis for the proactive exercise of control by data subjects and strengthens the justiciability of infringements, moving beyond a model reliant solely on post-hoc tort liability.

4.2. Optimizing the principles for personal information processing

The core principles of "informed consent" and "purpose limitation" require substantive optimization to regain their relevance. The "informed consent" model must evolve beyond its current pro-forma application. This can be achieved by mandating granular and layered consent for distinct processing purposes, prohibiting blanket authorizations. For low-risk, routine processing, presumed consent with easy opt-out mechanisms could be considered, while for high-risk scenarios like sensitive data processing, explicit and reaffirmed consent must be strictly required. The "purpose limitation" principle should be applied with necessary flexibility. A doctrine of compatible use should be legally recognized, allowing secondary processing for purposes that are reasonably aligned with the original collection context and respect the data subject's legitimate expectations, provided adequate safeguards are implemented. This balances protection with the legitimate need for data utility.

4.3. Constructing a diversified system for tort liability and remedies

A one-size-fits-all approach to liability is inadequate. A differentiated liability system must be constructed based on the actor's role and power. For commercial information processors (platforms, data brokers), the PIPL's presumption of fault should be maintained and strengthened. For public authorities, whose power is inherently

coercive, strict liability should apply for breaches, given their elevated duties and the significant power imbalance. Regarding damages, the system must be enhanced to ensure meaningful redress. The threshold for non-pecuniary damages should be lowered to recognize the disruption and anxiety caused by privacy violations, even without severe psychological injury. Furthermore, punitive damages should be introduced for intentional or grossly negligent violations, calculated as a multiple of the illicit gains or actual losses. Establishing a statutory minimum damages amount for certain infringements would counteract the rational apathy of victims facing small individual losses but collectively significant harm.

4.4. Perfecting the public interest litigation mechanism

To address large-scale, diffuse harms, the public interest litigation mechanism requires substantial refinement. The standing of plaintiffs needs a clearer definition and hierarchy. The People's Procuratorate should be designated as the primary plaintiff for initiating such lawsuits, leveraging its investigative authority and legal expertise. Qualified consumer organizations and other entities designated by the Cyberspace Administration should act as supplementary plaintiffs. The trigger condition of "infringing upon the rights and interests of numerous individuals" must be objectively defined, considering factors like the sensitivity of the data, the scale of the breach, and the potential social impact, rather than relying on a purely numerical threshold. Finally, the synergy between public and private litigation must be enhanced. Rules should allow for the suspension of private suits pending the outcome of a related public interest action, and findings of fact from a concluded public interest case should have a binding effect on subsequent private suits concerning the same mass infringement, thereby promoting judicial efficiency and consistency.

5. Conclusion

In conclusion, the civil law protection of personal information in the big data era requires systematic enhancement. By clarifying rights attributes, optimizing processing principles, diversifying remedies, and strengthening public interest litigation, a more resilient and balanced protection framework can be established. Future efforts should focus on implementing these reforms to safeguard individual rights while fostering responsible data innovation and utilization in the digital age.

Disclosure statement

The author declares no conflict of interest.

References

[1] Chen X, 2025, Research on the Civil Law Protection of Personal Information in the Network Environment. Legal Vision, 2025(16): 49–51.

[2] Wei YR, 2024, Research on the Civil Law Protection of Personal Information Rights in China under the Background of the Network Environment. Legal Vision, 2024(21): 34–36.

[3] Miao CG, 2024, Consumer Personal Information Protection from a Comparative Law Perspective. Journal of Global Research in Education and Social Science, 18(4): 30–34.

[4] Xu HJ, 2023, Research on the Civil Law Protection Norms of Citizens' Personal Information Rights under the

Background of Big Data. Legal Vision, 2023(12): 106–108.

[5] Huang H, 2024, Research on Cross-Border Protection of Personal Financial Information from the Perspective of China Civil Code. Beijing Law Review, 15(2): 563–575. https://doi.org/10.4236/BLR.2024.152035

[6] Fan LJ, 2022, Research on the Civil Law Protection of Personal Information. Culture Journal, 2022(12): 155–158.

[7] Chen CW, 2020, Investigation Report on the Current Situation of Civil Law Protection of Personal Information in China. Law and Economy, 2020(11): 61–62.