Academic Journal of Management and Social Sciences
ISSN: 2958-4396 | Vol. 15, No. 2, 2026

Balancing Security and Privacy: A Legal Analysis of Biometric Data Collection in Commercial Public Spaces in China Under the 'Minimum Necessity' Principle of Personal Information Protection Law

Jiajing Wu *

Department of Law, East China Normal University, Shanghai, 200062, China
*** Corresponding author Email:** wujayne2@gmail.com

Abstract: Nowadays, the collection of biometric information in commercial public places has become increasingly common. However, the potential legality issues have raised widespread public concerns about the security of personal information. This study focuses on the common problems in the collection of biometric information in commercial public places in China, such as unclear collection purposes, overly broad collection scopes, and insufficient notifications. Based on the Personal Information Protection Law, it proposes solutions such as improving laws and regulations, strengthening supervision, and enhancing merchants' awareness of compliance, to offer theoretical support and practical guidance for the legal development of biometric information collection in commercial public places. The research results aim to provide guidance for the compliance of information collection by enterprises and ensure the security of citizens' personal information rights and interests, promoting the rule of law in the digital society.

Keywords: Public Places; Biometric Information; Legality Review; The Principle of Minimal Necessity.

1. Introduction

The principle of minimum necessity under China's Personal Information Protection Law posits that personal information, as immutable sensitive data, embodies the absolute and exclusive nature of personality rights. Consequently, the collection and utilization of biometric data must be strictly confined to the minimal scope essential for achieving specific processing purposes, prohibiting any organization or individual from engaging in excessive data collection[1]. Serving as a cornerstone of the personal information protection framework, this principle aims to balance the rights of data subjects with the interests of information processors, thereby ensuring lawful utilization and security of personal data [2]. Regarding biometric information collection in commercial public spaces, the minimum necessity principle obligates businesses to clearly define collection purposes and restrict data acquisition to what is strictly necessary for achieving stated objectives. Simultaneously, they must fulfill comprehensive notification obligations by explicitly disclosing key details including specific usage purposes, storage methods, and retention periods[1]. The applicability of this principle extends to all commercial scenarios involving biometric information, encompassing but not limited to shopping malls, supermarkets, and financial institutions, thereby establishing legal foundations and institutional safeguards for standardized biometric data collection practices[2].

2. Investigation on the Current State of Biometric Information Collection in Commercial Public Spaces

In commercial public venues such as shopping malls, supermarkets, and banks, the primary methods for collecting biometric information include facial recognition and fingerprint identification technologies. Facial recognition technology, a biometric modality that identifies individuals based on facial feature data, is extensively utilized in identity verification scenarios—for instance, authenticating customer identities during payment transactions[3]. This technology offers advantages such as contactless operation and strong user autonomy, enabling the rapid acquisition of multiple facial images within a short timeframe. Furthermore, fingerprint identification technology captures users' fingerprint data for applications like access control systems or identity verification in financial transactions, thereby ensuring security objectives[4]. The collection of such biometric data primarily serves three purposes: first, identity verification to confirm the authenticity of service recipients; second, security enhancement to prevent unauthorized access to restricted areas or illicit transactions; and third, marketing analysis, where insights derived from customer behavior data inform and optimize business strategies. Nevertheless, the frequency of biometric information collection varies across different scenarios. For instance, facial recognition in a supermarket may only be triggered during the payment process, whereas in high-risk environments such as banks, fingerprint recognition might be required for every transaction. Such high-frequency collection practices raise concerns regarding potential risks of information misuse, including, but not limited to, privacy infringements arising from non-consensual identification and potential identity replication or exploitation due to improper application[5].

3. Legitimacy Review of the Principle of Minimum Necessity from Multiple Perspectives

3.1. Legitimacy Review of Information Collection Purposes and Scope

The collection of biometric information in commercial public spaces must be justified by a legitimate purpose that is directly related to the commercial services provided. In accordance with Article 1035 of the Civil Code and Article 5 of the Personal Information Protection Law, the processing of personal information must adhere to the principles of legality, legitimacy, and necessity, and must not be conducted through misleading, fraudulent, or coercive means. In judicial practice, the principle of legality often relies on specific regulatory support, while the principle of legitimacy involves ethical and moral considerations. Together, these principles form the foundation for assessing the legality of the purpose. For instance, the application of facial recognition technology for purposes such as enhancing public security or optimizing customer experience may be deemed legitimate. However, if employed for unrelated marketing analysis or undisclosed purposes, it may constitute excessive collection[6]. Therefore, when reviewing the purpose of information collection, emphasis should be placed on whether it is directly linked to the commercial service, while excluding collection activities justified by unreasonable purposes.

Concurrently, the collection of biometric information in commercial public spaces must be strictly confined to the minimum extent necessary to achieve the intended purpose and should not exceed the bounds of minimal necessity. According to the Personal Information Protection Law and relevant judicial interpretations, personal biometric information is highly sensitive and its collection must adhere to the "minimal collection" principle—that is, only information directly relevant to a specific purpose should be collected[7]. For example, when facial recognition technology is used for identity verification in shopping malls, the information collected should be limited to facial feature data and must not include other unrelated biometric information such as fingerprints or iris data[1].Furthermore, the legality of data collection also necessitates that merchants shall not arbitrarily expand the scope of usage or utilize the information for unauthorized purposes—such as analyzing individuals' economic status, consumption capacity and preferences, personal interests, health conditions, or other objectives—during information processing. Any collection exceeding the minimum necessary threshold may constitute an infringement of users' privacy rights, thereby triggering administrative penalties under Article 68 of the Personal Information Protection Law or giving rise to civil tort claims for compensation pursuant to Article 1034 of the Civil Code[8].

3.2. Legality Review of Information Collection Notification Obligations

Commercial public establishments must fully discharge their notification obligations when collecting biometric information by explicitly disclosing to users key details regarding the purpose, methods, scope of use, and retention period of such data. According to Articles 13 and 14 of the Personal Information Protection Law, the data subject's right to informed consent constitutes a fundamental prerequisite for lawful personal information processing, wherein awareness serves as the precondition for consent, and consent represents the primary objective of such awareness [2]. Specifically, businesses shall clearly inform users in advance about the specific purposes, processing methods, and potential risks associated with information collection, while ensuring that consent is granted voluntarily[9]. For instance, conspicuous signage or written explanations should be provided to clarify the application scenarios of the technology and corresponding data protection measures. Failure to adequately fulfill these notification obligations may undermine the legal basis for information collection, thereby exposing entities to potential legal sanctions.

4. Existing Issues Regarding the Legitimacy of Biometric Information Collection in Commercial Public Spaces

In commercial settings, there is a growing trend among businesses and specific institutions to collect and utilize individuals' biometric information. In some cases, the collection practices exhibit significant deviations from the principle of data minimization, manifesting as ambiguous purposes for data collection, excessively broad scopes of information gathered, and inadequate fulfillment of disclosure obligations[10][10]. Firstly, with respect to the purpose of collection, some entities fail to clearly articulate specific objectives for gathering biometric data, or the stated purposes lack direct relevance to the commercial services provided. For instance, in the case of Shanghai Rujuan Industrial Co., Ltd. (a supermarket operator) unlawfully deploying facial recognition systems, the technology was utilized for theft prevention and customer behavior tracking—objectives that frequently exceed consumer expectations and bear no direct relationship to the services received[11]. Secondly, the problem of disproportionately wide collection scopes is particularly pronounced. Certain businesses do not strictly limit biometric data acquisition to the minimum necessary for achieving specific purposes, opting instead to collect maximal possible data, including sensitive information unrelated to commercial services. Such practices not only elevate the risk of data breaches but may also lead to further infringement of users' privacy rights[4]. Finally, insufficient disclosure represents a prevalent concern. Many businesses fail to adequately fulfill their notification obligations when collecting biometric information, neglecting to clearly inform users about key aspects such as collection purposes, methods, usage scope, and retention periods. This lack of transparency impedes users' comprehensive understanding of how their personal information will be processed, thereby undermining their rights to informed consent and autonomous choice. Collectively, these issues pose serious threats to individuals' personal information rights, potentially resulting in privacy violations, financial losses, and even psychological harm, while simultaneously exacerbating societal concerns regarding technological misuse and data security[4][11].

5. Strategies for Resolving the Legality Issues in Biometric Information Collection in Commercial Public Spaces

5.1. Refinement of Laws and Regulations

Given that the current provisions of the Personal Information Protection Law regarding the collection of biometric information in commercial public spaces remain relatively broad, it is necessary to further refine relevant clauses and clarify the implementation standards of the data minimization principle within specific contexts. For instance, differentiated scopes of information collection and usage protocols should be established for various types of commercial venues (e.g., shopping malls, banks, etc.), to ensure the legal provisions are more actionable. Concurrently, it is extremely essential to specify the legal liabilities for violations of the data minimization principle to enhance the deterrent effect of the law.

5.2. Relevant Regulatory Authorities Should Intensify Supervision Over Biometric Information Collection Activities in Commercial Public Spaces and Establish a Routine Monitoring Mechanism.

This includes not only periodic inspections to ensure that merchants' information collection practices comply with the data minimization principle but also timely investigation and sanctioning of violations. For example, monitoring the information collection process through technical means or establishing reporting channels to encourage public participation in oversight can foster a collaborative governance approach.

5.3. Enhancing Merchants' Compliance Awareness

Through initiatives such as training programs, publicity campaigns, and educational efforts, the legal awareness of operators in commercial public spaces can be effectively elevated. Specifically, merchants should be educated on the requirements of the data minimization principle as stipulated in the Personal Information Protection Law, and case studies can be utilized to illustrate the legal consequences of unlawfully collecting biometric information. Furthermore, merchants should be guided to adopt appropriate attitudes toward information collection, enabling them to fully recognize the importance of lawful practices and voluntarily comply with relevant laws and regulations.

6. Conclusion

Against the backdrop of frequent incidents of personal information leakage and misuse, the legitimacy of biometric information collection in commercial public spaces is expected to evolve toward greater standardization and legalization in the future. Firstly, in terms of technological application, the use of technologies such as facial recognition and fingerprint identification must adhere to a risk-based hierarchical management principle, clearly defining the boundaries of their application in low-, medium-, and high-risk scenarios. Secondly, with the continuous refinement of the dedicated chapter on privacy rights and personal information protection established in the Civil Code of the People's Republic of China, user rights will be further strengthened. Future regulations are also anticipated to specify protection requirements for biometric information in greater detail, ensuring its collection and use are limited to the minimum necessary scope. Furthermore, international experience indicates that legislative trends regarding biometric information collection in public spaces are progressively shifting toward comprehensive prohibition or stringent restrictions, which offers valuable insights for the legal framework improvement in related domains within China.

In summary, the legitimate and compliant development of biometric information collection in commercial public spaces necessitates not only technological standardization but also relies on the enhancement of legal frameworks and enforcement capabilities. Such efforts will guide the industry toward a healthy and sustainable future.

References

[1] Ran, K.P. (2020) On Personal Biometric Information and Its Legal Protection. Social Sciences Journal, (06): 111–120.

[2] Shang, X.X. (2021) Institutional Orientation and Norm Construction of Public and Commercial Use of Biometric Information--Concurrent Discussion on the Reflection of the Personality Right Protection Model. Qinghai Social Sciences, (02): 141–152.

[3] Zhang, J.X. (2022) On the Dual Protection of Privacy Right and Personal Information in Commercial Face Recognition. Administration and Law, (08): 78–87.

[4] Cheng, Y.Y. (2021) Legal Regulation of Face Recognition Technology in Commercial Scenarios. Journal of Hunan Radio and Television University, (03): 55–63.

[5] Gu, L.P. (2021) Identification and Replication: Privacy Protection in the Application of Intelligent Biometric Technology. Journal of Hunan Normal University (Social Sciences Edition), 50(04): 123–130. DOI:10.19503/j. cnki. 1000-2529.2021.04.015.

[6] Yang, Y.F. (2024) Tort Remedy and Protection of Facial Information in Face Recognition Scenarios. Journal of Taiyuan University of Technology (Social Sciences Edition), 42(04): 85–94.

[7] Ye, T. (2022) Interest Measurement and Type Construction of Face Recognition Technology Application in Public Places. Zhejiang Social Sciences, (07): 41–49+157.

[8] Shi, J.Y. (2022) International Experience and Chinese Model of Face Recognition Governance. People's Tribune, (04): 48–53.

[9] Gao, Y.F., Zhang, N.C. (2021) Interpretation of the Personal Information Protection Law: Enterprise Compliance Requirements and Obligation Performance. Information Security and Communications Secrecy, (11): 9–18.

[10] Ran, K.P. (2020) How to Do a Good Job in the Protection and Supervision of Personal Biometric Information. People's Tribune, (24): 121–123.

[11] Lan, S.R., Luo, J. (2022) Attribute and Protection of Personal Biometric Information in Commercial Activities. Journal of Shaanxi Normal University (Philosophy and Social Sciences Edition), 51(02): 73–86. DOI:10.15983/j.cnki.sxss.2022.0307.