Proceedings of the 3rd International Conference on Global Politics and Socio-Humanities
DOI: 10.54254/2753-7048/2025.23023

Challenges and Legislative Responses to Privacy Protection in the Digital Age

Tong Lin

Law School, Shanghai University of International Business and Economics, Shanghai, China
779837150@qq.com

Abstract: In the digital age, the right to privacy faces more severe threats, which are reflected in the diversification of privacy infringement methods, the control of personal privacy by platforms and the associated risk of data breaches, and the increasing frequency of privacy violations. Currently, China has not established dedicated legislation for privacy protection; instead, there are scattered provisions in certain laws, administrative regulations, local regulations, and rules. The challenges in privacy protection are mainly reflected in the following aspects: incomplete legislation, difficulty in identifying privacy infringements, the exacerbation of privacy violations due to the imbalance of power between platforms and individuals, and insufficient legal remedies. In the digital age, privacy protection should be strengthened in three key areas: first, improving privacy protection legislation; second, establishing mandatory information disclosure obligations for businesses; and third, enhancing legal remedies for users.

Keywords: Right to privacy, Digital age, Personal Information Protection Law

1. Introduction

Privacy rights are a fundamental human right and are of great significance for safeguarding human dignity and ensuring a peaceful life. However, with the advent of the digital age, the protection of individuals' privacy rights faces enormous challenges. The traditional tort liability framework established under civil law is no longer sufficient to fully achieve the objective of privacy protection. This is because digital communication has broken down the inherent boundaries of physical transmission and personal privacy domains. The diversity of digital technologies and data acquisition methods provides more avenues for others to access personal privacy information. Currently, Chinese scholars have mainly explored privacy protection in the digital age from two perspectives: legislation and theory. In terms of optimizing the legislative framework for privacy protection in the digital era, scholars have proposed developing a hierarchical privacy protection system based on constitutional principles [1], protecting privacy rights from a societal standpoint [2], and establishing privacy rights as a legal obligation to limit public power and protect vulnerable groups. Regarding the balance between public and private interests in the use of data in the digital age, scholars have suggested balancing data flow with the exclusivity of personal rights [3], and establishing absolute, strict, general, and weak public law protection mechanisms to balance social and personal interests [4]. Furthermore, to more comprehensively protect privacy information in the digital age, some scholars have proposed more refined classifications of personal privacy information. Suggestions include distinguishing between sensitive personal information and private information [5] and differentiating

© 2026 The Authors. This is an open access article distributed under the terms of the Creative Commons Attribution License 4.0 (https://creativecommons.org/licenses/by/4.0/).

DOI: 10.54254/2753-7048/2025.23023

between privacy rights and personal information rights in the application of laws and regulations [6]. However, existing research still largely relies on traditional civil law concepts to consider privacy protection and does not adequately account for the particular challenges posed by the digital age. This paper attempts to analyze the unique challenges faced by privacy protection in the digital age and proposes legislative improvements to strengthen the protection of privacy rights.

2. Increased risks of privacy infringement in the digital age

2.1. Diversity of methods for privacy infringement

The development of digital technologies, while providing convenience to people, has also increased the potential for privacy infringement [7]. This is reflected in two main aspects: first, it has become easier to access others' private information; second, the methods of infringing on privacy have become more diverse. For example, facial recognition information is a key factor in identifying personal characteristics and is highly sensitive, as it is linked to a large amount of personal privacy information. In recent years, the proliferation and refinement of facial recognition technology have increased the number and scale of scenarios where facial data is collected and analyzed, thereby posing a threat to individuals' privacy rights. A typical case is the 2019 contract dispute between Guo and Hangzhou Wildlife World Co., Ltd., heard by the Fuyang Court in Hangzhou, which involved the unauthorized collection of facial recognition data by a commercial entity.

Another common issue is the privacy consent terms attached to software downloads. These standardized terms, which govern the collection of personal information such as photos and phone files, create a power imbalance between businesses and users. Such terms are typically coercive: if users refuse to grant access to their personal information, they lose the right to use the software [8]. This creates an unequal dynamic in information acquisition and control, where the authorization of personal information becomes a precondition for using the software, exposing users to significant privacy risks.

2.2. Risks of privacy control and data leaks on digital platforms

Platforms have become the primary repositories for collecting and storing personal privacy; however, issues such as hacking, excessive data collection, and data leaks are prevalent in the digital economy. The root causes of these problems lie in the conflict between the pursuit of commercial interests by platforms and the inequality in access to informational resources. First, the pursuit of commercial interests undermines social ethics. Different platforms hold varying degrees and amounts of user information, which creates competitive advantages within the industry. Personal information allows businesses to generate profits through data monetization and establish a competitive edge over rivals. To gain this advantage, many companies compromise user privacy by excessively collecting, misusing, and leaking personal information. Some platforms engage in illegal practices, such as forced collection of personal data and deep mining of personal privacy. In practice, some apps have been found to force users to provide personal information without offering an option to withdraw consent. When an app fails to provide users with a convenient mechanism for withdrawing consent, the app is held responsible for deleting the collected data and compensating the user for any damages. This reflects the tension between the commercial incentives of platforms and the protection of personal privacy. Second, inequality in access to informational resources puts individuals at a disadvantage when negotiating terms of service. Platforms define the scope and level of information access through standardized terms, without engaging in genuine negotiation with users. To access more personalized and convenient services, users are often compelled to surrender more personal information [9]. This imbalance in data access capabilities and contract formation capacity creates a structural disadvantage for users[10]. Faced with the data collection dominance of platforms, many

DOI: 10.54254/2753-7048/2025.23023

users opt to trade privacy for convenience, exposing themselves to increased risks of privacy infringement. The state faces significant regulatory challenges due to the technological complexity of monitoring platform behavior. Platforms' extensive accumulation of data resources and informational advantages give them substantial leeway in how they handle user data, creating difficulties for state governance and enforcement.

2.3. Increasing harm from privacy breaches

In the digital age, people's growing dependence on electronic technologies has made it easier for platforms to access and control personal privacy information, such as phone numbers, home addresses, and family details. While these technologies offer convenience, they also increase the risk of privacy breaches and misuse of personal data. Many apps, after collecting users' private information, illegally sell this data to third-party merchants or sales agents, leading to serious privacy violations and negative consequences for individuals. For instance, in the unauthorized authorization case involving an automotive information app, a user named Lü used an automotive app to check car prices. Subsequently, his phone number was illegally leaked to car dealers through the app's backend data-sharing arrangements, infringing upon his personal privacy. This highlights how personal data, once collected, can be unlawfully exploited for commercial purposes. Moreover, digital communication platforms like WeChat, QQ, Weibo, and email have become essential tools for daily communication, making it easier for others to invade personal privacy. Individuals' private spaces, personal information, and private activities—things they wish to keep confidential—are increasingly vulnerable to breaches. A landmark case ruled by the Shanghai High People's Court—the Wu vs. Wang privacy dispute case—illustrates the psychological and emotional toll of privacy breaches. In this case, the defendant repeatedly harassed the plaintiff through phone calls, text messages, and emails, severely disrupting the plaintiff's private life. The plaintiff eventually developed depression due to the intense psychological pressure, significantly affecting their mental health and overall well-being. The escalation in harm caused by privacy breaches underscores the need for stronger legal responses. The increasing complexity and evolving nature of privacy violations present new and greater challenges for the existing legal framework, requiring more robust legislative and regulatory measures to protect individuals from such infringements.

3. Legislative status of privacy protection in China

The primary function of privacy protection legislation in the digital age is to address the risks of privacy infringement caused by the expansion of the public domain due to digital technology. Currently, China's legal framework for protecting privacy consists of two levels: at the central level, there are the Civil Code, the Data Security Law, and some administrative regulations; at the local level, there are local regulations that elaborate on the central legislation. This paper will outline the existing laws and regulations regarding privacy protection from both the central and local legislative perspectives.

3.1. Legal framework

An examination of national-level legislation reveals that China has made considerable progress in privacy protection. First, there is basic legislation concerning privacy rights. For example, Article 50 of the Constitution stipulates that "the freedom and secrecy of citizens' communications are protected by law," thereby safeguarding individual privacy that may be involved in communication secrecy as a basic civil right. Chapter 6 of the Civil Code of the People's Republic of China (hereinafter referred to as the "Civil Code") specifically addresses privacy rights and personal information protection, explicitly prohibiting the infringement of others' privacy (Articles 1032-1039). Articles 1032 and

DOI: 10.54254/2753-7048/2025.23023

1033 of the Civil Code provide detailed regulations, ensuring that personal information of individuals is legally protected, and it cannot be unlawfully collected, used, processed, or transmitted. For example, personal information such as an individual's ID number or bank passwords, which are classified as private information, should not be illegally used or collected by others, and such actions are protected under the Civil Code.

In addition to basic legislation, privacy protection is further reflected in several specific laws. Separate regulations exist for various types of privacy protection. For example, the Personal Information Protection Law of the People's Republic of China is China's first systematic and comprehensive law in the field of personal information protection. As personal information contains private data, this law plays an essential role in safeguarding individual privacy. Particularly, Article 28 of the law lists examples of sensitive personal information and employs a general provision to more broadly protect the security of related personal privacy data. Article 42, Section 6 of the Public Security Administration Punishments Law of the People's Republic of China stipulates that "peeping, secretly photographing, eavesdropping, or spreading others' privacy shall result in detention for up to five days or a fine of up to 500 yuan; in more serious cases, detention for over five but under ten days, and a fine of up to 500 yuan." This provision seeks to protect individuals' privacy rights by imposing financial and liberty penalties for acts such as eavesdropping and stealing information. The Cybersecurity Law of the People's Republic of China addresses the changes in information transmission and dissemination modes in the digital age. It regulates the collection and use of personal information by network operators, requiring that their actions must meet clear collection purposes and obtain user consent. This law helps enhance individuals' control over their privacy information and reduces illegal use. Since personal information contains private data, it also serves to protect privacy rights. The Consumer Rights Protection Law of the People's Republic of China, in Article 29, requires that operators collecting and using consumers' personal information must be transparent and ensure confidentiality, prohibiting the leakage or sale of such data. In the process of transactions between businesses and consumers, personal privacy such as phone numbers and home addresses may be collected. The law mandates that businesses keep this information confidential and not engage in illegal sales, thereby protecting transaction and privacy security.

3.2. Administrative regulations and departmental rules

Privacy protection is also reflected in numerous administrative regulations and departmental rules. For instance, the Regulations on the Administration of Credit Rating Services issued in 2013 regulate how credit agencies handle personal information, clarifying the rights of information subjects. The Regulations on the Security Protection of Critical Information Infrastructure, issued in 2021, aim to enhance the protection of important data and personal privacy information. The Measures for Data Exit Security Assessment, issued in 2022, aim to regulate the security assessment process for the outbound transfer of personal information and critical data. The Personal Information Exit Standard Contract Measures, issued in 2023, clarify the requirements for standard contracts concerning personal information transfer abroad.

3.3. Local legislation and administrative normative documents

To strengthen privacy rights protection, local governments and relevant institutions have refined personal privacy protection measures based on national regulations. For example, the Regulations of the Shenzhen Special Economic Zone include a dedicated chapter on personal privacy information protection. The Trial Measures for Personal Credit Rating Management in Shanghai limit how legally established personal credit rating agencies may use customer personal information [2]. By regulating public institutions' acquisition and use of personal privacy information, these local regulations further

DOI: 10.54254/2753-7048/2025.23023

safeguard individuals' rights. Additionally, the Cybersecurity Standard Practice Guidelines issued by the National Network Security Standardization Technical Committee, in Articles 3 and 4 and the Appendix, list various common types of sensitive information and advise information collection companies to carefully evaluate whether the information in question constitutes sensitive personal information. These efforts provide a more comprehensive explanation and protection for the application of privacy protection laws. In 2019, the General Office of the National Internet Information Office, the General Office of the Ministry of Industry and Information Technology, the General Office of the Ministry of Public Security, and the General Office of the State Administration for Market Regulation jointly issued the Method for Identifying Illegal Collection and Use of Personal Information by Apps, which specifies standards for recognizing illegal behavior related to personal information collection by apps.

4. Dilemmas in privacy protection in the digital age

4.1. Incomplete legislation

The importance of privacy protection in the digital age is growing, and legislation should actively address emerging privacy-related issues to play a positive role in safeguarding individual rights. Since personal information holds certain "commercial value," China's legislative system aims to balance the conflicting interests between data value and privacy protection. However, the current legal framework is insufficient to comprehensively safeguard personal privacy and requires continuous improvement. First, Chinese legislation has failed to effectively distinguish the boundaries between personal information and privacy information. According to Article 28 of the Personal Information Protection Law, sensitive information is classified as personal information. However, judicial interpretations reveal some overlap between the scope of sensitive information and personal privacy, though differences remain. Sensitive information refers to personal data that, if disclosed or unlawfully used, could lead to harm to a person's dignity or property security, such as genetic data, fingerprints, and specific identity information. Privacy, on the other hand, refers to secret spaces, activities, or information that individuals wish to keep private, with a greater emphasis on the subjective views and attitudes of the individual. Privacy encompasses various aspects of personal life, including emotional experiences and living habits [11]. It not only includes information that impacts property or personal dignity but also involves personal thoughts, feelings, and other subjective information that individuals tend to conceal. As a result, personal information and privacy rights overlap in the domain of sensitive information. Due to the significant differences in the level of protection and legislative values concerning personal information and privacy protection, and the separate regulation of these areas under the current system, the unclear boundary between them can lead to inadequate protection of information. Second, the lack of an effective accountability mechanism for privacy protection in China has resulted in a low cost for privacy violations. Currently, legislation primarily addresses personal information protection and data security, but there is no dedicated legislation or institutional design specifically for privacy protection in the digital age. As mentioned earlier, privacy rights are unique and require specialized institutional design. The absence of specific legislation in this area prevents sufficient institutional support for privacy protection. China's approach to privacy protection is scattered across various laws and regulations, including the Civil Code, the Personal Information Protection Law, the Data Security Law, and the Supreme People's Court's Provisions on the Application of Law in Civil Disputes Involving Infringements of Personal Rights Using Information Networks (Fa Shi [2020] No. 17). However, a comprehensive accountability mechanism has not yet been formed, and detailed provisions for handling cases of widely disseminated information are lacking. Furthermore, in the balancing act between the economic value of data and the protection of users' privacy rights, there has been a stronger focus on the

DOI: 10.54254/2753-7048/2025.23023

economic value of data, with insufficient punishment for data platforms that misuse personal information. This has resulted in many companies profiting from data with relatively low legal consequences.

4.2. Difficulty in identifying privacy infringement

In the context of the rapid expansion of digital information and social media, privacy violations in the digital age are often hidden and difficult for individuals to recognize. Personalized services provided by online platforms offer businesses channels through which they can access users' private information. A large amount of user data is leaked during the process of offering personalized services, including information about users' professions, home addresses, and details of other family members. This data is integrated and packaged into personalized profiles, which are then resold to dealers, who, driven by economic incentives, target consumers with precise advertisements [12]. In just the first half of 2023, platforms monitored 19,500 incidents of user data leakage across various industries, including finance, logistics, aviation, and e-commerce, causing harm to the privacy rights of numerous users. Many users are aware that their profession or home information has been illegally shared, but they often do not realize that such information is gathered through personalized services or backend operations provided by these platforms. Moreover, with the advent of screenshot capabilities on smartphones, personal privacy information is often unintentionally posted online and easily spread by others. According to China's Personal Information Protection Law, platform operators are obligated to remove content that infringes on personal privacy. However, due to the rapid spread of such content, many cases involving screenshots or related images cannot be retrieved or fully destroyed in judicial practice, resulting in continuous harm to the individuals involved.

4.3. The growing inequality between platforms and individuals intensifies privacy violations

In the digital age, online platforms control more resources and hold greater power, placing individuals in a subordinate position and thereby increasing the risk of privacy violations. With the widespread use of smart software, businesses have expanded the scope of data collection from individuals. From simply allowing software to send messages to users, to accessing users' photos and phone information, and further extending to intelligent devices and multi-scenario data, platforms are collecting more comprehensive personal data. Various standardized consent forms outline the terms under which businesses collect, store, and use data. However, if users reject these terms, platforms often refuse to provide services. Faced with powerful algorithms and service optimization demands, most individual users choose to relinquish their data rights. This results in platforms gaining extensive data rights, which in turn creates risks of data leakage or illegal use. Once platforms obtain this data, they frequently leak user information. Platforms use algorithms to analyze users' browsing history, travel records, and shopping habits to predict and recommend products based on users' preferences.

4.4. Insufficient legal remedies for privacy rights in the digital age

Privacy infringements in the digital age differ significantly from traditional privacy violations, making it difficult to define and prove these infringements. Currently, China's privacy protection laws still apply the fault-based liability system under the traditional Civil Code. In traditional privacy infringement cases, clear physical boundaries are necessary to determine harm, but the digital age introduces blurred boundaries of infringement, making it difficult for individuals to provide evidence. Most violations are not conducted through traditional, obvious methods, such as by mail, electronic messages, or phone calls, but through covert digital means, such as secret eavesdropping, backend data integration and transmission, and "human flesh" search techniques. As a result, individuals face challenges in obtaining evidence of the infringement process, making it difficult to protect their rights

DOI: 10.54254/2753-7048/2025.23023

effectively. Therefore, the current legal remedies for privacy rights in China are insufficient to fully protect individuals' interests. The inequality between platforms and individuals means that the private law remedies provided by the Civil Code cannot effectively address privacy violations.

5. Optimizing privacy protection in the digital age

Privacy, as a fundamental right of individuals, plays a vital role in protecting personal freedom, dignity, social interactions, personal secrets, and individual development. Digital privacy, as a core issue in the development of the digital age, should be central to privacy protection efforts. This includes gradually improving the legislative system for privacy rights in the digital age, while also fully utilizing the commercial value of non-sensitive personal information and establishing multi-platform supervision. It is essential to assign more regulatory responsibilities to operating platforms, businesses, and national supervisory authorities to balance the interests and values of privacy protection.

5.1. Improving legislation for privacy protection

5.1.1. Scientifically defining privacy

First, the definition of privacy in China focuses on strengthening and improving protections against new forms of privacy violations. Generally speaking, traditional privacy violations are easily recognized by the parties involved, but new forms of privacy violations are more difficult for individuals to identify and sue. Therefore, the scope of privacy rights should be more clearly defined to help individuals recognize violations and effectively protect their rights. New forms of privacy violations in the digital age primarily occur through the use of business-operated platforms, where businesses obtain vast amounts of private information from users or consumers via personalized recommendation services and then integrate and resell this data to enable targeted advertising for their own platforms. Individuals' privacy information exists not only in physical space but also in cyberspace. Therefore, the traditional concept of privacy protection, which focuses on "private space," should be expanded to include "information private space." Businesses' collection of users' digital information should be stored in this information private domain and must not be illegally integrated or resold without the natural person's consent. Second, the protection of sensitive personal information should fall under the scope of privacy rights protection. Sensitive information is the intersection between privacy and personal data. However, China's legislation on privacy and personal information protection adopts different principles and levels of protection. Privacy protection legislation generally employs stricter regulatory measures, with protection standards typically higher than those for personal data. According to Article 1032 of the Civil Code of the People's Republic of China, it is prohibited for organizations or individuals to infringe upon another person's privacy in various ways. On the other hand, personal information protection tends to focus more on protecting the economic value of the data, and personal information rights have not been established as an independent natural person’s right. When sensitive information is violated, it can cause personal harm or financial losses to individuals, significantly impacting their normal life. Therefore, to better protect sensitive information, it should be safeguarded under privacy-related laws and regulations.

5.1.2. Draw on international experience to develop specialized legislation

The challenges in privacy protection have become more prominent in the digital age, and the demand for enhanced protections is growing [13]. Thus, it is necessary to establish specialized legislation for privacy rights protection. This legislation should regulate aspects such as the definition of privacy rights, new forms of privacy violations in cyberspace, and the accountability mechanisms for online

DOI: 10.54254/2753-7048/2025.23023

platforms. At the same time, China can draw on international legislative experiences to improve its own privacy laws. For example, the United States has established the Privacy Act to protect privacy in the digital age, requiring platforms to obtain user consent before using their data and ensuring that personal data is not misused by online platforms. In 2018, the California Privacy Protection Agency issued the California Consumer Privacy Act, providing a pathway for businesses to comply with privacy regulations. In the digital age, businesses exploit their information advantage to “force” individuals into agreeing to share private information, a practice known as the "dark pattern," which effectively undermines and damages users’ autonomy, decision-making, and choices. Agreements obtained under these conditions do not constitute valid consumer consent [14]. It is worth noting that Colorado has also enacted the Colorado Privacy Act to regulate "dark patterns." By learning from international legislative experiences and combining them with China’s legal characteristics, a comprehensive and systematic privacy protection law can be formulated, which will more effectively safeguard individuals' rights.

5.2. Establishing disclosure mechanisms for privacy collection and use

The privacy access policies of platforms provide users with unequal advantages, so a disclosure mechanism for the collection and use of privacy information should be established to protect users' right to be informed. The scope of the platform’s disclosures should cover the entire process from data collection to data usage, including the range of data collected by the platform, the permissions for using the data, and the reasons for data collection. Firstly, during the data collection phase, the platform should disclose the scope of information collection to users through clear terms to ensure users are informed about the data being collected. When seeking users' consent to access their data, the platform should give special attention to the terms regarding data collection. For instance, these terms should be bolded or highlighted to draw users' attention, along with details such as the range of data being collected and the reasons for the collection. Additionally, the platform should provide consumers with the ability to limit the use of their sensitive information. While users who refuse privacy access may face certain restrictions in their platform experience, services should not be denied to these users. Secondly, during the data usage phase, the platform should disclose any sharing of data with other platforms. Platforms using user data for personalized recommendations and customization still involve the use of privacy information. If the platform has signed contracts with other platforms regarding data collection, it should disclose terms related to data resale or usage. This obligation should not only apply to service providers but also to new entities such as contractors. The platform’s disclosure of relevant data can effectively reduce the risk of users' data being violated.

5.3. Optimizing supervision and remedy mechanisms

Currently, the primary remedy for privacy protection is litigation; however, there are issues regarding insufficient protection. Public authority protection of individuals' rights not only provides civil remedies but also involves the supervisory and remedial measures from administrative agencies and social organizations. Firstly, specialized administrative regulatory agencies should be established to improve the oversight of administrative bodies concerning businesses and platforms' compliance in collecting and using user privacy data. Since businesses hold an information advantage and contractual performance advantage when collecting users' privacy data, to better safeguard consumer rights, in addition to the voluntary disclosure of data by businesses, dedicated administrative agencies should inspect and oversee the handling of users' privacy data. These agencies would be responsible for supervising relevant enterprises, institutions, and organizations' compliance with data protection laws. Their tasks would include ensuring businesses disclose related information, comply with the legal use of user privacy data, and provide consumers with access to legal remedies. Administrative

DOI: 10.54254/2753-7048/2025.23023

agencies should exercise vertical regulatory powers to manage business data, aiming to minimize the risks of information advantage harming consumer rights. As foreign experience shows, Germany has established an independent data protection regulatory agency (the Federal Data Protection and Freedom of Information Commissioner), which operates independently from both commercial interests and government, efficiently overseeing the enforcement of data protection laws. This body actively participates in policy development, offering professional advice and recommendations to legislative bodies to jointly improve data protection laws and policies [15,16]. Secondly, public interest litigation should be promoted to protect the information data of vulnerable users. Chinese legislation aims to achieve substantial equality of legal status between both parties in a contract and provides a route for public interest litigation to protect vulnerable users and consumers. Public interest litigation organizations can offer professional legal advice to the victims and provide investigative and evidence-gathering means. Prosecutors, by leveraging their public interest litigation functions and formal inspections, can gradually provide comprehensive protection for citizens' personal privacy information.

6. Conclusion

Optimizing privacy protection in the digital age is a fundamental response to the significant increase in privacy infringement risks. The specific measures are as follows: First, by defining privacy and its scope more clearly and drawing on international legislative experiences to establish specialized legislation, China can improve its privacy protection laws. Second, by establishing a disclosure mechanism for businesses to report how they collect and use user privacy data, the information disadvantage that users face compared to businesses can be weakened, thus ensuring users' right to be informed about their data. Third, by optimizing remedy mechanisms and supplementing with administrative supervision and public interest litigation, users can receive professional knowledge and enhanced investigative capabilities, ultimately achieving substantive equality in the legal status between users and businesses.

References

[1] *Li, Z. (2021). Constitutional construction of privacy rights in the digital age. Journal of East China University of Political Science and Law, 24(3), 42–54.*
[2] *Yu, C. (2023). Social theoretical reconstruction of privacy rights in the digital age. Chinese Journal of Law, 2, 184.*
[3] *Ren, Y. (2022). Juridical construction and rule reconstruction of privacy rights protection in the digital age. Eastern Law Review, 2, 188–200. https://doi.org/10.19404/j.cnki.dffx.20220225.002*
[4] *Chen, J. (2023). From private law to public law: The model extension of privacy rights protection in the digital age. Politics and Law, 11, 24–38. https://doi.org/10.15984/j.cnki.1005-9512.2023.11.004*
[5] *Li, S. (2024). Legislative responses to privacy rights protection in the digital age. Legal Studies, 3, 17–31.*
[6] *Ding, X. (2023). Jurisprudence of the relationship between privacy rights protection and personal information protection: A discussion on the application of the Civil Code and the Personal Information Protection Law. Legal and Commercial Studies, 6, 73.*
[7] *Personal Information Protection Law of the People's Republic of China.*
[8] *Sun, D. (2021). Social risks and legal regulation of facial recognition technology. Science of Science and Management of S&T, 39(1), 12–20, 32. https://doi.org/10.16192/j.cnki.1003-2053.20200729.001*
[9] *China Security Association. (2020). An analysis of the application of facial recognition technology in public security.*
[10] *Zhang, Z. (2021). Privacy protection in the big data surveillance society: An observation based on practices in the US and Europe. In Big Data and Privacy (p. 48). Shanghai People's Publishing House.*
[11] *Shanghai Municipal Government. (2020). [Privacy policy document]. Retrieved from https://www.shanghai.gov.cn/nw11226/20200813/0001-11226_901.html*
[12] *Shenzhen Municipal Legal Affairs Bureau. (n.d.). [Regulations on privacy protection]. Retrieved from http://szwljb.sz.gov.cn/flfg/fl/*
[13] *Personal Information Protection Law Article 28.*

DOI: 10.54254/2753-7048/2025.23023

[14] *Duan, Q., & Zhou, Y. (2022). A discussion on the causes of privacy violations in the digital age: From the perspective of attribution theory. Editing Journal, 3, 30–36.*

[15] *Nahra, K. J., Jessani, A. A., Mercer, S. T., Higgins, H., Gopinathan, A., & Pinto, T. Y. (2023). California Privacy Protection Agency releases draft CPRA regulations. WilmerHale.*

[16] *The role of prosecutorial agencies in protecting citizens' personal information through public interest litigation. (2021). Retrieved March 4, 2025, from https://www.12309.gov.cn/llzw/jyjl/202103/t20210329_514325.shtml*