Scientific and Social Research, 2025, Volume 7, Issue 10
https://ojs.bbwpublisher.com/index.php/SSR
Online ISSN: 2981-9946
Print ISSN: 2661-4332

Research on Legal Issues of Adolescent Data Security from the Perspective of Global Data Security Law

Weiwei Li*, Fangyu Liu*

High School Affiliated to BIT, Beijing 100089, China

**Authors to whom correspondence should be addressed.*

Abstract: Adolescents, as active participants in the digital era, face increasing risks to data security, including online education breaches, social media misuse, and unlawful data collection. This paper defines adolescent data (ages 12–18) and underscores its importance for individual growth and social stability. Through literature review, case analysis, and comparative study of the EU's GDPR, the U.S. COPPA, and laws in Japan and South Korea, it finds shared principles of necessity, security, and consent, yet divergent approaches in regulation, penalties, and scope. While China's Law on the Protection of Minors and related statutes provide a foundation, problems remain: vague definitions, weak regulatory mechanisms, and limited industry self-regulation. To address these, the paper proposes clarifying definitions and rights, strengthening sanctions, improving regulatory coordination with advanced technologies, and enhancing self-discipline and public awareness. These measures aim to refine China's legal framework and better protect adolescent data security in line with global best practices.

Keywords: Youth data security; Global data security law; Data breaches and misuse

Online publication: October 29, 2025

1. Introduction

Adolescents are key participants in the digital era but face serious data security threats, including breaches, misuse, and unlawful collection. Protecting their data is essential to close legal gaps and safeguard rights during a critical stage of development. Internationally, the U.S. *Children's Online Privacy Protection Act* (COPPA) and the EU's *General Data Protection Regulation* (GDPR) provide important safeguards, though challenges in cross-border governance and emerging technologies remain [1]. In China, the *Law on the Protection of Minors* and the *Data Security Law* have laid foundations, yet problems of vague definitions, weak enforcement, and limited localization persist. This study adopts literature review, case analysis, and comparative research, integrating legal, sociological, and psychological perspectives to propose more comprehensive and practical improvements for China's adolescent

data protection framework.

2. Theoretical analysis of adolescent data security

2.1. Definition and scope of adolescent data

Definitions of adolescence vary: the UN and China's Law on the Protection of Minors set 18 as the upper limit; the WHO defines 10–19; and Erikson's theory identifies 12–18 as the stage of identity formation. For this study, adolescence is defined as ages 12–18, a period of high digital engagement and limited risk resilience, thus requiring focused legal protection [2].

Adolescent data includes personal identity data (e.g., names, ID numbers) vulnerable to theft and fraud; health data (medical and psychological) at risk of privacy breaches and discrimination; educational data (grades, learning habits) affecting fairness in evaluation and admissions; and social data (friend lists, messages) prone to bullying, privacy violations, and psychological harm [3–4].

2.2. The critical value of adolescent data security

Adolescent data security is essential for individual well-being and social stability. Leaks can cause anxiety, harm privacy, and expose youth to consumerist manipulation. At the societal level, secure data reduces fraud and bullying, supports educational fairness by ensuring proper use of student information, and helps maintain a safe online environment, thereby fostering healthy adolescent development.

3. Analysis of the current status of global data security laws

3.1. Overview of data security laws in major countries and regions

The analysis in **Table 1** shows both convergence and divergence in adolescent data protection. All jurisdictions stress consent, minimization, and limits on secondary use, reflecting recognition of adolescents as a vulnerable group [5]. Differences remain: the EU adopts strict, comprehensive regulation; the U.S. applies a fragmented federal–state model; and Japan and South Korea combine statutory rules with varying self-regulation. These divergences complicate cross-border data flows and pose challenges for adapting foreign models to China's context.

3.2. Comparison and lessons from international data security laws

Across jurisdictions, adolescent data protection converges on key principles: necessity and minimization in collection, secure storage, rights of access and deletion, and consent-based sharing. Differences remain in governance models, enforcement, and scope. The U.S. FTC is efficient but resource-limited [6]; the EU enforces strictly but at high coordination costs; Japan's system is fragmented; and South Korea's body needs stronger collaboration. Penalties are heavier in the U.S. and EU, lighter in Asia; coverage is broad in the EU, narrower elsewhere [7]. For China, lessons include creating a unified regulator, raising sanctions, and balancing domestic needs with cross-border governance. The age definition of adolescents in different countries' laws is presented in **Figure 1**.

Table 1. Comparative analysis of adolescent data security laws in major jurisdictions (EU, U.S., Japan, and South Korea)

Comparative dimension	European Union (Centered on GDPR)	United States (Centered on COPPA and State Laws)	Asian countries (Japan, South Korea)
Core Legal Basis	*General Data Protection Regulation (GDPR)*, effective 2018	1. *Children's Online Privacy Protection Act (COPPA)*, enacted in 1998 2. State-level laws (e.g., Student Online Personal Information Protection Act in California)	1. Japan: *Act on the Protection of Personal Information* 2. South Korea: *Personal Information Protection Act*
Applicable Age Range	No unified lower limit; for minors under 16, parental/ guardian consent required	1. COPPA: under 13 2. State laws: often cover K–12 students (approx. ages 5–18)	1. Japan: under 15 as minors; parental consent required; varies depending on context (14 years in some cases) 2. South Korea: under 14 defined as minors; parental consent required
Data Collection Rules	Emphasis on "data minimization"; prohibit excessive collection; mandatory clear informed consent	1. COPPA: prohibits collecting personal info (e.g., photos, messages) without parental consent 2. State laws: prohibit unnecessary student data collection	1. Japan: under 15, collection requires parental consent; explicit prohibition on collecting unnecessary adolescent data 2. South Korea: requires prior consent; limits data to "minimum necessary for purpose"
Data Storage Requirements	Strict: enhanced protection, mandatory deletion after achieving purpose; storage period must be "no longer than necessary"	No unified storage period; requires reasonable safeguards. State laws demand protection of student data security and prohibit unauthorized disclosure	1. Japan: requires clear technical standards; industries must comply 2. South Korea: requires clear storage periods and prohibits "excessive long-term retention"
Data Usage Restrictions	EU principle of "purpose limitation"; explicit right to access, correct, erase; prohibition of secondary use beyond original purpose	1. COPPA: use only for specified purposes 2. State laws: prohibit use of student data for non-educational purposes (e.g., targeted advertising)	1. Japan: no restriction on use scope, but prohibits transfer for commercial purposes 2. South Korea: prohibits unauthorized commercial use of adolescent data
Supervisory Authorities	EU level: European Data Protection Board (EDPB); national level: supervisory authorities (e.g., German Federal Data Protection Authority)	1. Federal: Federal Trade Commission (FTC), e.g., 2019 fined YouTube $170M 2. State: state-level *Attorney General* offices	1. Japan: Personal Information Protection Commission; supplemented by industry self-regulatory bodies 2. South Korea: Personal Information Protection Commission (specialized supervisory body)
Key Challenges	High compliance costs; cross-border conflicts; burdens for SMEs	Federal and state law fragmentation; weak mobile app/data broker regulation; enforcement challenges	1. Japan: weak industry self-discipline; insufficient enforcement capacity 2. South Korea: fragmented supervisory authorities; enforcement mechanisms incomplete

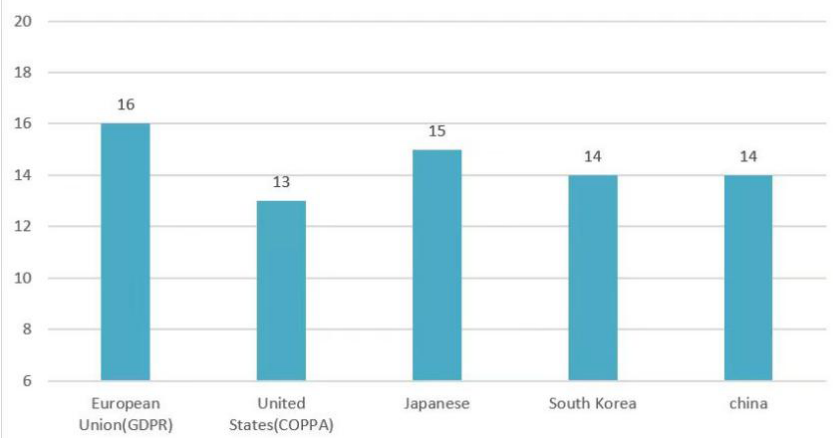

Figure 1. Age definition of adolescents in different countries' laws

4. Challenges and threats to adolescent data security

4.1. Risks of data breaches in the online environment

Adolescents face increasing risks from large-scale data breaches. In 2024, U.S. ed-tech company PowerSchool suffered a cyberattack in which hackers exploited employee credentials to steal tens of millions of minors' Social Security numbers and medical records, causing identity theft risks and reputational damage. Beyond individual cases, many platforms still lack adequate safeguards: authentication often relies on weak passwords without multi-factor verification, encryption is poorly implemented, and access controls allow unauthorized internal or third-party data use, all contributing to persistent vulnerabilities.

4.2. Data misuse and improper use

Commercial misuse is widespread. Institutions collect browsing and purchase histories to push targeted ads, reinforcing consumerist values, while illicit markets trade adolescent data, as shown in a 2023 case involving over 50,000 stolen records [8]. Government agencies also face compliance issues: over-collection of student data, irregular sharing without clear accountability, and weak storage protections all increase exposure to misuse and cyberattacks, undermining minors' rights.

4.3. Risks of cross-border data flows

Globalization of education and social platforms has expanded cross-border transmission of adolescent data, raising compliance risks due to legal divergences. The U.S. emphasizes self-regulation, while the EU enforces strict GDPR standards, complicating corporate compliance [9]. Multi-jurisdictional flows often create overlapping or absent regulatory authority, making coordinated responses to breaches difficult and exacerbating systemic security risks.

5. The current status and problems of legal protection for adolescent data security in China

5.1. Protection of adolescent data security in China's existing legal system

China has built a multi-layered framework for adolescent data security. The Law on the Protection of Minors requires lawful, necessary processing and guardian consent for those under 14, with rights of correction and deletion. The Personal Information Protection Law reinforces these requirements with specific rules and safeguards, while the Cybersecurity Law mandates lawful collection, clear purpose, and user consent. Together with recent regulations, these laws form the backbone of China's adolescent data protection system.

5.2. Problems and deficiencies

China's adolescent data protection still faces three main challenges: ambiguous provisions, weak regulation, and poor self-regulation. Current laws lack a unified definition of "adolescent data" responsibility among platforms, processors, and third parties remains unclear, and sanction standards are vague. Regulatory mechanisms suffer from overlapping duties, insufficient inter-agency coordination, and outdated technical capacity, limiting effective enforcement [10]. At the same time, enterprises often neglect disclosure and safeguards, industry associations lack binding authority, and cooperation across firms is minimal, leaving systemic risks inadequately addressed.

6. Pathways to improve China's legal protection system for adolescent data security

To strengthen adolescent data security, China should refine legislation, optimize regulation, and promote industry–society co-governance. Legislation must explicitly define adolescent data (ages 12–18), include sensitive categories such as biometric and health information, and grant minors and guardians stronger rights of consent, information, correction, and deletion. Sanctions should be stricter, and criminal liability applied to serious violations. On regulation, a national authority should coordinate adolescent data protection, supported by specialized roles for cyberspace, public security, and education departments, with inter-agency mechanisms ensuring coherence. Advanced technologies such as big data, AI, and blockchain should be integrated into monitoring and enforcement. At the societal level, industry associations should develop binding codes and oversee compliance, while enterprises strengthen transparency, internal management, and third-party controls. Public awareness must also be enhanced through school education, guardian training, and media outreach. Together, these measures would establish a more coherent, technology-enabled, and participatory framework for safeguarding adolescent data in China.

7. Conclusion and prospects

This study reviewed global adolescent data security laws, noting that while the EU's GDPR, the U.S. COPPA, and Japan–South Korea frameworks share a protective orientation, they differ in supervision, penalties, and scope. China's legal system provides a foundation but still faces vague definitions, weak regulation, and limited industry self-discipline. To address these issues, this paper proposes refining legislation, clarifying responsibilities, enhancing regulatory tools, and fostering industry and social co-governance. Future research should examine the dual risks and potential of emerging technologies, explore unified cross-border governance mechanisms, and strengthen long-term public awareness, all of which are crucial for building a more comprehensive and future-oriented framework for adolescent data security.

Disclosure statement

The authors declare no conflict of interest.

References

[1] Raina K, 2022, Children's Privacy and Safety. International Association of Privacy Professionals (IAPP), Portsmouth. https://iapp.org/resources/article/childrens-privacy-and-safety/

[2] Garfinkel S, 2000, Database Nation: The Death of Privacy in the 21st Century. O'Reilly Media, Sebastopol.

[3] Keenan TP, 2014, Technocreep: The Surrender of Privacy and the Capitalization of Intimacy. OR Books, New York.

[4] Packard V, 1964, The Naked Society. David McKay Publications, New York.

[5] McCabe K, 2017, Protecting Your Children Online: What You Need to Know about Online Threats to Your Children. Rowman & Littlefield, Lanham.

[6] Zhang L, Kollnig K, 2024, Theory and Practice: The Protection of Children's Personal Information in China. International Data Privacy Law, 14(1): 37–52. https://doi.org/10.1093/idpl/ipad017

[7] Milkaite I, Verdoodt V, Lievens E, 2021, Children's Reflections on Privacy and the Protection of Their Data. Children and Youth Services Review, 2021(128): 106137. https://doi.org/10.1016/j.childyouth.2021.106137

[8] Verdoodt V, Milkaite I, Lievens E, 2023, Safeguarding the Child's Right to Privacy and Data Protection. International Journal of Children's Rights, 31(2): 269–293. https://doi.org/10.1163/15718182-31020004

[9] Crepax T, 2022, Information Technologies Exposing Children to Privacy Risks. Technology in Society, 2022(68): 101912. https://doi.org/10.1016/j.techsoc.2021.101912

[10] Xu H, Tan BCY, Chiu CM, 2023, Developing and Testing the Children's Online Privacy Scale. Journal of Consumer Affairs, 57(1): 231–254. https://doi.org/10.1177/07439156231165250