Open Journal of Legal Science 法学, 2025, 13(9), 1999-2005
Published Online September 2025 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2025.139276

Hans汉斯

行政法视域下人脸识别技术的法律规制困境与路径优化

朱浩正

广西大学法学院，广西 南宁

收稿日期：2025年7月25日；录用日期：2025年8月5日；发布日期：2025年9月3日

摘　要

本研究旨在探讨行政法视角下人脸识别技术应用的规制困境与优化路径。通过文献分析与案例研究，系统梳理了人脸识别技术在隐私保护、人格尊严及财产权益等方面引发的侵权风险，揭示了当前行政法在信息保护范围界定、监管体系构建及救济机制完善等方面存在的不足。研究发现，现有法律体系对技术应用的特殊性考量不足，存在权益性质模糊、监管权责交叉、惩戒力度薄弱等问题。基于此，提出构建事前预防体系、健全事中监督机制及完善事后惩戒引导的三维治理框架。研究结果表明，通过明确法律边界、建立分级监管制度、强化行政问责及推动行业自律，可有效平衡技术创新与权利保障。本研究为完善人脸识别技术行政监管提供了理论支撑与实践方案，对促进数字经济时代个人信息保护与公共安全协同发展具有现实意义。

关键词

人脸识别技术，行政法，法律规制

The Legal Regulation Dilemma and Path Optimization of Facial Recognition Technology from the Perspective of Administrative Law

Haozheng Zhu

Law School of Guangxi University, Nanning Guangxi

Received: Jul. 25th, 2025; accepted: Aug. 5th, 2025; published: Sep. 3rd, 2025

文章引用: 朱浩正. 行政法视域下人脸识别技术的法律规制困境与路径优化[J]. 法学, 2025, 13(9): 1999-2005.
DOI: 10.12677/ojls.2025.139276

Abstract

This study explores the regulatory challenges posed by facial recognition technology applications through the lens of administrative law, examining risks to privacy, human dignity, and property rights. Research findings identify significant gaps in legal definitions, fragmented supervisory structures, and insufficient penalty mechanisms within current frameworks. The proposed solution establishes a comprehensive governance model featuring preventive protocols, hierarchical oversight mechanisms, and reinforced accountability measures to reconcile technological advancement with fundamental rights protection. This work develops practical policy recommendations for aligning facial recognition deployment with evolving digital legal standards, delivering actionable insights for lawmakers and regulatory bodies, achieved through identification of legislative deficiencies in existing facial recognition regulations, establishment of context-specific standards for governmental and commercial implementations, and construction of an integrated governance framework combining state administration, industry self-regulation, and judicial oversight. The methodology synthesizes doctrinal legal analysis with empirical case studies, generating findings that contribute to international discourse on digital governance while addressing ethical considerations in emerging biometric technologies.

Keywords

Facial Recognition Technology, Administrative Law, Legal Regulation

1. 引言

人脸识别技术是一种通过机器对静态或视频中的人脸图像进行特征提取和分类识别，以实现身份鉴别的生物识别技术。该技术提取面部多维信息建立识别模型，将捕获的人脸数据与数据库中的特征模板进行比对，最终完成个体身份验证或监控追踪[1]。当前中国已进入数字经济红利大规模释放的时代，人机共存与人机交互的应用范围持续扩大，因而不可避免地产生个人信息被过度采集和非法使用的显著风险。

人脸识别技术的法律规制研究一直是学术界的关注热点之一。本文选择行政法视角，必要性体现在两方面，学术层面，现有研究多集中于商业应用，忽视政府为公共管理目的收集处理信息的特殊场景；在实践层面，政府广泛应用该技术于行政许可、行政处罚及新业态监管等行政任务。法律的滞后性决定了，若不及时采取规制措施，则无法充分准确地适应复杂的社会关系。因此，在扩大人脸识别技术应用范围以提高人们生活便利性的同时，也应将其置于隐私保护视角下进行反思和审视。基于此，本文旨在分析技术应用的侵权风险，揭示行政法规制的困境，探讨信息采集利用的风险防范与责任承担。

2. 人脸识别技术的侵权风险

随着网络与计算技术的迅猛发展，人脸识别技术在提升智能服务体验、优化社会治理效率并创造显著经济效益的同时，也引发了显著的社会经济风险。这一问题的核心在于数据作为新兴生产要素，使人脸识别信息兼具人格、财产等多重属性，导致其权利界定面临严峻挑战。

在隐私与安全层面，人脸作为可识别信息的终端载体，承载着个人身份相关的多重标签属性，这些信息直接或间接反映权利义务关系，甚至涉及人格特征与行为习惯。现实中，许多商家以便利为由，通过人脸识别技术过度采集顾客信息，却未能明确告知数据处理方式及不当使用的救济措施。这种模糊的同意模式严重违背了用户协议的平等原则，加剧了个人隐私泄露的风险。

在人格尊严方面，人脸识别技术通过抓取个体生物特征，将具有独立人格与尊严的人抽象为数字符码，导致人格价值稀释与人的物化。当个体被简化为数据库中的一行行数据时，自然人面临人格权益贬损，其作为人的尊严被系统性弱化[2]。随着生物信息存储范围的扩大，这些数据可能被整合至不同数据库，用于提升识别技术的精准度，甚至沦为商业机构或政府部门侵害个体权益的工具。例如，部分企业通过拍摄顾客人脸照片进行分类分析，以优化营销策略，这种行为不仅侵犯公平交易权，更对个人尊严构成潜在风险。更恶劣的是，某些商家通过付费交换或共享人脸数据库，进一步加剧信息整合的深度，使个体陷入更严重的数字化监控与透明化困境。

在财产权益保护方面，人脸识别技术的广泛应用使其采集的生物识别信息承载着巨大的民事权益价值。一旦这些信息被滥用，其兼具的人格与财产属性可能导致难以挽回的损害。此外，技术驱动的算法监控模式取代传统人工监控后，人脸信息一旦泄露，不仅可能被用于非法交易，还会给账户安全带来重大隐患，使个体面临持久的经济损失风险。

3. 行政法在规制人脸识别技术应用的困境

人脸识别技术的应用已从身份识别升级至用户画像与实时追踪，这一升级使个人信息披露途径在某种程度上持续扩张，给个人信息保护带来新问题。当前我国对人脸信息的保护主要体现于个人信息规制之中，而对个人信息的规制主要采用特别立法与分散立法相结合的模式。然而考虑到人脸识别的特殊性，法律解释与适用面临一系列棘手问题，例如人脸识别技术侵害的权益性质模糊、危害行为难以认定、风险损害存在不确定性等。下文将探讨行政法在规制人脸识别技术时面临的困境。

3.1. 信息保护范围未清晰界定

《个人信息保护法》采用概括性立法加“列举加兜底条款”的模式，在一定程度上保证了稳定性、简明性等优势，为个人信息保护提供了较为全面、多层次且多元化的依据。例如《个人信息保护法》虽在第四章规定了个人在个人信息处理中享有的大量权利，如对个人信息的知情权与决定权、限制或拒绝他人处理个人信息的权利等。但其第 6 条确立的“最小必要”原则缺乏细化标准，导致行政机关及商业主体在处理人脸信息时，对“必要性”和“最小范围”的理解与裁量空间过大。且现阶段，《个人信息保护法》与《民法典》《刑法》等法律规范的衔接仍存在诸多问题，在可操作性方面存在不足，亟需立法部门对其相互协调与适用做出完整解释。相较于日本在个人信息保护法系列法规中采用的“基本法概括 + 配套法规(解释)列举”及“一般 + 例外”的立法模式，《个人信息保护法》部分条款对行为的认定缺乏统一标准，对不当及违法处理个人信息的行为未能全方位覆盖，为个人信息处理者从事违规操作提供了空间。再者，相关行政立法针对性及有效性不足，无法充分适用于具体应用场景。此外，《个人信息保护法》第 29 条设定了严格的“单独同意”规则，但在实际应用中，如在公共场所部署的人脸识别系统，其“无感”采集特性使得有效获取个体“单独同意”几乎不可能，引发合法性争议[3]。

3.2. 行政规范体系不健全

数据信息的流动呈现出高速化特征，这一趋势在为个人信息资源再利用提供便利的同时，也显著加剧了信息泄露风险。从规范体系的事前预防维度观察，当前数据共享机制虽提升了信息资源的流通效率，

却为持有非法意图的主体实施不法行为创造了条件。值得注意的是，个人信息披露行为呈现明显的收益与成本失衡状态——信息披露所获收益远高于所需承担的成本，这种失衡极易诱发次生犯罪行为的发生[4]。在信息收集的事中实施阶段，《个人信息保护法》第14条强调同意应基于个人自愿。然而，实践中，部分信息处理者利用技术或格式条款优势，通过预设同意选项(默认勾选)、将人脸信息采集捆绑基础服务、或使用冗长晦涩的隐私政策等方式，实质上剥夺了用户的真实选择权，违背了其对有效“同意”的核心要求。就事后追责机制而言，尽管个人信息滥用行为频发，但现行刑事处罚力度明显不足，难以形成有效震慑[5]。这种轻缓的惩戒措施不仅无法遏制违法行为的发生，反而可能助长信息处理者的侥幸心理，导致违规成本长期处于低位运行状态。

3.3. 行政监督机制发挥失灵

总体而言，我国现行行政监管体系是适应国情的较为系统的制度，具备多重行政监管主体与组织、多样行政监督方式与渠道。但在具体监管实践中，监管主体之间实则缺乏有效沟通协调配合。具体表现在，我国尚未设立专门负责人脸识别技术等数字化应用的行政监管机构。《个人信息保护法》第六章规定监管体制由国家网信部门统筹协调，实行多机构混合分头监管，即由公安机关、国家网信部门、市场监管总局等国家机构共同承担监管责任。这导致在行政监管过程中，各部门之间对接工作不通畅，存在监管责任模糊、多头执法、相互推诿、效率低下的现象。

行政机关职能与权限重叠的根本原因在于，我国行政法律法规具有显著的部门立法特征，存在委托立法与行业立法弊端。诸多行政法规仅着眼于部门自身利益与行业保护，全然忽视法律法规的整体意识与系统观念。进一步而言，各法律部门立法与修订时间不一致，立法程序常显仓促，导致构建精准高效行政监督体系所需的系统性统筹考量与必要条件缺失。同时，人脸识别技术的评估、监管、追踪及具体行政处罚方面缺乏具有实操性的规范与监督制度规定。尽管《个人信息保护法》第66条设定的罚款额度上限(五千万元以下或上年度营业额百分之五以下)以及责令暂停相关业务、吊销许可等处罚措施，虽较此前立法有所提升，但对于大型平台或造成严重后果的违法行为，其威慑力仍被质疑不足。行政监管人员在行使监管权时，只能从分散于《民法典》《刑法》《个人信息安全规范》等法律法规中的规范性文件查找适用行政法规。然此该复杂性显著提升了行政监管主体的执法成本，监管效率与效能亦因此难以保障[6]。

3.4. 行政诉讼救济渠道有待完善

在人脸识别技术应用的侵权要件中，侵害主体、归责原则、损害认定及因果关系等存在巨大理论争议，加剧了司法实践的救济难度[7]。无论选择隐私权救济途径，抑或个人信息权益救济途径，均以财产损害赔偿为主，难以切实维护信息主体权益，更遑论打击肆意侵害人脸信息的信息收集者[8]。在现有精神损害赔偿司法解释中，若精神痛苦程度仅达“一般”之非严重程度，受害者的精神损害赔偿诉求常难获法院支持。

法律实践中，人脸识别信息凭借其侵权成本低、维权成本高的特性，日益显现被广泛采集的趋势。然行政权力对非法采集、售卖与使用等违法行为的介入过于滞后，对应救济措施常待人脸识别信息受侵害后方予采取。事前与事中完善的法律监管制度及制度保障机制过少。此外，当前人脸识别案件鲜少通过行政途径解决，纵使经行政途径处理，行政机关亦难以提供完善畅通的司法救济渠道。

4. 构建人脸识别技术行政法监管路径

当前我国行政法对人脸识别技术侵权的规制体系存在明显滞后性，相关监管规范分散且缺乏精准指向，由此引发的隐私权益保障缺失、公众知情权限缩、数据掌控失衡等问题持续凸显。现有研究多聚焦

技术应用后的法律救济，对事前风险防控机制的构建尚处空白状态。基于此，在推进人脸识别技术社会化应用的过程中，亟需构建兼顾效率与安全的行政监管框架，实现技术赋能与隐私保护的动态平衡。本文从行政立法与监管实施维度，提出系统性规制路径。

4.1. 构建事前行政预防体系

构建事前行政预防体系需从法律释义、权责划分、行业准入、政府责任及技术标准五方面完善。首先应明确《个人信息保护法》核心概念的法律边界，重点界定“最小必要范围”“公共利益”等弹性条款的适用标准，防止技术滥用风险。当前法律中“最小范围”“公共利益”等概念因语义模糊易导致非法侵害行为游离于监管之外，需通过司法解释或配套法规予以明确化[9]。

其次建立分级分类监管制度。根据应用场景风险差异，划定行政机关及授权机构在技术许可、运行监管、违规惩戒等环节的权责清单。将人脸识别技术应用场景划分为“必须使用”“授权使用”“禁止使用”三类，严格限定采集行为边界。例如公共安全领域可纳入“必须使用”范畴，商业营销场景则需遵循“授权使用”原则，非必要场景应明确禁止采集行为。同时要求行政机关与授权机构在各自权限范围内履行许可审核、日常监督及违规处罚职责，构建权责明晰的监管框架[10]。

在行业准入层面，建议依据《个人信息保护法》第 52 条关于处理敏感信息需具备相应条件的规定，通过行政许可制度筛选合格市场主体，要求信息处理主体必须取得专项资质认证，并建立准入负面清单。提高非政府组织的市场准入门槛，建立多层次技术许可制度，要求从事人脸信息采集、存储、处理的机构必须获得国家相关部门颁发的资格证书，从源头阻断不合格主体进入市场。

强化政府责任需构建公民数字权利保障机制。政府部门应依据《个人信息保护法》第 51 条关于处理者安全保障义务的规定，要求行政机关带头履行高标准的保护义务，包括开展专项普法、落实全流程透明告知、定期进行安全审计等。同时要求信息处理主体在采集环节明确告知采集目的、存储期限、安全措施及救济途径等内容，保障公民的信息权、选择权、公平交易权等合法权益。在公共利益与商业利益的平衡方面，需避免过度强调公共安全而忽视个体权益，也要防止个人信息保护阻碍生物识别技术的合理应用。

技术标准制定需双轨推进。一方面加速推进强制性与推荐性国标、行标的研制，结合《个人信息保护法》第 62 条关于国家支持制定相关标准的规定，通过技术研发提升防伪鉴别能力，特别是在活体检测、数据加密存储传输、访问控制、防伪鉴别等技术要求。另一方面完善跨领域法律衔接，针对公共管理与商业应用场景建立差异化的安全管理制度。重点监管信息访问权限配置，明确不同场景下的数据留存期限、共享范围及安全防护等级、匿名化处理标准等方面。如在公共安全领域可适度放宽访问权限，但需配套严格的审计机制；商业应用场景则应严格限制数据使用范围，禁止过度采集与关联分析。

通过上述措施的系统实施，可在前端构建起覆盖法律释义、过程监管、主体准入、权利保障及技术规范的全方位预防体系。这种预防性治理模式既能为技术发展预留创新空间，又能有效防范个人信息泄露与滥用风险，实现技术赋能与权利保护的动态平衡。

4.2. 健全事中行政监督机制

应构建覆盖技术全生命周期的协同监管框架，建立政府主导、多元主体参与的监督网络，确保信息采集全程遵循用户真实意愿，并建立实时信息披露机制以防范数据窃取风险。鉴于人脸识别技术风险的长期性与复杂性，政府部门需承担引导公民关注人脸信息使用的责任，构建多层次、跨部门、全流程的行政执法协同监督体系。该体系既能高效监督政府职能履行，又能切实保障公民权益。具体措施包括：政府需第一时间核查人脸信息收集使用是否基于公民真实意愿，并即时告知身份信息使用情况，防止他

人利用时间差实施非法窃取；若发生信息泄露，政府部门应能精准打击伪造公民人脸信息的违法犯罪行为，及时惩处盗用身份信息的违法者，并为后续法律追责提供依据。

针对信息泄露事件，需建立快速响应机制，及时追溯责任主体并固定电子证据。同时应设立专职监管机构，整合网信、公安、市监等多部门职能，解决当前监管权责交叉、标准不一的治理难题。虽然我国已相继成立“国家网信办”、“国家信息中心”等国家级监管机构及“大数据应用发展管理局”等省市级监管机构，但多重行政部门监管模式仍存在权责关系交叉、模糊与空白等问题，这不仅降低政府工作效率、影响行政权威，更为不法分子利用个人信息从事违法犯罪活动提供了可乘之机，阻碍有为政府建设。因此，亟需通过立法明确行政监管主体，设立专门负责识别、评估与控制个人信息的监管机构，以弥补监管主体缺位问题，提升行政效率与社会治理水平。该监管机构应具备对开发者与处理者实施差异化、分类分级监管的能力，及时作出预警提示与风险评估；同时建立独立、高效、客观、公正、统一的政府信息公开机制与监督投诉机制，提升监管精准度与靶向性，为公民司法救济提供全方位支持[11]。

在备案审查方面，需建立双重审查标准：政府层面重点考察技术应用的合法性基础与程序合规性；商业主体层面则需验证用户权利保障机制、技术能力资质及人工审核制度的完备性。健全行政备案审查与风险评估综合体系是扭转人脸识别技术监管理念的关键，应从被动应对转向主动预防风险。从政府机构审查视角，需评估人脸识别技术应用是否符合法律规定、应用内容与程序是否合规、应用范围与方法是否与目的相符、人脸信息采集目的是否正当、采集类型与规模是否遵循“最小必要原则”；从商业实体审查视角，需确认用户知情权、同意权、选择权与正当利益追诉权是否得到保障，运营主体是否具备相应资质条件，信息企业的技术能力与管理水平是否胜任人脸数据采集处理，自动化程序是否配备有效的人工审核机制[12]。

4.3. 完善事后惩戒引导机制

当前行政救济体系在数字空间治理方面存在明显短板，亟需构建新型维权机制。现有行政救济法主要针对实体空间行政争议，对数字空间新型纠纷的规制明显滞后，其受案范围仍局限于传统行政法律行为，未能涵盖数据采集等行政事实行为。虽然《个人信息保护法》已引入公益诉讼制度，但面对日益严峻的个人信息侵权问题，仍存在救济不足的困境。为此，应建立检察机关、消费者组织与网信部门协同的立体化维权机制，通过完善行政程序规则、拓宽救济渠道、健全责任机制等方式，提升数字空间治理效能。

在行政处罚方面，应构建梯度化惩戒体系。对一般违规行为，可采取警告、罚款、数据删除等常规处罚措施；对恶意侵权主体，则需实施市场禁入、高额罚金等严厉制裁。行政机关在制定处罚标准时，应综合考量违法行为的危害程度、影响范围、企业整改情况等因素，建立科学合理的裁量基准。特别是对情节特别严重、主观恶性大、社会影响恶劣的违法行为，应处以高额罚款、列入黑名单、市场禁入等顶格处罚，形成有效震慑。

推动行业自律规范建设同样重要。建议采用“政府监管 + 行业自治”的协同治理模式，支持行业协会制定技术应用标准与伦理准则，赋予其自律审查与违规处置权限。通过政策引导，促进行业协会建立人脸识别技术使用自律规范，形成“行业引领 + 外部约束”的良性互动格局[13]。具体而言，政府部门应带头建立不规范应用惩戒机制，完善行政问责制度，同时为行业自律组织提供政策支持，赋予其事前审核与事后评估权限，从源头防范技术滥用风险。

社会监督机制的完善也不容忽视。应建立健全举报奖励制度，提升公众风险防范意识，引导信息主体通过合法途径维护权益。当前多方协同监管机制下的社会监督渠道，能够及时响应信息主体诉求，提供有效处理方案。公众在享受技术便利的同时，也应警惕个人信息泄露风险，对涉嫌违法违规行为应及

时投诉举报。通过构建政府主导、行业自律、社会监督的多元共治格局，实现对人脸识别技术应用的全方位监管。

5. 结语

数字时代的人脸识别技术犹如双刃剑，在提升社会运行效率、优化用户体验、激发创新活力的同时，也对产业安全和社会稳定构成威胁。但信息化与大数据亦可成为应对经济全球化挑战的治理工具。唯有持续完善个人信息保护行政法律体系，细化相关规定，明确各主体权利义务边界，针对不同应用场景制定差异化监管重点，才能筑牢数据安全防线，有效保障公民信息安全，推动政府权力规范高效运行，促进社会公平正义。

参考文献

[1] 朱天才, 周晓波. 基于深度学习的人脸识别方法研究综述[J]. 现代计算机, 2023, 29(17): 36-40.

[2] 马俊军, 王星宇. 人脸识别法律规范初探: 权利属性、保护基础与法律对策[J]. 特区实践与理论, 2023(3): 60-66.

[3] 陆青. 个人信息保护中“同意”规则的规范构造[J]. 武汉大学学报(哲学社会科学版), 2019, 72(5): 119-129.

[4] 李振林. 非法取得或利用人脸识别信息行为刑法规制论[J]. 苏州大学学报(哲学社会科学版), 2022, 43(1): 72-83.

[5] 陈伟, 宋坤鹏. 个人信息依托型电信诈骗犯罪联防共治模式探究——基于某省 400 份判决书的实证分析[J]. 犯罪研究, 2020(2): 43-54.

[6] 张涛. 探寻个人信息保护的风险控制路径之维[J]. 法学, 2022(6): 57-71.

[7] 程海玲. 个人信息侵权风险性损害的证成与认定[J]. 重庆大学学报(社会科学版), 2023, 29(5): 198-211.

[8] 焦艳玲. 人脸识别的侵权责任认定[J]. 中国高校社会科学, 2022(2): 117-128, 160.

[9] 杨华. 人脸识别信息保护的规范建构[J]. 华东政法大学学报, 2023, 26(2): 68-79.

[10] 刘学涛. 个人数据保护的法治难题与治理路径探析[J]. 科技与法律, 2019(2): 19-26, 35.

[11] 张涛. 人脸识别技术在政府治理中的应用风险及其法律控制[J]. 河南社会科学, 2021, 29(10): 44-55.

[12] 项定宜. 个人信息处理必要性原则的规范体系研究[J]. 北方法学, 2021, 15(5): 27-37.

[13] 刘学涛. 大数据时代个人信息的行政法保护分析: 内涵、困境与路径选择[J]. 南京邮电大学学报(社会科学版), 2018, 20(6): 23-31.