Economics, Law and Policy
ISSN 2576-2060 (Print) ISSN 2576-2052 (Online)
Vol. 9, No. 1, 2026
www.scholink.org/ojs/index.php/elp

Original Paper

The Dilemma and Perfection of the "Substituted Decision-Making" Mechanism in the Protection of Minors' Personal Information

Xinyu Liu[1]

[1] Dalian Ocean University, Dalian, Liaoning, China

Received: January 5, 2026 Accepted: January 11, 2026 Online Published: January 13, 2026

doi:10.22158/elp.v9n1p35 URL: http://dx.doi.org/10.22158/elp.v9n1p35

Abstract

In the context of the digital economy, the protection of minors' personal information encounters challenges in coordination and implementation, necessitating stronger institutional safeguards. Such information embodies dual interests: the minor's own personal information rights and the parental guardianship rights. Effective governance requires clear age thresholds and balanced consideration of relevant interests. Central to the legal framework is the guardian consent mechanism, which is based on the "substituted decision-making" model from civil guardianship theory. To address practical gaps, this mechanism should be refined in terms of identity verification, validity of consent, and consent withdrawal. Enhancing these aspects can help resolve key difficulties in protecting minors' personal data.

Keywords

Minors, personal information protection, substituted decision-making, guardian consent mechanism

1. Introduction

Amidst technological advancements and data proliferation, the specialized protection of minors' personal information has emerged as a global imperative in the digital era, reflecting a universal societal commitment to safeguarding the well-being of younger generations (Fu, X. H., 2018, pp. 38-48). Grounded in empirical research, this study examines the distinctive legal attributes of minors' personal information and systematically analyzes the practical challenges within China's current legal protection framework, thereby contributing to the theoretical development in this field. In accordance with the latest legislative intent of the Law of the People's Republic of China on the Protection of Minors (hereinafter referred to as the "Minors Protection Law"), this paper further elucidates the

specific application of the "guardian consent" clause under Article 1035 of the Civil Code of the People's Republic of China (hereinafter referred to as the "Civil Code") in the context of minors' personal information protection. The analysis aims to provide a reference for the systematic enhancement of institutional development in this critical area.

2. Research Questions

In the field of minors' personal information protection, China's theoretical foundations and institutional practices have generally aligned with internationally prevalent approaches represented by Europe and the United States (Wang, Y., 2019, pp. 78-86). However, the domestic regulatory framework remains in its early stages, characterized by overly broad rule design, insufficient systematic coherence, and limited practical operability. Currently, China adopts a fragmented legislative model, resulting in scattered legal norms and a lack of integrated systemic construction. At the micro level, existing legislation primarily offers specific protections for minors from a privacy perspective within particular legal domains. For instance, several regulations in the field of criminal justice impose strict requirements on the protection of minors' personal data, case files, and other information carriers in judicial proceedings. The underlying claims are based on multiple laws, which may overlap and compete with one another. Moreover, the abundance of sector-specific regulations and the absence of comprehensive legislation have contributed to difficulties in the accurate application of the law. While the Civil Code, the Minors Protection Law, and the Regulations on the Cyber Protection of Children's Personal Information all stipulate guardian consent and disclosure obligations, none specify verifiable methods for obtaining such consent. This gap creates challenges in determining the standards and validity of guardian informed consent in practice, ultimately affecting the effectiveness of minors' personal information protection. Therefore, refining the legal application of the informed consent mechanism and enhancing its practical feasibility both legally and technically are crucial for effectively safeguarding the legitimate rights and interests of minors. At present, the protection of minors' personal information in China faces the following main issues.

2.1 Determination of Consent Validity

Currently, the normative framework for the protection of minors' personal information in China exhibits a fragmented structure, with relevant provisions dispersed across civil legislation, administrative regulations, departmental rules, and industry standards.These norms often overlap and duplicate in design, tend to be overly principled in formulation, and lack concrete operational guidelines—particularly in areas such as defining informed consent, which requires further refinement. While the understanding of personality rights has evolved from a passive model of "ex-post relief" to an active one emphasizing "autonomous decision-making," specific regulations to effectively safeguard the rights of minors and their guardians remain insufficient. Furthermore, there is a notable scarcity of guiding judicial cases in China at present. The application of guardian consent rules lacks clarity, and relevant judicial precedents largely remain confined to the paradigm of privacy rights protection,

failing to develop an independent adjudicative logic tailored to personal information protection.

2.2 Identity Verification Mechanism

In practice, the need to identify minor users has led to increased collection of relevant information; however, the misuse of identification regulations may result in excessive gathering of minors' personal data. Thus, how to accurately and effectively determine the true age of underage users has become a critical practical issue. Currently, national regulations are progressively requiring data processors to perform identity verification, while various internet-related normative documents also urge operators to implement real-name registration systems using technologies such as user profiling and biometric recognition. Nevertheless, standards and enforcement levels vary across industries. Since the gaming industry introduced the "online game anti-addiction" system in 2007—requiring game operators to verify users' age and restrict underage players through the anti-addiction mechanism—sectors such as gaming and finance have established relatively stringent real-name authentication and identification standards for minors. In contrast, platforms such as social media, dating applications, event platforms, information services, and e-learning tools tend to adopt looser regulations. Driven by commercial interests and due to a lack of institutional incentives for proactive identification, online operators often rely passively on age information voluntarily provided by users during registration, without further verification during subsequent usage. As a result, mechanisms designed to identify minors remain largely ineffective in practice.

3. Analysis of the Protected Legal Interests in Minors' Personal Information

3.1 Legitimacy of the Guardian Consent Mechanism

The personal information of minors embodies both the interests of the child and the parental rights of the parents, with the corresponding guardian consent mechanism and the consent mechanism under parental rights being interrelated yet distinct (Li, Y. S., 2015, pp. 179-192). In practice, due to limited cognitive and self-protective capacities, minors inevitably rely on the substitute protection and assistance of guardians or parents when facing frequent, hidden, and causally complex information infringements.

On the one hand, guardians possess the right to know and the right to act on behalf of the minor regarding their personal information based on the guardianship relationship. However, the exercise of these rights is aimed at protecting the minor's interests and is subject to corresponding limitations, intended to compensate for the minor's deficiencies in cognition and capacity to act, thereby enabling choices that better serve their well-being and fostering a more favorable environment for their growth. On the other hand, for parents, the leakage of their child's personal information may expose the child to danger, causing emotional distress and anxiety (Shi, S. K., 2000, p. 34). Parents hold parental rights as identity-based rights rooted in blood relations, reflecting an ethical order. State intervention in such rights must adhere to the principle of proportionality to avoid harming the parent-child relationship. Parental rights, grounded in identity, have evolved in meaning from "power" to "right" and further to

"obligatory rights," whereas guardianship emphasizes the duty of "supervision and care," is not strictly tied to identity, and is narrower in scope than parental rights. Thus, the protection of minors' personal information concerns both the immediate interests of the minor and the parental rights of the parents.

The guardian consent system is firmly grounded in legal theory and normative foundations. Article 1035 of the Civil Code stipulates that the processing of minors' personal information must comply with the principles of legality, legitimacy, necessity, and non-excessiveness, and requires the consent of their guardians. This provision rests on three key theoretical bases: First, the Civil Code establishes the principle of the best interests of the minor, which necessitates the refinement of guardian consent rules to address complex social realities. Second, minors exhibit notable rational deficiencies due to age-related limitations in cognitive and behavioral capacity; thus, the law primarily protects them by restricting their autonomy and allowing guardians to make decisions on their behalf. Third, the core of personal information self-determination lies in the positive capacities of informed consent. Given minors' limited comprehension, coupled with the unique issues concerning liable parties, applicable subjects, and the identifiability and sensitivity of personal information, the exercise of informed consent by parents on behalf of their children becomes essential (Feng, Y., 2019, pp. 98-110). Therefore, the protection of minors' personal information constitutes a legal paradigm rooted in information self-determination, wherein parents exercise the rights to know and consent as substitutes for their children.

3.2 Age Demarcation in the Protection of Legal Interests

When establishing special protection regulations for minors' personal information, a cost-benefit analysis should be applied to comprehensively balance various socioeconomic values and identify the most efficient and feasible normative model. The question of "at what age a child can consent to the processing of their own data" has been referred to by European data law experts as the "million-euro question." Scholars point out that determining the age at which rights are acquired or protection is lost requires balancing the minor's interest in informational self-determination as a rights-holder against the public interest in special state protection, while respecting the evolving capacities of the minor. Currently, there is no consensus on the age threshold for special protection of minors' personal information (Hodgkin, R., Newell, P. et al., 2002, p. 1). For instance, the U.S. Children's Online Privacy Protection Act (COPPA) sets it at 13, while the EU General Data Protection Regulation (GDPR) allows member states to determine the age—ranging from 13 to 16—at which special protection applies.

In practice, setting an age threshold defines the scope of special protection. Such protection typically takes the form of restrictive safeguards, meaning the minor's right to informational self-determination is subject to specific regulations such as guardian consent. Determining this age should involve comprehensive consideration of legislative coherence, provisions on civil capacity, challenges in distinguishing sensitive information, and practical difficulties in protecting minors' personal data. In China, although the Personal Information Security Specification is a recommended national standard, it

carries substantial market influence and serves as a key reference in enforcement. It classifies the personal information of minors under 14 as "personal sensitive information." The age of 14 has gradually emerged as a demarcation line in China's fragmented legal framework, informed by judicial practice and the developmental characteristics of minors. For example, relevant criminal offenses concerning children under the Criminal Law generally use 14 as the threshold. This approach is also reflected in Article 15 of the Personal Information Protection Law (Draft) published in October 2020, which stipulates that processing personal information of minors under 14 requires guardian consent, thereby aligning with the Regulations on the Cyber Protection of Children's Personal Information.

Accordingly, a tiered protection mechanism can be constructed:

First, for minors under 14, their personal information should be treated as sensitive and governed by a guardian consent rule based on the "substituted decision-making" model. This model applies when minors lack full capacity, characterized by the negation of their decision-making ability in specific matters, decisions made by guardians based on the "best interests" principle—even if contrary to the minor's wishes—and the exercise by guardians of consent, representation, and other powers to fulfill protective duties (Li, X., 2019, pp. 64-78).

Second, for minors aged 14-18, protection should follow the general principles of guardianship and parental rights, shifting toward a "supported decision-making" model. This approach centers on respecting the minor's autonomous decisions, with guardians playing a supportive role to balance their growing "freedom of will." Furthermore, minors aged 16 or older who primarily rely on their own labor income may be granted full informational self-determination to reduce barriers to social participation and avoid unduly restricting their labor and social rights.

The newly revised Minors Protection Law includes a dedicated chapter on cyber protection, integrating compulsory administrative measures with educational guidance to create a comprehensive governance framework covering both online and offline contexts. Moving forward, efforts should continue to refine the guardian consent system based on the "substituted decision-making" model, clarifying coordinated safeguards and conflict-resolution rules across different scenarios to systematically enhance the effectiveness and precision of minors' personal information protection.

4. Guardian Consent Mechanism Based On the "Substituted Decision-Making" Model

4.1 Defining Rules of Validity

In the protection of minors' personal information, guardian consent serves as a core rule, and the determination of its validity must adhere to a strict standard of "autonomy of will." Obtaining consent is only the first step toward compliance; subsequent data processing may still be deemed invalid or unlawful if it violates specific regulations (Lu, Q., 2019, pp. 149-160). From a comparative law perspective, the U.S. Children's Online Privacy Protection Act (COPPA) establishes an enforcement system centered on "verifiable parental consent," dynamically assessing corporate compliance efforts through a "sliding scale" approach and creating a "safe harbor" mechanism to encourage industry

self-regulation. The EU General Data Protection Regulation (GDPR), on the other hand, sets forth four elements of consent—voluntary, specific, informed, and unambiguous—supported by codes of conduct and certification mechanisms, thereby forming a layered regulatory framework.

Although current Chinese regulations have introduced the requirement of explicit consent, they lack specific operational rules regarding identity verification and consent validation, leading in practice to widespread reliance on blanket authorizations and passive compliance. To enhance the effectiveness of the system, refinement should focus on three core stages: "prior acquisition–adequate notification–explicit consent." The prior acquisition stage should implement an "opt-in" mechanism, avoiding the replacement of active consent with standard terms; the adequate notification stage must disclose key information clearly and comprehensibly to safeguard the right to know; and the explicit consent stage should integrate identity verification and validation technologies to ensure the genuineness of consent. Furthermore, in statutory exceptional circumstances such as public interest, consent may be exempted, provided that such exemptions are constrained by the principles of proportionality and due process.

4.2 Perfecting Identity Authentication Regulations

The effective protection of minors' personal information is contingent upon the accurate identification of underage subjects, thereby enabling the application of special rules grounded in the principle of protecting the vulnerable. Drawing from European and American legislative models, a comprehensive assessment—considering factors such as service content, language, advertising, and audience composition—should determine whether an online service targets minors. If so, operators must actively collect age information to distinguish underage users (Matecki, L. A., 2010, pp. 318-347). To mitigate social costs and data exposure risks, enforcement should evaluate relevant factors like service nature and marketing methods to decide the applicability of specific rules and penalties. Since reliance solely on self-declaration is insufficient, institutional incentives are needed to motivate operators to proactively identify minors.

Improvements can focus on two areas: First, establishing a certification mechanism for minors' personal information protection. Learning from the GDPR's third-party certification model, such a system would assess compliance, risk control, and technical standards to create a credible "commercial appearance," incentivizing corporate compliance and providing practical references for refining rules. Second, implementing a centralized identity verification system. It is advisable for the national cyberspace authority to lead the development of a unified platform for verifying minors' identities, utilizing technologies like AI for non-retentive identity checks. This platform could integrate with a guardian registration system, supporting multi-channel consent verification (e.g., phone, email) and allowing users to preset a "negative list" to restrict the collection of sensitive information from the outset.

4.3 Refining the Standards for Informed Consent

Minors undergo continuous physical and mental development, during which their perspectives and cognition remain relatively fluid. Influenced by age-specific behavioral traits and emotional fluctuations, they are more vulnerable to harm in the online environment. Therefore, when minors later realize that their prior consent to the processing of personal information may have compromised their privacy or reputation, they should have the right to request that operators delete the relevant data—that is, to exercise the right to withdraw consent and the right to erasure. China's Regulations on the Cyber Protection of Children's Personal Information have established the right to erasure, requiring operators to promptly delete information when guardians withdraw consent or when services are terminated. The Shenzhen Special Economic Zone Data Regulations (Draft for Comments), issued in July 2020, also clarify that natural persons may withdraw consent at any time and that operators must delete the collected data accordingly. Such rules are particularly important for the protection of minors, as they ensure that the lifecycle of personal information remains subject to the data subject's autonomy and prevent information processing from becoming disorderly. Thus, comprehensive legislation on the protection of minors' personal information should uniformly establish rules on consent withdrawal and the right to erasure.

In practice, many online services, particularly mobile applications, often obtain user consent in opaque ways. For instance, while privacy policies may specify the scope and purposes of data collection, actual processing practices may deviate from these policies due to operational changes, effectively rendering the consent meaningless. Therefore, the law must focus on safeguarding the right to information of minors and their guardians. Although claiming erasure through civil liability after an infringement occurs remains an available remedy, the effectiveness of the right to erasure is significantly diminished at that stage. It is more crucial to establish mechanisms that allow data subjects to keep track of how their personal information is being used in real time, rather than passively waiting for harm to materialize. Thus, the core issue shifts from "whether one can request erasure" to "what information one can request to be erased," making the right to information a prerequisite for exercising subsequent rights.

Enforcement practices under the COPPA framework in the United States reveal that most cases involve a lack of transparency and failures in the consent mechanism, primarily manifested as insufficient disclosure to guardians about data processing practices or the collection and disclosure of children's information without valid consent. Moreover, processing children's information in violation of existing privacy policies is also a common issue.

Therefore, information controllers should establish proactive disclosure mechanisms, regularly informing minors and their guardians about the types and scope of personal information under their control or providing accessible summaries in account management interfaces, thereby effectively safeguarding the right to information and the subsequent right to erasure. Furthermore, in the digital environment, when information flows from the private to the public sphere, operators should bear a

duty of prudent review and proactively notify minors and their guardians when the processing is likely to involve minors' personal information. This not only aligns with the principles of social protection and cyber protection under the Minors Protection Law but also represents an important aspect of corporate social responsibility. For example, when minors post information online that may expose them to risks, operators should promptly alert guardians and, when necessary, take protective measures directly.

5. Conclusion

The key to protecting minors' personal information lies in establishing an operational framework centered on "verifiable guardian consent." While China's current regulatory system has laid a foundational structure, its effectiveness is significantly undermined by the absence of concrete rules for identity verification and consent validation.

Therefore, building upon the legal rationale of "substituted decision-making," the framework must be refined through specific measures: establishing dynamic compliance assessment standards, developing certification and third-party verification mechanisms to incentivize proactive compliance, and exploring the creation of a state-led integrated identity verification platform. The fundamental objective is to translate the principle of "the best interests of the child" into enforceable and verifiable rules, thereby achieving an effective balance between rights protection and digital development.

References

Feng, Y. (2019). The Modern Transformation of Child Guardianship Models and Their Proper Arrangement in the Civil Code. *Oriental Law, 2019*(4), 98-110.

Fu, X. H. (2018). The Dilemma and Response to the Legal Protection of Children's Data in the Big Data Era: Also Commenting on Relevant Provisions of the EU General Data Protection Regulation. *Journal of Jinan University (Philosophy & Social Science Edition), 2018*(12), 38-48.

Hodgkin, R., Newell, P. et al. (2002). *Implementation Handbook for the Convention on the Rights of the Child* (p. 1). New York: United Nations.

Li, X. (2019). Supported Decision-Making Replacing Substitute Decision-Making in Adult Guardianship: Also on the Addition of Guardianship and Support in the Marriage and Family Section of the Civil Code. *Chinese Journal of Law, 41*(1), 64-78.

Li, Y. S. (2015). On the Privacy Right of Minors. *Law and Social Development, 2015*(6), 179-192.

Lu, Q. (2019). The Normative Structure of the "Consent" Rule in Personal Information Protection. *Wuhan University Journal (Philosophy & Social Science), 72*(5), 149-160.

Matecki, L. A. (2010). Update: COPPA Is Ineffective Legislation! Next Steps for Protecting Youth Privacy Rights in the Social Networking Era. *Northwestern Journal of Law & Social Policy*, *5*(2), 318-347.

Shi, S. K. (2000). *Law of Domestic Relations* (p. 34). Beijing: China University of Political Science and Law Press.

Wang, Y. (2019). The Legislative Approach to Online Personal Information Protection for Minors in China: Rethinking the "Guardian or Parental Consent" Mechanism. *Journal of Xi'an Jiaotong University (Social Sciences)*, *39*(6), 78-86.