Vol.6 Iss.4 2025
Modern Law Research
https://doi.org/10.37420/j.mlr.2025.030

The Current Situation and Risk Prevention of Facial Recognition Technology in China: A Legal and Governance Perspective

Lingjie Jiang*
School of Agricultural Economics and Rural Development, Renmin University of China, Beijing 100872, China
***Corresponding author E-mail: jianglingjie1105@163.com**

Abstract
Facial recognition technology (FRT) presents profound challenges to existing social and legal frameworks. While enhancing public safety and commercial efficiency, the immutable nature of biometric data and its characteristic of non-consensual collection have raised significant concerns regarding systemic erosion of privacy. This paper argues that the current regulatory system faces multiple dilemmas: the substantive failure of the traditional "informed consent" framework when confronted with technological reality, coupled with insufficient remedies for infringement and fragmented regulatory oversight. Although China has recently established a specialized governance framework through the Personal Information Protection Law of the People's Republic of China and the Security Management Measures for the Application of Facial Recognition Technologies, achieving a sustainable balance between technological innovation and the protection of citizens' rights necessitates further systemic efforts. These include constructing a refined legislative system based on "risk-tiering and scenario-differentiation," implementing a dynamic regulatory mechanism characterized by "collaborative penetration and data-intelligent empowerment," expanding diversified rights protection channels that integrate public interest litigation with individual remedies, and fostering an industry co-governance ecosystem guided by "ethical internalization and standard leadership." This paper aims to offer a theoretically grounded framework and practical guidance for clarifying the boundaries of FRT applications and improving its systematic legal regulation, ultimately contributing to a stable and predictable governance equilibrium.

Keywords
facial recognition technology; privacy protection; legal regulation; informed consent; collaborative governance

1 Introduction

Facial recognition technology has permeated numerous daily life scenarios, from residential access control to mobile payments, becoming a hallmark of societal digital transformation [1]. The deep integration of artificial intelligence and big data has enabled FRT, as a key supporting technology, to enhance social operational efficiency while simultaneously giving rise to novel risks such as privacy leakage and data misuse. This duality

has sparked profound societal concern regarding technological ethics and legal boundaries. China's legislative and judicial bodies have responded: since the emergence of the first prominent FRT litigation, regulations including the Civil Code, the Supreme People's Court's judicial interpretations on FRT-related civil cases, and the PIPL have successively enacted, explicitly incorporating facial information into the legal protection system. However, the existing normative framework still faces challenges, including difficulties in implementing principles and insufficient operational specificity. The enactment of the Security Management Measures for the Application of Facial Recognition Technologies (hereinafter "the Measures") in 2025 marks a pivotal step towards specialized governance. Nevertheless, its effectiveness in resolving deep-seated issues like the consent dilemma under non-consensual collection and clarifying necessity boundaries in complex scenarios remains contingent upon the synergistic refinement and dynamic adaptation of the broader institutional framework [2].

Existing scholarship has largely examined specific facets of FRT, such as privacy risks or isolated regulatory approaches. A systematic integration of the "technology-law-governance" nexus and the design of collaborative institutional frameworks based on the latest regulations remain underexplored [2]. Building on this foundation, this paper moves beyond partial analysis to systematically examine the multi-dimensional legal risks triggered by FRT, focusing on the structural causes of its privacy dilemmas. Subsequently, building upon the new regulatory landscape post-Measures, it proposes an integrated legal governance framework spanning legislation, supervision, remedy, and co-governance. It seeks to contribute in three key aspects: first, by elucidating the mechanism behind the substantive failure of the "informed consent" principle in non-consensual scenarios; second, by exploring concrete pathways for graded classification and scenario-based regulation informed by the Measures and national standards; third, by constructing a quadripartite collaborative governance system involving government supervision, industry self-regulation, judicial remedy, and public participation. This paper hopes to provide theoretical and practical guidance for China in navigating a sustainable equilibrium between technological advancement and fundamental rights protection.

2 Technology Overview: Characteristics, Evolution, and Dual Effects

FRT has evolved over decades, forming a mature system from theoretical exploration to large-scale application. Its basic process involves collecting and analyzing individual facial biometric information to achieve automatic identity verification. In a narrow sense, the technology refers to specific applications that directly use facial features for identity verification (e.g., facial payment); in a broad sense, it encompasses the complete technological chain and algorithm set from image capture, preprocessing, feature extraction to comparison and decision-making, and has become a key identity recognition technology centered on human facial biometrics.

2.1 Characteristics of FRT

FRT's widespread adoption stems from key features: 1) Non-contact and Convenience: Enables remote, rapid identification. 2) Non-consensual Collection: Allows continuous identity capture without the subject's

active cooperation or knowledge. 3) Mature Hardware Foundation: Ubiquitous high-performance cameras reduce deployment costs [3]. 4) Ease of Integration and Scalability: Facilitates connection with existing systems and expanded analytical functions [4]. 5) Accelerating Standardization: National standards like GB/T 41819-2022 (Information Security Technology-Security Requirements for Face Recognition Data) are gradually formalizing data processing procedures [5].

2.2 Development History of FRT

The technology's evolution spans five stages: 1) Early Theoretical Exploration (1950s-60s): Manual geometric features, limited practicality. 2) Automation Germination (1990s): Feature-based methods achieved preliminary automation. 3) Deep Learning Breakthrough (Post-2013): Convolutional Neural Networks (CNNs) drastically improved accuracy. 4) Commercialization & Platformization (Post-2017): Lowered barriers led to rapid cross-industry penetration. 5) Governance & Standardization (Present): Concurrent advancement of innovation and compliance-driven governance.

2.3 Benefits and Inherent Risks

FRT exhibits a pronounced dual effect. Its benefits include enhanced efficiency and security in public safety, finance, healthcare, and transportation, also enabling novel business models like contactless payment. Despite these significant benefits, the widespread adoption of FRT is accompanied by inherent and pronounced risks. These risks are manifest: 1) Prominent privacy and data security risks: As immutable biometrics, facial data leakage leads to irreversible, continuous harm. 2) Insufficient Legal Regulation & Enforcement: Despite foundational laws like the Cybersecurity Law and PIPL, specialized operational details are lacking, and regulatory coordination is poor. 3) Imperfect Infringement Remedy Mechanisms: The technical concealment and specialization create high evidentiary barriers for individuals, limiting judicial remedy effectiveness. The introduction of the Measures marks a step toward refined governance in China. However, implementation challenges persist.

2.4 Technical Principles and Application Scenarios

Modern FRT centers on deep learning. Its process mainly includes: face detection and localization, liveness detection and anti-spoofing, deep feature extraction, feature comparison, and recognition decision-making. Currently, the technology is widely applied in the following scenarios: public safety and governance (e.g., security surveillance, port inspection); finance and commerce (e.g., facial payment, remote account opening); public services and transportation (e.g., transit hub access, smart community management); personal consumer electronics (e.g., device unlocking); and specific industries like education, healthcare, and entertainment.

3 Legal Risks and Institutional Dilemmas

The widespread application of FRT, while enhancing efficiency, has triggered acute legal risks and institutional dilemmas due to the profound tension between its technical attributes and existing legal-social frameworks.

3.1 Compound Infringement of Personality and Property Rights

As unique, lifelong stable, and directly identifiable biometrics, unauthorized facial data processing poses a composite threat to citizens' personal dignity and property security. Judicial practice has increasingly and clearly demonstrated the extensiveness and potential severity of such infringements.

3.1.1 Multi-dimensional Impact on Personality Rights

Regarding portrait rights, the non-consensual collection and storage of facial information essentially involve fixing and using an individual's portrait without their knowledge or consent, directly violating the exclusive right to create portraits. In practice, such behaviors—from real estate sales offices secretly capturing visitors' faces for "customer profiling" to covert recognition devices deployed in some public areas—have stripped citizens' "facial images" from their autonomous control [6]. The harm to privacy and personal information interests is deeper, linking identity, travel trajectories, and social relationships, creating a state of digital "transparency". Its leakage and misuse not only intrude upon the private sphere "that one wishes to keep from others" but also trap individuals in a state of "transparency" in the digital world. Domestically, the landmark case of Guo Bing v. Hangzhou Safari Park [7], recognized as "the first facial recognition case," and the lawsuit filed by residents of a Chongqing community against a property management company [8], both highlight how disguised coercion or non-consensual collection of facial information in consumer and residential contexts infringes upon the right to personal information self-determination.

3.1.2 Emerging Property Threats & Shifting Criminal Paradigms

FRT misuse facilitates new property crimes based on biometric impersonation, shifting from "stealing objects" to "hijacking digital identities." Attack methods have evolved from using static photos to sophisticated assaults involving dynamic videos, highly realistic 3D masks, and even deepfake technology. Cases have emerged domestically where AI face-swapping technology was used to bypass facial recognition systems for fraudulent payments or unauthorized online loans [9], while international criminal organizations have even specialized in selling facial video data to circumvent identity verification [10]. This criminal approach is more concealed, remote, and technologically advanced, making it difficult for victims to prevent attacks or provide evidence. As a result, financial losses are frequently irrecoverable, posing severe challenges to traditional frameworks of property rights protection.

3.2 Applicability Crises of Core Legal Principles

The core principles within the current legal framework for personal information protection generally face applicability crises when confronted with FRT, among which the substantial failure of the "informed consent" principle is the most typical.

3.2.1 Formalization and Circumvention of "Informed Consent"

This principle encounters three challenges in practice: i) Loss of Voluntariness due to structural coercion in the scenario. When "face scanning" becomes the only or optimal path to access services or enter premises, users are confronted with the binary dilemma of "consent or exit." ii) Technological black boxes and

non-consensual collection undermine effective “informedness.” The specialized and opaque nature of the technology makes it difficult for ordinary users to comprehend its risks, while non-consensual collection directly bypasses the possibility of prior notification. iii), the "specificity" of consent is diluted within complex backend processing chains. One-time, broad consent often fails to cover subsequent uses such as data sharing, integration, or algorithmic training, thereby deviating from the original intent of safeguarding individual autonomy.

3.2.2 Ambiguity of "Minimum Necessity" and "Purpose Limitation"

Although both PIPL and the Measures establish that personal information processing must adhere to the principles of "minimum necessity" and "explicit purpose," there is a lack of clear judicial or administrative interpretive standards for what constitutes "necessity" or whether a purpose is "explicit" in specific contexts. For instance, in commercial customer flow analysis and public security surveillance, debates often arise over whether the scope of facial information collection, storage duration, and usage methods comply with "minimum necessity," creating significant ambiguity in corporate compliance efforts and regulatory enforcement.

3.3 Erosion of Social Trust and Ethical Crises

The dual nature of technology is particularly evident in its social impact. While empowering social governance and commercial efficiency, its misuse and uncontrolled application have sparked widespread crises of social trust and ethical debates.

3.3.1 Chilling Effects & Trust Erosion

Large-scale, indiscriminate surveillance may inhibit free behavior and expression in public spaces, creating a chilling effect. For instance, the use of facial recognition systems in schools to analyze students' classroom expressions has been criticized as "emotional surveillance," distorting the trust and atmosphere of freedom essential to education [11]. Public actions such as "wearing helmets to view properties," driven by public concerns over covert identification, reflect the collapse of social trust and individual resistance triggered by technological abuse.

3.3.2 Algorithmic Discrimination & Social Equity

If the training data for facial recognition algorithms contains bias, it may lead to varying recognition accuracy across different racial, gender, and age groups. This could exacerbate existing social inequities in contexts such as security checks, recruitment, and credit assessments. The existence and harms of such algorithmic biases have been repeatedly highlighted in international academic and industry circles [12]. Moreover, the excessive integration of FRT with punitive mechanisms like social credit systems may give rise to a new form of digital social control based on biometrics, raising profound ethical concerns.

3.3.3 Global regulatory reflection and public backlash

International scrutiny of FRT is deepening. The European Data Protection Board (EDPB) has explicit-

ly stated that remote biometric identification in public spaces poses a high risk to fundamental rights and should be strictly limited [13]. In the United States, cities such as San Francisco and Boston have legislated to prohibit municipal use of the technology, reflecting societal concerns over "surveillance capitalism" and the abuse of public power [14]. These global debates and legislative trends indicate that the application of the technology has transcended its role as a mere efficiency tool, touching upon core public values such as freedom, anonymity, and social equity.

4 The Generative Mechanism and Structural Causes of the Privacy Dilemma

The compound infringements and principle crises described above stem from deeper structural causes analyzed below.

4.1 Legal System Lag and the "Hard Law-Soft Standard" Gap

China's legal regulatory system has demonstrated an evolutionary trajectory from "principles subsumption" to "specialized governance" when responding to disruptive technological challenges. However, its inherent lag and ambiguity constitute the institutional soil for the dilemma.

The evolution and gaps from "homogeneous protection" to "specialized regulation": Prior to the enactment of the PIPL, the Civil Code and the Cybersecurity Law failed to provide special protection for biometric information distinct from general personal information, resulting in a problem of "homogenized protection" where the level of protection did not match the level of risk. Although the introduction of the PIPL and subsequent Measures established a specialized governance framework—explicitly classifying facial information as sensitive personal information and introducing innovative rules such as "separate consent" and "non-exclusive verification"—gaps remain in the transformation of principled provisions into specific operational rules [15]. For example, there is a lack of authoritative, unified interpretation on how to achieve "separate consent" in public, non-consensual collection scenarios and what constitutes the specific criteria for "minimum necessity." This leaves vast ambiguity for corporate compliance and regulatory enforcement.

The "disconnect between hard law and soft standards" in linking legal norms with technical standards: The current governance model attempts to establish a synergistic system where "laws set the framework, and standards set the details." However, the technical standards like GB/T 41819-2022 are recommendatory ("soft standards"), lacking direct legal force unless referenced by higher law ("hard law"). Non-compliance with this standard by enterprises does not directly constitute a legal violation unless explicitly referenced by higher-level laws. This leads to a potential disconnect between technical compliance and legal compliance, creating a linkage dilemma characterized by a disjunction between hard law and soft standards. Consequently, refined security technical requirements may be weakened or circumvented in practice.

4.2 Technological Deconstruction of Traditional Legal Principles

Beyond the institutional gaps described above, the very technological attributes of FRT deconstruct the foundational assumptions of traditional legal principles for personal information protection.

Physical Bypass of "Informed Consent" by Non-consensual Collection: The traditional "informed consent" principle is premised on the existence of interaction between the information processor and the data subject, where notification is possible. However, the "non-consensual collection" feature of FRT enables information gathering to occur automatically without the individual's knowledge or any interaction. This renders the legally presumed "notice-consent" procedure physically hollow. Post-hoc privacy policy notifications cannot compensate for the fundamental absence of "prior knowledge," plunging the principle into functional failure.

Structural Erosion of "Voluntariness" by Compulsory Exclusivity: In many commercial and social management scenarios, facial recognition is configured as the exclusive method for accessing services or entry. Users face a binary choice of "complete acceptance" or "total exclusion," lacking genuine alternatives. This structural coercion negates the premise of "voluntariness" in consent, reducing so-called user agreement to forced compromise within asymmetrical power or service relationships. Although the Measures stipulate the "non-exclusive verification principle," defining "reasonable alternative methods" and ensuring their availability remains a practical challenge.

Cognitive Undermining of "Rationality" by the Technical Black Box and Risks: The validity of "informed consent" implicitly assumes that users can make judgments based on reasonable understanding. However, the complexity and opacity of facial recognition algorithms (the "black box" effect), coupled with emerging attack vectors (e.g., AI face-swapping, 3D mask attacks), involve technical risks far beyond the comprehension of ordinary users. Expecting users to provide consent based on full awareness of these rapidly evolving, highly specialized technical risks is practically implausible, thereby undermining the rationality of consent [3].

4.3 Weak Implementation and Remedy Mechanisms

When preventive rules (such as informed consent) are deconstructed by technology, ex-post oversight, enforcement, and rights remedy mechanisms should sever as the last line of defense. However, the current mechanisms exhibit systemic weakness in this regard.

Fragmented Oversight and Limited Penetrative Capacity: FRT spans multiple domains, including cyberspace administration, public security, market regulation, health, and transportation, leading to a dilemma of "fragmented oversight with overlapping responsibilities." This often results in regulatory gaps or redundant enforcement. Moreover, regulatory approaches remain skewed toward ex-post penalties and document reviews, while the capacity for "penetrative oversight"—such as real-time monitoring of technical system operations, dynamic tracking of data flows, and substantive review of algorithmic logic—is still under development. This makes it difficult to effectively preempt or intervene in concealed, technologically mediated infringements [16].

The "High Cost-Low Benefit" Dilemma for Individuals: The concealment and specialization of technical processing mean that evidence of infringement is often unilaterally controlled by the information processor, placing individuals at a significant disadvantage in providing proof. Furthermore, the harm caused by a single infringement case may be dispersed and difficult to quantify. The high time, economic, and professional

knowledge costs of individual litigation often contrast with limited compensation. This severe imbalance between cost and benefit greatly discourages individuals from seeking judicial remedies, leaving many infringements outside judicial scrutiny.

Complementary Yet Limited Role of Public Interest Litigation: The introduction of the procuratorial public interest litigation system has provided a robust public remedy tool to address large-scale and technology-driven infringements [17]. However, its effectiveness is also subject to certain limitations. On one hand, the intervention of procuratorial authorities is selective and cannot cover all infringement scenarios. On the other hand, when confronting complex corporate technological architectures and data flow pathways, investigation and evidence collection still face technical expertise barriers. Public interest litigation primarily serves as a mechanism for “ex-post correction” and “exemplary deterrence,” while its role in preventive measures and routine supervision remains limited.

4.4 Conflicts in and Lessons from Global Governance Paradigms

From a global perspective, different legal jurisdictions, grounded in their distinct legal traditions and value orientations, have developed markedly divergent governance paradigms. The conflicts among these paradigms, as well as their inherent challenges, further reflect the profound complexities involved in governing FRT.

The tension between the "rights protection" and "innovation development" paradigms: The "rights protection" paradigm, exemplified by the EU's General Data Protection Regulation (GDPR) and the AI Act, adheres to the precautionary principle, grants data subjects extensive rights, and imposes strict restrictions on high-risk applications [18]. In contrast, the "innovation development" paradigm, represented by legislation in certain U.S. states (such as the Illinois Biometric Information Privacy Act, BIPA), relies more heavily on ex-post judicial remedies and substantial punitive damages to deter corporate misconduct, thereby preserving greater space for technological innovation [9, 19]. These two paradigms reflect different value trade-offs between privacy rights and innovative efficiency. China's current governance approach attempts to strike a balance between them. However, how to precisely calibrate this balance across diverse application scenarios remains an ongoing challenge.

The Clearview AI case is a prime example, as its business model—scraping facial data from the public web to build a database for law enforcement queries—poses fundamental challenges to traditional legal frameworks [20]. The company's defense, arguing that it caused no "concrete harm" to individuals and that its service holds public value, exposes the crisis of interpretative inadequacy within traditional tort and privacy law. Traditional tort and privacy laws, centered on concepts like "notice and consent" and "concrete harm," struggle to effectively regulate new AI business models based on publicly available data, aggregate analysis, and services for vaguely defined public purposes. This indicates that merely patching the existing legal framework may be insufficient, necessitating more fundamental legal rethinking.

5 Pathways for Improving the Legal Regulation in China

In the face of rapid technological iteration and the boundless penetration of application scenarios, the existing legal framework still exhibits structural shortcomings characterized by "emphasizing principles over detailed rules," "prioritizing ex-post penalties over ex-ante prevention," and "focusing on government supervision over multi-stakeholder governance." To balance the incentives for technological innovation with the protection of citizens' rights, the legal regulation of FRT in China should shift towards a systematic pathway. This pathway should be grounded in refined legislation, driven by collaborative oversight, supported by diversified remedies, and guided by the internalization of ethical principles. This section aims to address the aforementioned challenges by proposing targeted solutions.

5.1 Legislative Dimension: A "Risk-Tiering and Scenario-Differentiation" Rule System

The current principle-based framework centered on the Measures urgently needs to evolve towards more operable, scenario-specific rules. The core lies in establishing a dynamic "grading and classification" regulatory standard. In response to the aforementioned challenges of ambiguous legal principles and unclear scenario boundaries, as illustrated in Table 1, a three-tier regulatory paradigm can be constructed based on the potential impact level of application scenarios on individual rights and public interests.

Table 1: Example of Risk Tiering and Regulatory Paradigm for FRT Application Scenarios

Risk Tier	Typical Scenario Examples	Core Regulatory Principle	Key Regulatory Measure Examples
High Risk	Mass surveillance in public spaces; Social credit/law enforcement based on FRT; Emotion/behavior analysis (workplace, classroom).	Prohibited in principle, permitted only by statutory exception	Authorization by specific law (not just regulation); Mandatory algorithm safety/bias audits; Annual independent third-party audits; Full-process data logging for penetrative review.
Medium Risk	Access control/attendance in smart communities/ offices; Non-identifying customer flow statistics; Identity verification for specific public services (remote bank account opening, self-service border clearance at airports).	Strictly limited, with strengthened consent	Must provide non-biometric alternative ("non-exclusive verification"); Fulfill prominent notice & "separate consent"; Mandatory Personal Information Protection Impact Assessment (PIPIA) with filing.
Low Risk	Personal device unlocking/ login; User-authorized, controllable entertainment apps (filters).	Informed consent, data minimization	Apply standard informed consent rules; Encourage Privacy-Enhancing Technologies (e.g., on-device processing); Regulatory focus on spot checks & ex-post complaint handling.

The key to this tiered framework lies in establishing a dynamic adjustment mechanism. Regulatory authorities should periodically assess and update scenario classifications. Furthermore, accountability mechanisms must run through the entire data lifecycle, clarifying the joint liability of algorithm designers, system integrators, and operators, while reinforcing the "data controller's" burden of proactive proof.

5.2 Regulatory Dimension: A "Collaborative Penetration and Data-Intelligent Empowerment" Mechanism

Effective oversight is crucial for translating legal text into practice. Firstly, a collaborative regulatory structure with clearly defined authorities and responsibilities must be established. Given the cross-domain and inter-departmental nature of FRT, it is recommended to set up a collaborative governance mechanism at the central level. This mechanism would be led by the Cyberspace Administration of China and involve the Ministry of Public Security, the State Administration for Market Regulation, and relevant industry regulators. Its responsibilities would include top-level design, policy coordination, and adjudication of major disputes, supported by a standing office to manage inter-departmental coordination and address the challenges of fragmented oversight [16].

Secondly, regulatory tools must be innovated to implement risk-based, collaborative and penetrative oversight. At the technical level, an algorithm registration and audit system should be promoted. At the data level, regulators should actively leverage regulatory technology (RegTech) to dynamically monitor data flows in key venues and verify compliance with principles such as "data minimization." At the behavioral level, conclusions from "Personal Information Protection Impact Assessments" should serve as a core basis for administrative approvals and inspections. Compliance records should be integrated into corporate credit systems to enable differentiated supervision.

Finally, the disclosure of regulatory information and the normalization of public supervision should be advanced. Regular publication of regulatory white papers, typical cases, and lists of violations should be institutionalized. Exploratory measures could allow certified public interest organizations, under compliance frameworks and with appropriate de-identification, to access specific datasets for public oversight. This would foster a synergistic force combining administrative regulation and societal co-governance.

5.3 Governance Dimension: An "Ethical Internalization and Standard Leadership" Ecosystem

External legal constraints must integrate with internal industry drivers to cultivate a healthy and sustainable technology development ecosystem. First, the normative and supervisory functions of industry self-regulatory organizations should be deepened. They should be guided to develop group standards and technical ethics covenants that are stricter than national standards, and to establish a unified platform for registering and disclosing information processing activities, thereby enhancing industry transparency.

Second, enterprises should be encouraged to deeply integrate privacy protection and ethical principles into their organizational culture and product lifecycle. This includes promoting the establishment of Chief Privacy Officer positions, incorporating data protection performance into executive evaluations, and regularly publishing transparency reports.

Finally, strengthening public digital literacy and risk awareness education forms the foundation of collaborative governance. Governments, schools, media, and social organizations should collaborate on public awareness campaigns to improve citizens' understanding of technological risks and their own rights, fostering broad societal oversight to curb technology misuse [21].

5.4 Remedy Dimension: A "Diversified, Accessible, and Effective Deterrence" Network

As the legal maxim states, a right without remedy is no right at all. The effectiveness of public remedies through administrative supervision and public interest litigation must be strengthened. Regulatory authorities should conduct proactive inspections and enforce laws strictly, utilizing measures such as substantial fines and orders to suspend operations. Simultaneously, procuratorial public interest litigation should be fully activated, and exploration into allowing consumer organizations to initiate civil public interest lawsuits should be considered.

Second, civil litigation rules should be optimized to genuinely lower the threshold for individual rights protection. Introducing punitive damages in the field of biometric information infringement could be explored. During litigation, the inversion of the burden of proof regarding the legality of processing activities should apply, placing the primary burden of proof on the information processor. The proactive exploration of behavioral injunction systems is also necessary to prevent ongoing harm during legal proceedings.

Finally, efficient and low-cost alternative dispute resolution mechanisms should be streamlined. This includes encouraging industry associations to establish internal mediation platforms and promoting the setup of independent third-party arbitration bodies comprising legal and technical experts to provide more flexible dispute resolution options.

6 Conclusion

The governance of FRT exemplifies the persistent tension between technological advancement and the protection of fundamental rights in the digital age. The implementation of the Security Management Measures for the Application of Facial Recognition Technologies in 2025 marks a crucial step in China's regulatory approach, transitioning from principle-based subsumption toward specialized governance. However, whether these measures can effectively address the consent dilemma inherent in "unperceived collection" and clarify the boundaries of necessity within complex scenarios still depends on the synergistic refinement and dynamic adaptation of the institutional framework. This paper argues that the fundamental solution lies in promoting a systemic transformation of the governance model: shifting from "one-size-fits-all" control toward precision regulation based on "risk-tiering and scenario-differentiation," and moving from government-dominated oversight toward a multi-stakeholder collaborative governance framework characterized by "legislative boundary-setting, penetrative supervision, judicial safeguarding, industry self-regulation, and public oversight." In the future, only through continuous refinement of rules, enhancement of regulatory capacity, and the active participation of diverse stakeholders can a stable and predictable legal equilibrium be constructed, one that both encourages technological innovation and firmly upholds the baseline protection of rights.

Reference

[1] ZHANG Lianhan. Characteristics and Application Risks of Facial Recognition Evidence Materials in Criminal Litigation[J]. Faxue Yanjiu, 2025(2): 82-95. (In Chinese)
[2] BAI Wen-yu, JI Yan-tao. Research on Legal Issues of Facial Recognition Technology under the Trend of Datafied Privacy[J]. Dangdai Jingji, 2023(5): 123-129. (In Chinese)
[3] WEI Han-tao. Top-Level Design of Criminal Law Regulation on Misuse of Facial Recognition Technology[J]. Dangdai Faxue, 2024, 38(2): 3-15. (In Chinese)
[4] MA Teng-fei, FENG Xiao-qing. Research on Legal Regulation of Facial Recognition under the Background of Government Data Opening[J]. Journal of CUPL, 2023(3): 88-102. (In Chinese)
[5] HU Xiao-meng, LI Lun. Ethical Risks of Facial Recognition Technology and Its Regulation[J]. Journal of Xiangtan University (Philosophy and Social Sciences), 2021, 45(4): 101-107. (In Chinese)
[6] Controversy over 'Imperceptible Capture' by Facial Recognition in Property Sales Offices[N]. Southern Metropolis Daily, 2020-11-23(A16). (In Chinese)
[7] Fuyang District People's Court of Hangzhou City, Zhejiang Province. (2020) Zhe 0111 Min Chu No. 6971 Civil Judgment[Z]. 2020. (In Chinese)
[8] Chongqing Court Orders Property Company to Delete Forcefully Collected Homeowners' Facial Information[N]. China Consumer News, 2021-11-10(3). (In Chinese)
[9] Anhui Police Crack First 'AI Face-Swapping' Fraud Case[EB/OL]. CCTV News Client, (2023-08-10)[2024-11-30]. https://news.cctv.com/2023/08/10/ARTIqK7X8m9Z6w3sY1QkLr7j230810.shtml
[10] INTERPOL. Global Landscape on Face Recognition Technology: 2022 Operational Report[R]. Lyon: INTERPOL, 2022.
[11] Classroom Facial Recognition Sparks Controversy: Smart Education or Student 'Surveillance'?[EB/OL]. The Paper, (2019-09-04)[2024-11-30]. https://www.thepaper.cn/newsDetail_forward_4312345
[12] Thales Group. Biometric Vulnerability Assessment: A Case Study on Face Recognition Spoofing [R/OL]. 2023[2024-11-30].
[13] European Data Protection Board. Guidelines 3/2019 on processing of personal data through video devices[Z]. 2020.
[14] San Francisco Bans Facial Recognition Technology[EB/OL]. BBC News, (2019-05-15)[2024-11-30]. https://www.bbc.com/news/technology-48276660
[15] HONG Yan-qing. Theory and Institutional Approach to Tiered Governance of Facial Recognition Technology Applications[J]. Science of Law (Journal of Northwest University of Political Science and Law), 2024, 42(1): 89-100. (In Chinese)
[16] QU Ying. Analysis on the Path to Improve Regulatory Effectiveness in the Transformation of Chinese Government Regulation[J]. Studies in Law and Business, 2018(6): 78-85. (In Chinese)
[17] LUO Xiang. On the Limits and Application of Criminal Law Regulation of Facial Recognition—Based on Guiding Cases of the Crime of Infringing on Citizens' Personal Information[J]. Journal of Comparative Law, 2023(2): 17-31. (In Chinese)
[18] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such

data, and repealing Directive 95/46/EC (General Data Protection Regulation)[Z]. Official Journal of the European Union, L 119, 4.5.2016: 1–88.
[19] In re Facebook Biometric Information Privacy Litigation, 3:15-cv-03747 (N.D. Cal. Feb. 26, 2021) (Final Approval Order).
[20] Clearview AI Is Taking Facial Recognition Privacy to the Supreme Court[EB/OL]. e-traces, (2025-02-09)[2024-11-30]. https://etraces.domainepublic.net/clearview-ai-is-taking-facial.
[21] HONG Yanqing. Public Participation in Digital Governance: A Case Study of Facial Recognition Technology[J]. Chinese Public Administration, 2024, (5): 112-120. (In Chinese)