Proceedings of the 4th International Conference on International Law and Legal Policy
DOI: 10.54254/2753-7048/2025.28039

The Impact of Facial Recognition Technology on Personal Information Protection and Corresponding Responses

Wenxuan Xia

North China University of Science and Technology, Tangshan, China
xiawenxuan050913@163.com

Abstract. Facial information, as a highly identifiable biometric trait, possesses triple legal attributes: sensitive information, biometric information, and personality interests. Based on the particularity of facial information, this paper analyzes the operational mechanisms of existing facial recognition technologies and systematically examines the processing logic and regulatory status of facial information throughout its full data lifecycle. The impact of facial recognition technology on personal information protection is primarily reflected in three aspects: legitimacy disputes in the information collection stage, technical risks during information processing, and rights infringements during information use. After analyzing these inherent contradictions, this paper proposes systematic response strategies from both legal regulation and technical governance perspectives.

Keywords: Facial Recognition Technology, Personal Information Protection, Facial Information, Informed Consent

1. Introduction

The report of the 20th National Congress of the Communist Party of China explicitly emphasizes strengthening personal information protection. Against this backdrop, laws and regulations such as the Personal Information Protection Law and the Data Security Law have been successively introduced, providing a normative foundation for the protection of personal information rights. In the context of rapid digital economic development, facial recognition technology, with its efficiency and convenience, has been widely applied in areas such as security surveillance, financial services, and transportation, significantly enhancing social operational efficiency. However, its application has also raised numerous legal issues. Existing legal norms have to some extent addressed the practical need to protect facial information rights, but they have not fundamentally solved the problem. Academic research has shown considerable attention to this issue, focusing primarily on two aspects. On one hand, studies examine the legal regulation of facial recognition technology [1,2]; on the other hand, research explores judicial remedies for personal rights protection [3,4]. Notably, the "first facial recognition case" in Hangzhou was selected as one of the "Top Ten Rule-of-Law Events in China in 2021," highlighting the significance of protecting facial information rights in both judicial practice and theoretical research. In view of this, this paper focuses on the legal attributes of facial information, revealing the inherent contradictions that facial recognition technology poses to personal information protection. Adopting a problem-oriented approach, it seeks

© 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: 10.54254/2753-7048/2025.28039

to improve and construct governance pathways for personal information protection within facial recognition technology.

2. Legal attributes of facial information

The core function of facial recognition technology lies in automatically extracting and comparing facial features to achieve identity authentication in fields such as public services, intelligent security, and convenient payment systems [5]. The application of this technology is based on the collection and processing of facial information. As a type of biometric data, facial information possesses three primary legal attributes: Sensitive Information Attribute: Facial information is directly linked to personal identity, and its leakage or misuse may pose security risks. It falls within the scope of sensitive personal information as defined by the Personal Information Protection Law. Biometric Attribute: As an inherent physiological characteristic of the human body, facial information is unique, stable, and immutable, serving as a key element in biometric recognition. Personality Interest Attribute: Facial information embodies personal dignity and image rights. Its processing implicates multiple personal rights, including portrait rights and privacy rights. Thus, the sensitive information, biometric, and personality interest attributes of facial information highlight its special status in personal information protection.

2.1. Sensitive information

Current Chinese law explicitly includes facial information within the scope of protected sensitive personal information. Article 28 of the Personal Information Protection Law classifies biometric information as sensitive information and emphasizes that any leakage or illegal use of such data can directly threaten an individual's dignity, personal safety, or property security. The 2020 revision of the Information Security Technology – Personal Information Security Specification also explicitly recognizes personal biometric information as sensitive personal information.

Scholars generally agree that facial information exhibits typical sensitive characteristics [6]: Privacy Concerns: Facial information contains a wealth of personal privacy, including physical features, health status, age, and ethnicity. Disclosure of such information leads to exposure of personal privacy. Link to Key Rights: Facial information is often associated with financial accounts, movement trajectories, and other critical rights. If misused, it may directly threaten an individual's property safety. The Hangzhou "First Facial Recognition Case" confirms the sensitive nature of facial information: although the court did not find actual damage, it clearly noted that once facial information is leaked, remedies are difficult, fully aligning with the Personal Information Protection Law's definition of sensitive information as that which "can easily endanger personal or property safety." Therefore, due to its inherent characteristics, facial information is indisputably classified as sensitive information.

2.2. Biometric information

The Personal Information Protection Law explicitly recognizes facial information as a typical biometric feature. Article 28 defines biometric information as "information based on physiological characteristics of the human body" that "can identify a specific natural person either alone or in combination with other information."

The uniqueness of facial information is manifested in three aspects: Uniqueness: Facial features have a one-to-one correspondence with natural persons. Immutability: Current technology cannot

DOI: 10.54254/2753-7048/2025.28039

alter inherent physiological features. Direct Identifiability: Identity can be verified without combining other information. These characteristics distinguish facial information from general personal information, necessitating specific legal regulation [7]. From a normative perspective, current law provides multiple layers of protection: The Civil Code's section on personality rights includes identifiable external appearances within the scope of portrait rights while classifying atypical facial feature information under privacy rights or general personal information protection. The Interpretation by the Supreme People's Court and Supreme People's Procuratorate on Several Issues Concerning the Application of Law in Handling Criminal Cases of Infringement of Citizens' Personal Information lists categories of personal information. Although "facial information" is not explicitly mentioned, it is encompassed under personal information through the criterion of identifiability.

2.3. Personality interest attribute

Due to its unique biometric characteristics, facial information serves as a core carrier of personal dignity, possessing personality interest attributes [8]. This is reflected in three aspects: Core Value of Personal Dignity: Facial information, as a directly identifiable biometric feature, involves portrait rights, privacy rights, and other personal rights, while also carrying the core value of personal dignity. Each individual has a unique emotional recognition of their facial image, which constitutes a foundational element of personality recognition. Judicial Reinforcement of Protection: Judicial practice strengthens the protection of facial information through typified regulations. The Supreme People's Court's Provisions on the Application of Law in Civil Cases Involving the Use of Facial Recognition Technology to Process Personal Information lists eight types of conduct that infringe upon personality rights, including processing personal information without consent, failing to ensure security, and violating the principle of proportionality. This exemplifies the close relationship between facial information and personality rights. Dual Attribute of Personality Interests: Facial information possesses both a defensive function (negative right) and a controlling function (positive right). Its dual nature provides the traditional defensive features of personality rights while reflecting the modern reality of informational self-determination.

In conclusion, facial information is not only a sensitive and biometric type of information but also embodies core personality interests. It meets the legal definition of personal information and thus falls within the scope of personal information protection.

3. Operational mechanism of facial recognition technology

Facial recognition technology, as a widely applied identification method, warrants examination not only to understand its core technical principles but also to reveal key characteristics related to personal information protection. Its operation primarily involves the full lifecycle management of information, including the creation and collection of facial information, organization and processing, storage and dissemination, and discovery and retrieval [9]. This comprehensive operational chain highlights the unique value of biometric technology in protecting personal information.

3.1. Creation and collection of facial information

The creation and collection of facial information are based on its uniqueness, immutability, and direct identifiability. The Personal Information Protection Law explicitly classifies facial information as "sensitive personal information." Collection must adhere to the principles of legality,

DOI: 10.54254/2753-7048/2025.28039

legitimacy, and necessity. Specifically, information processors are required to fulfill complete disclosure obligations, clearly explaining the purpose of collection, processing methods, and the scope of data in an understandable manner, and must obtain explicit consent from the data subject.

In practice, facial information is widely applied in residential property management, shopping malls, and mobile applications. For example, in the case of Zhang v. Jiangsu Zeyuan Property Company, the court, based on the principle of informed consent established in Article 1035 of the Civil Code, ruled that the property company could not use facial recognition as the sole authentication method and must provide alternative verification options. This judgment both protected personal information rights and illustrated the concrete application of the principle of proportionality. It is also noteworthy that Article 1034 of the Civil Code incorporates personal information rights within the scope of privacy protection. However, in practice, some enterprises rely on standardized contract clauses to force users' consent, intentionally conceal details of data usage, or set facial information collection as a default "opt-in" option. This makes it easy for the public to authorize data use unknowingly, infringing upon users' rights to informed consent and autonomous choice.

3.2. Organization and processing of facial information

The organization and processing of facial information constitute the core stage in the full lifecycle of personal information. The organization phase mainly involves two steps: first, cleaning, labeling, and linking facial information data; second, consolidating images of the same individual collected from different scenarios into a unified record, or constructing a multidimensional retrieval system by adding labels such as age and gender [10]. In the "First Facial Recognition Case," the venue associated ticket buyers' facial information with their identity and ticket purchase records, representing a typical organizational activity of facial information.

Processing refers to the deep mining of organized facial data through algorithmic models. Based on the source of input data, existing research can be divided into two categories: (1) three-dimensional facial acquisition and reconstruction in controlled environments; and (2) three-dimensional facial acquisition and reconstruction in uncontrolled environments. For instance, in applications such as emotion analysis and behavior prediction, the opacity of algorithms may generate new risks to individual rights. The fairness and transparency of these algorithms directly affect the legality and reasonableness of data processing outcomes. Some e-commerce platforms analyze users' facial images to infer consumption preferences and deliver targeted recommendations. Although personal information is not directly disclosed, this practice may exceed the reasonable expectations of data subjects, raising concerns over potential algorithmic misuse.

3.3. Storage and release of facial information

The Personal Information Protection Law defines facial information as biometric data "based on physiological characteristics of the human body" that "can identify a specific natural person either alone or in combination with other information," and sets special rules for its storage and release. Information processors are required to fulfill strict disclosure obligations and obtain personal consent.

In the storage stage, facial information exhibits both technological dependency and high-risk characteristics. On one hand, storage involves systematic technical operations such as data format conversion, security protection configuration, and lifecycle management. On the other hand, because

DOI: 10.54254/2753-7048/2025.28039

facial information is susceptible to theft, tampering, and loss, processors must bear strict responsibilities for secure custody.

In the release stage, the release of facial information is structured as a systematic process integrating mathematical tools and privacy protection techniques. This process begins with the matrix modeling of facial images [11], converting original images into two-dimensional real-number matrices to preserve spatial structural features, and applying normalization to eliminate interference factors such as lighting variations.

3.4. Discovery and acquisition of facial information

The discovery of facial information is essentially the process by which technical systems identify and locate facial features within visual data. Its core function is to isolate a particular individual's facial information from complex backgrounds, establishing the target for subsequent processing.

From a technical perspective, the discovery process involves identification and localization of facial information. Its core characteristics include: Diversity of Input Forms: This encompasses both static images and dynamic video streams [12]. Variability of Technical Approaches: Traditional computer vision algorithms perform preliminary screening by extracting features such as light and dark contrasts of facial organs [13], whereas deep learning models, by learning deep facial features, achieve higher localization accuracy even in complex scenarios involving profile views or occlusions. Legal Relevance: Improved technical precision brings previously unrecognizable or blurry faces within the processing scope, necessitating a reassessment of the boundaries of legality [14].

In the acquisition stage, the legitimacy of collection depends on justifiable grounds as stipulated in the Law on the Protection of Facial Information. In practice, different scenarios are subject to varying legal evaluation standards depending on the degree of public accessibility and the qualifications of the data subjects. It is particularly important to consider technical requirements during collection. For instance, forcibly removing a mask to capture a clear facial image may constitute excessive interference with an individual's lawful rights, highlighting the need to balance technical necessity with rights protection.

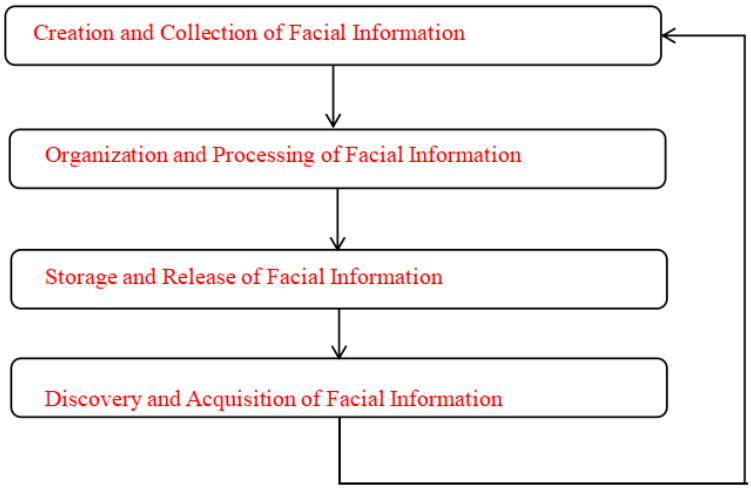

Figure 1. Lifecycle model of facial information

DOI: 10.54254/2753-7048/2025.28039

4. Impact of facial recognition technology on personal information protection

The widespread application of facial recognition technology has exerted multidimensional impacts on personal information protection, with key controversies spanning the entire process of information collection, processing, and use. On one hand, facial recognition technology provides highly efficient solutions for social governance and commercial services; on the other hand, potential rights infringements, excessive data collection, and misuse of the technology have raised significant public concern.

4.1. Legitimacy controversies in the information collection stage

The recognition of legality in the information collection stage faces multiple challenges. First, mandatory consent mechanisms can render personal information protection formalistic. In some scenarios, the collection of facial information relies on bundled authorization in standardized contract clauses. This approach has inherent flaws regarding the authenticity and voluntariness of consent, creating a tension with the legality requirements of personal information protection. Articles 9 and 10 of the Supreme People's Court Interpretation on Several Issues Concerning the Application of the General Principles of the Contract Section of the Civil Code of the People's Republic of China also address the validity of such clauses, reflecting a cautious judicial stance. Second, the consent mechanism itself has unclear boundaries, particularly regarding the distinction between implied and explicit consent [15]. In the collection of sensitive information such as facial data, the conditions and scope of implied consent lack clear legal definition, while the high standard of explicit consent, combined with technical application requirements, further complicates the assessment of legality in data collection activities.

4.2. Technical risks in information processing

The information processing stage harbors various technical risks that directly threaten the security of personal information. On one hand, due to the uniqueness and immutability of facial biometric data, such information is more vulnerable to attacks during storage, transmission, and computation. Any leakage not only infringes personal privacy but may also lead to identity theft, fraud, and other derivative security issues, resulting in irreversible harm. On the other hand, secondary misuse beyond the initial purpose underscores deficiencies in information control mechanisms. As a key tool for identifying facial information, facial recognition technology simultaneously increases the risk of misuse [16]. During "face-scanning" processes, personal users' facial details and biometric features face two typical threats: Some institutions collect and use users' facial information without explicit consent, seriously violating privacy [17]. Inadequate database security allows hackers or insiders to steal information, creating widespread social risks. For example, in June 2024, the Hangzhou Cyber Police Bureau uncovered the country's first privacy infringement case involving AI face-swapping technology. The criminal group used an overseas multimodal large model to generate live-action videos through textual prompts, bypassing platform facial authentication, acquiring a large amount of victims' personal and sensitive information, and profiting from its sale [18].

4.3. Rights infringement in the information use process

During the use of information, infringement of individual rights is also pronounced, with algorithmic discrimination being particularly notable. The algorithmic models underlying facial

DOI: 10.54254/2753-7048/2025.28039

recognition technology may, due to biases in training data or design flaws, treat individuals differently in identity verification, access control, and other processes based on specific characteristics. Such discriminatory outcomes not only violate equality rights but also pose potential threats to social fairness and justice. Furthermore, the realization of rights remedies faces significant obstacles, mainly because victims find it difficult to prove a causal link between algorithmic infringement and resulting harm. The "black box" nature of algorithmic decision-making obscures the mechanisms of infringement, breaking the causal chain and making the burden of proof in traditional tort law difficult to apply [19].

Judicial practice has already encountered related disputes. In the case of Wang v. China Railway Chengdu Group Co., Ltd., the plaintiff filed a lawsuit because the railway company failed to clearly inform passengers about face-scanning activities. The court held that the railway company's facial verification was a statutory duty based on public safety needs, which fell under circumstances where separate consent was not required; however, the duty to inform still needed to be fulfilled. This case illustrates that even when pursuing lawful objectives, information processors must still fulfill disclosure obligations.

5. Endogenous contradictions of facial recognition technology's impact on personal information protection

The impact of facial recognition technology on personal information protection exhibits inherent contradictions, primarily reflected in the formalization of the informed consent principle and the breach of the principle of data minimization.

5.1. Formalization of the informed consent principle

The principle of informed consent serves as a cornerstone of personal information protection. Its core purpose is to ensure that data subjects voluntarily and explicitly provide consent based on full knowledge, thereby providing a legal basis for the processing of personal information. This principle requires information processors to clearly and explicitly inform data subjects of the purpose, methods, scope, and potential risks of processing, while guaranteeing the right to refuse or withdraw consent [20].

However, in the context of facial recognition technology, this principle faces a serious crisis of formalization [21], manifested in several ways. First, the disclosure process often contains significant deficiencies. Information is typically presented through lengthy, ambiguous user agreements or privacy policies, making it difficult for data subjects to truly understand the consequences of processing their biometric data. Second, consent mechanisms frequently employ "bundled authorization" or default opt-in settings, effectively depriving users of meaningful choice, reducing consent to a mere procedural formality. Furthermore, when facial recognition devices are deployed in public spaces, data collection often occurs under "implied consent" or entirely without consent, leaving individuals without basic notification or the opportunity to choose [22].

5.2. Breach of the principle of data minimization

The principle of data minimization is a guideline that restricts information processing, requiring that the collection and processing of personal information be strictly limited to the minimum scope necessary to achieve a specific purpose, and that processing not exceed what is reasonably related to that purpose [23]. Article 6 of the Personal Information Protection Law further stipulates that

DOI: 10.54254/2753-7048/2025.28039

personal information collection must adhere to the minimum necessary scope for achieving the processing purpose and must not involve excessive collection.

In practice, however, facial recognition technology frequently exceeds the boundaries set by the principle of data minimization, particularly through excessive collection and processing of facial information. In shopping mall scenarios, for example, some operators deploy facial recognition systems without obtaining fully informed and explicit consent from consumers. These systems not only collect facial information necessary for the original purposes of security monitoring and foot traffic statistics but also use the data to construct consumer profiles, analyze shopping habits, preferences, and even behavior trajectories [24]. Such processing clearly goes beyond what is necessary to achieve the initial purpose. Security monitoring and foot traffic statistics require only facial information for quantity counting or verification, without correlating it with consumer behavior data or forming personalized user profiles. In essence, this practice violates the requirements of "purpose specification" and "necessity of means."

6. Response strategies for personal information protection in the application of facial recognition technology

The application of facial recognition technology presents numerous challenges for personal information protection. Effective responses should be constructed from multiple dimensions, including legal improvement, technical standards, and rights protection.

6.1. Systematic improvement of legal regulation in facial recognition technology applications

To address technical security risks, a standardized application framework for facial recognition technology should be established. On one hand, processors should be mandated to encrypt facial information during transmission and storage using nationally approved cryptographic algorithms; on the other hand, privacy-preserving technologies such as secure computing and federated learning should be actively promoted to achieve the principle of "data usable but not visible." In order to solve the problem of opaque algorithms, algorithm filing system should be used to reduce algorithmic discrimination by requiring processors to disclose the basic principles and decision-making logic of face recognition algorithms involving public interest and to accept compliance assessment by third-party organisations [25].

To resolve ambiguities in current regulatory implementation, operational standards should be further specified under the framework of the Personal Information Protection Law. First, specific operational norms for separate consent should be clarified, including clear definition of scenarios for facial information collection, prohibiting bundled authorization via standardized clauses, and requiring information processors to present processing purposes, scope, and potential risks in a clear and understandable manner to ensure authenticity and revocability of consent. Second, to effectively implement the principle of data minimization, judicial interpretations or administrative regulations should explicitly define "excessive processing" scenarios—for instance, clearly prohibiting the use of facial information in public spaces such as shopping malls for non-essential purposes like consumer profiling.

6.2. Construction of security safeguards in facial recognition technology applications

In the full lifecycle of facial information processing, any entity collecting, transmitting, or storing facial information over public networks should adopt encryption measures and fragmentary storage

DOI: 10.54254/2753-7048/2025.28039

techniques to technically reduce the risk of large-scale data leakage. At the same time, unauthorized public disclosure must be strictly prohibited, establishing a primary defense against information misuse.

To achieve system-level security, strict access control mechanisms should be established, regular security inspections of facial recognition systems should be conducted, and network security devices such as firewalls, penetration testing systems, and intrusion prevention systems should be employed to protect systems from cyberattacks. Data processing activities must strictly adhere to the principle of data minimization, with both technology providers and information processors limiting application and processing to the minimum scope required to achieve the intended purpose [26]. Where feasible, non-biometric alternatives should be prioritized to prevent excessive or misappropriated collection of facial data. Advanced encryption algorithms should be used for secure storage, and a data lifecycle management system should ensure timely deletion of unnecessary facial information, balancing technological development with privacy protection.

6.3. Optimization of rights remedy mechanisms in facial recognition technology applications

To address obstacles in rights remedies, civil litigation procedures should introduce a presumption requiring information processors to bear the burden of proof regarding the legality of their facial recognition activities, thereby balancing the parties' litigation positions [27]. Additionally, the establishment of a comprehensive public interest litigation system for personal information protection should authorize procuratorial authorities or qualified social organizations to file lawsuits against large-scale violations of facial information rights, creating a collaborative mechanism between individual rights protection and public interest enforcement [28].

To ensure accountability, a traceable system for facial information operations should be implemented, recording queries, usage, modifications, downloads, and other activities, including key elements such as the operator, time, and location. This enables post-event traceability, providing technical support for establishing liability and enforcing accountability.

Strict compensation mechanisms should also be explicitly stipulated. Regardless of the nature of the facial information user, if collected facial data is stolen, leaked, illegally used, sold, or provided to others, and causes harm to the data subject, the collector should bear joint liability for actual damages. In cases where actual loss is difficult to prove, statutory compensation standards should be established, allowing victims to claim statutory damages, even if actual losses are lower, thereby strengthening the protection of victims' rights [29].

7. Conclusion

In recent years, facial recognition technology has developed rapidly, significantly enhancing social efficiency and convenience, while simultaneously posing unprecedented challenges to personal information protection. This paper begins by examining the legal attributes of facial information, elucidating its threefold characteristics as sensitive information, biometric data, and a carrier of personal dignity and interests. It then reveals the legal disputes, technical risks, and rights infringements associated with the application of this technology. Faced with such complex challenges, a single regulatory approach is clearly insufficient. It is imperative to construct a multi-dimensional governance system that integrates legal regulation, technical safeguards, and rights remedy mechanisms. In the future, as facial recognition technology continues to advance, sustained attention should be paid to the dynamic balance between technological development and legal

DOI: 10.54254/2753-7048/2025.28039

norms. Through institutional innovation and practical exploration, it is possible to promote the coordinated progress of technological innovation and personal information protection.

References

[1] Ni, N., & Wang, M. (2022). Legal regulation of personal information protection in facial recognition technology. Renwen Magazine, (2), 121–131.
[2] Lin, L. (2021). Protection of facial recognition information from the perspective of "personality rights–usufruct rights." China Publishing, (23), 41–46.
[3] Hong, Y. (2024). Layered governance theory and institutional approaches for the application of facial recognition technology. Legal Science (Northwest University of Political Science and Law Journal), 42(1), 89–99.
[4] Shi, J. (2022). International experience and Chinese model of facial recognition governance. People's Forum, (4), 48–53.
[5] Guo, C. (2020). Governance of facial recognition technology in the era of digital human rights. Modern Law Science, 42(4), 19–36.
[6] Wang, L. (2022). Basic issues in the protection of sensitive personal information: Interpretations under the Civil Code and Personal Information Protection Law. Contemporary Law Review, 36(1), 3–14.
[7] Liu, Q. (2022). The rule of law logic of inclusive and prudent regulation in the digital economy. Law Studies, 44(4), 37–51.
[8] Shi, J., & Liu, S. (2021). Personal information protection in facial recognition technology: On the construction of dynamic consent models. Finance and Law Review, (2), 60–78.
[9] Liang, Y. (2021). Legal mechanisms for government data openness and public data governance. Jianghan Forum, (8), 127–130.
[10] Hu, X., & Li, L. (2021). Ethical risks and regulation of facial recognition technology. Journal of Xiangtan University (Philosophy and Social Sciences Edition), 45(4), 134–138.
[11] Wang, W., Zhang, Y., & Fang, F. (2006). Review of face detection and recognition technologies. Journal of Hefei University of Technology (Natural Science Edition), (2), 158–163.
[12] Song, Z., & Wang, Q. (2021). Legal issues in facial recognition data processing. Information Network Security, (S1), 82–85.
[13] Cheng, M., Yang, K., & Song, W. (2021). The paradox and unintended consequences of "precise recognition": A critical reflection on facial emotion recognition in university classrooms. Chongqing Higher Education Research, 9(6), 78–86.
[14] Zhang, X., & Wang, X. (2023). Risks and governance of facial recognition technology and applications. Studies in Science of Science, 41(3), 385–393.
[15] Tian, Y. (2018). Dilemmas and solutions of informed consent in the era of big data: The case of personal information protection in biobanks. Law and Social Development, 24(6), 111–136.
[16] Wang, Z. (2025). Rights paths and institutional choices of facial recognition in investigation. Journal of Chinese People's Public Security University (Social Science Edition), 41(2), 92–101.
[17] Zhao, J. (2022). From general rules to governance logic of face-scanning issues: Taking technological transparency as the basic stance. Northern Jurisprudence, 16(1), 5–14.
[18] Zhang, L. (2024). Sora empowers video creation: Opportunities, challenges, and prospects. Contemporary Television, (6), 4–10.
[19] Guo, J. (2025). Rule of law for inclusive and prudent regulation in digital finance. Northern Jurisprudence, 19(2), 21–38.
[20] Liu, P., & Tian, Y. (2009). Analysis of the first judicial case of human flesh search. Contemporary Law Review, 23(3), 127–131.
[21] Jia, L. (2023). Structural dilemmas and optimization paths in personal information processing rules. Study and Exploration, (6), 81–90.
[22] Dong, S., & Li, Z. (2023). On privacy concession in the post-pandemic era of big data. Qilu Journal, (4), 62–72.
[23] Jiang, H. (2020). Personal information protection under the epidemic: From the perspective of the proportionality principle. Journal of China University of Political Science and Law, (4), 183–194+209.
[24] Sun, Y. (2022). Metaverse and adjustment of legal order in intelligent society. Law Research, (2), 45–56.
[25] Li, S. (2024). Legislative responses to privacy protection in the digital era. Law, (3), 17–31.
[26] Ning, Y. (2020). Regulation of personal information protection in health code usage. Law Review, 38(6), 111–121.

DOI: 10.54254/2753-7048/2025.28039

[27] Yang, H. (2023). Normative construction of facial recognition information protection. Journal of East China University of Political Science and Law, 26(2), 68–79.
[28] Song, D., & Zhang, J. (2024). Legal regulation of facial recognition technology application under the new security framework. Science Decision, (2), 143–154.
[29] Xing, H. (2021). Protection and utilization of personal financial information in the era of big data. Eastern Jurisprudence, (1), 47–60.