Open Journal of Legal Science 法学, 2024, 12(10), 5882-5887
Published Online October 2024 in Hans. https://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2024.1210836

Hans汉斯

人脸识别技术下个人信息法律保护探究

顾琪娇

宁波大学马克思主义学院，浙江 宁波

收稿日期：2024年8月30日；录用日期：2024年9月11日；发布日期：2024年10月11日

摘 要

人脸识别技术作为人工智能领域的重要分支，在提升社会管理效率、增强公共安全、优化用户体验等方面都展现出巨大潜力。然而，这一技术的广泛应用也引发了关于个人信息保护的法律挑战。本文针对个人隐私权受到威胁、法律法规适用范围不明确、行政监管机制不足、技术滥用蕴藏安全隐患等人脸识别技术下个人信息保护面临的法律困境，提出了解决该问题的现实路径，包括完善隐私权保护指导原则、明确法律适用范围、强化行政监管能力以及加强人脸识别行业自律，旨在帮助人脸识别技术规范发展，为有效保护个人信息权益提供理论支持与实践指导。

关键词

人脸识别技术，个人信息保护，法律保护

Exploration of the Legal Protection of Personal Information under Face Recognition Technology

Qijiao Gu

Marxism School of Ningbo University, Ningbo Zhejiang

Received: Aug. 30th, 2024; accepted: Sep. 11th, 2024; published: Oct. 11th, 2024

Abstract

As a pivotal branch of artificial intelligence, face recognition technology has demonstrated immense potential in enhancing social management efficiency, bolstering public security, and optimizing user experiences. Nonetheless, the widespread adoption of this technology has also ignited legal challenges concerning personal information protection. This paper addresses the legal dilemmas confronting personal information safeguarding under face recognition technology, including

文章引用: 顾琪娇. 人脸识别技术下个人信息法律保护探究[J]. 法学, 2024, 12(10): 5882-5887.
DOI: 10.12677/ojls.2024.1210836

threats to individual privacy rights, ambiguity in the scope of applicable laws and regulations, inadequacies in administrative oversight mechanisms, and latent security risks stemming from technology misuse. To tackle these issues, this paper proposes practical pathways, encompassing refining guiding principles for privacy protection, clarifying legal scopes of application, strengthening administrative supervision capabilities, and fostering self-regulation within the face recognition industry. These measures aim to facilitate the normative development of face recognition technology and offer theoretical underpinnings and practical guidance for effectively safeguarding personal information rights.

Keywords

Face Recognition Technology, Personal Information Protection, Legal Protection

1. 引言

近年来，随着人工智能技术的不断发展，以人脸识别技术为代表的生物识别信息技术对于人们而言已不陌生，并且已广泛渗透至社会公众日常生活的多维度空间，其应用场景呈现出日益多元化与广泛化的趋势，涵盖公共安全、城市管理、远程医疗等多个关键领域。人脸识别技术的出现大大提升了社会管理效益。然而，与此同时，人脸识别技术的广泛应用也引发了安全领域内的重大挑战，尤其是公民个人信息安全问题。现行的《个人信息保护法》《网络安全法》以及《人脸识别数据安全要求》等法律规范，虽为我国加强人脸识别应用治理、保障个人信息安全搭建起了法律屏障，但仍不够完善。如何在充分利用人脸识别技术的同时，保证公民个人信息受到法律保护，成为人工智能时代亟待解决的重大课题。

2. 人脸识别技术及其运用

2.1. 人脸识别技术的概念

“计算机人脸识别技术也就是利用计算机分析人脸图像，进而从中提取出有效的识别信息，用来‘辨认’身份的一门技术”[1]。人脸识别技术的流程可以概括为：人脸图像采集和预处理，人脸特征提取，人脸图像分类、验证及识别[2]。具体而言，进行一次人脸识别首先需要通过检测器在图像中定位人脸并采集图像；其次，对图像进行预处理，包括归一化、空间变换对齐特征点、肤色检测及背景处理等；再次，提取人脸特征，转化为稳定且具有唯一性的矢量数据；最后，将处理后的图像与数据库中的模板进行匹配，输出匹配度最高的结果作为识别结果。因此，从本质上而言，人脸识别技术就是利用计算机的高速计算能力，对数据库中储存的个人面部信息进行筛选比对，进而进行身份确认或查找的一种技术。

2.2. 人脸识别技术的运用优势

1) 高效性：人脸识别技术的高效性主要体现在并行数据采集的高效性以及信息处理与匹配的高效性两方面。在并行数据采集方面，人脸识别系统能够在其监测范围内，同时捕获并处理多个独立主体的面部图像与面部特征。这种并行数据采集的能力显著提高了数据采集的效率，使得系统能够在短时间内收集到大量人脸数据，为后续的识别与验证工作奠定了坚实的基础。随着人脸识别算法的不断发展与优化，系统对采集到的面部图像进行特征提取、比对和识别的速度越来越快。利用终端摄像技术，在极短的时

间内完成复杂的面部特征分析与匹配过程，从而实现身份认证的即时性。用户只需简单配合(如眨眼、转头等)，系统就能在几秒内完成身份验证，从而大幅度提高核验效率，节省数据采集时间。

2) 非接触性：与其他传统生物识别技术相比，人脸识别技术最大的优势就在于用户无需直接与识别对象进行物理接触，只要信息主体的面部未被大幅度遮挡，人脸识别设备就能实现远距离的信息采集。这样不仅极大地缩减了人工参与，提升了使用的便捷性与安全性，还优化了用户体验，并有效促进了社会管理效益的增强。人脸识别技术的应用也标志着生物识别领域向更加高效、安全、便捷的方向迈进。

3) 应用领域广泛性：在安全领域，它成为安防监控和门禁系统的得力助手，通过实时人脸比对和识别，显著提升了公共场所和特定区域的安全保障能力；金融服务方面，人脸识别技术能够有效确保用户身份的真实性与可靠性，大幅提升了支付系统和金融认证的便捷性与安全性；此外，智能设备尤其是智能手机，将人脸识别作为标配功能，为用户带来前所未有的便捷体验；公共交通领域也借助人脸识别技术优化了票务查验和乘客追踪流程，提高了运营效率；人脸识别还渗透至社交网络，用于身份验证和个性化服务推荐，为促进社会进步、提升生活质量方面发挥了不可替代的作用。

3. 人脸识别技术下个人信息保护的法律困境

3.1. 个人隐私权受到威胁

隐私权是自然人享有的基本权利之一，根据《中华人民共和国民法典》等相关法律规定，隐私权具有不可侵犯性，任何组织或个人不得以刺探、侵扰、泄露、公开等方式侵害他人的隐私权。人脸识别技术采取的人脸信息是具备唯一性的个人生物识别信息，在大数据驱动下，人脸识别技术不仅能用来识别个人身份，还能进一步追踪个人日常活动轨迹、进行亲属关系匹配，对特定人经常接触人员进行匹配等。通过对这些数据进行收集、处理和分析，可以建构出精准的个人综合行为档案，数据控制者能精准地“阅读”并掌控人们的行为，从而对公民的隐私权造成极大冲击[3]。例如，在公共场所，部分商家或机构有可能在未经用户明确同意的情况下，擅自收集、存储和使用人脸信息，导致个人隐私权的侵犯。此外，一些人脸识别系统还可能被黑客攻击，进一步加剧了隐私泄露的风险。个人面部信息的使用渐渐偏离了最初的收集目的，公民对于自己的面部信息被如何收集和使用缺乏必要的知情权和控制权。

3.2. 法律法规适用范围不明确

首先，对于“人脸识别信息”这一关键概念，目前法律上并没有统一的界定。人脸识别信息作为人脸信息的子类概念，其具体的法律性质、范围和边界尚不明确。这种概念上的模糊性不仅给法律适用带来困难，也增加了技术滥用和侵权的风险。其次，当前的法律体系并未对人脸识别技术的应用场景、数据处理方式以及应用限制进行明确的定义。由于人脸识别技术跨越了众多领域，从安防、金融到零售和教育等，其应用范围广泛且多样，但现有的法律规定往往无法涵盖所有可能的应用场景，这种不具体的法律指导使得在实际应用中出现了诸多灰色地带[4]。尽管《民法典》《网络安全法》《个人信息保护法》等法律以及相关的司法解释中包含了与个人信息保护相关的条款，但这些条款大多较为原则性、概括性，且分散于不同的法律文件中，缺乏针对人脸识别技术的具体规定。这种立法现状导致在实际应用中，对于人脸识别技术的监管和执法存在较大的自由裁量空间，难以形成统一、明确的法律适用标准。最后，对于人脸识别技术的违法行为，目前法律上缺乏明确的责任规定。一方面，对于违法采集、使用人脸识别信息的行为，如何界定其违法性、如何确定责任主体和责任范围等问题尚待明确；另一方面，对于因人脸识别技术滥用导致的侵权行为，如何确定赔偿责任、如何保障受害人的合法权益等问题也缺乏具体的法律依据。这种责任上的不明确不仅使得受害人难以获得有效的法律救济，也降低了违法者的违法成本。

3.3. 行政监管机制不足

随着人脸识别技术的广泛应用和快速发展，行政监管的重要性日益凸显。然而，当前的行政监管机制存在滞后性，难以适应技术发展的需求。首先，监管手段单一。多数案件为“责令改正”和“罚款”的形式，而“警告”的方式占比较低。整体的行政监管机制体现为处罚性监管机制，对于事前监管机制以及事中监管机制并未覆盖提及，行政监管机制效用尚有不足，难以有效应对人脸识别技术的隐蔽性和复杂性([5]: p. 121)。

其次，监管体系不完善。缺乏跨部门、跨领域的协同监管机制，导致监管合力不足，难以形成有效的监管网络。目前，我国人脸识别应用监管立法层级多呈现“地方先行、软法治理”的特点，监管规范多为地方性法规、部门规章甚至各类通知、通告、政策等规范性文件，位阶低、法律效力不足，难以全面覆盖人脸识别技术的各个环节和场景，导致监管空白和漏洞较多。个人信息保护工作和相关监督管理工作主要由国家网信部门统筹，工信、商务等有关部门共同实施，监管的分散导致各部门权责不明[6]。

3.4. 技术滥用蕴藏安全隐患

目前，人脸识别技术被广泛应用于公共安全、场所进出、信息处理等多重领域，人脸识别技术的滥用也给社会和个人来了种种安全隐患。部分企业或个人在数据存储安全、访问控制、加密措施等方面存在明显不足，导致数据泄露风险增加。同时，人脸识别技术运用主体的技术条件和管理水平良莠不齐，让一些不法分子有机可乘，他们往往开发黑客工具来绕过、干扰或攻击人脸识别技术背后的系统和算法，进而引发盗窃、诈骗、侵入住宅等下游犯罪违法行为，危及被害人的数据安全、财产安全乃至人身安全，进一步加剧了个人信息保护的法律困境。此外，随着生成式人工智能的突破性发展，“深度伪造”等不法技术的出现，使得身份冒用和欺诈行为的风险显著增加，从而不仅危及公民的人身和财产安全，甚至会影响社会公共秩序。

4. 完善人脸识别技术下个人信息保护的现实路径

4.1. 完善隐私权保护指导原则

在人脸识别技术迅猛发展的背景下，许多场景中人脸识别成为了核验身份的唯一方式，公众只能被动接受而别无选择，公民隐私权多方面曝光于众，因此，隐私权保护原则亟待完善[7]。这不仅是对个人基本权利的尊重，也是技术伦理与社会责任的体现。因此，必须明确一系列隐私权保护的核心原则：首先，确立并强化“知情同意原则”，即任何个人信息的收集、使用都需建立在个体充分知情并自愿同意的基础上，避免信息的不当获取与滥用；其次，坚持“最小必要原则”，即仅收集与处理实现特定、合法目的所必需的最少信息，减少数据冗余与泄露风险；再者，严格遵守“专采专用原则”，即确保个人数据的使用不偏离初始声明的合法目的，维护数据的合法性与正当性；最后，强化“数据安全原则”，即采取先进的技术与管理措施，确保个人数据在收集、存储、传输、处理及销毁等各个环节中的安全无虞，防止数据泄露、篡改或非法访问。这些原则的完善与落实，能够更好保护个人隐私权，促进与规范人脸识别技术的健康发展。

4.2. 明确法律适用范围

在当前人脸识别技术广泛应用的时代背景下，针对个人信息保护面临的严峻挑战，法律体系亟需迅速响应。第一，法律应尽快明确界定人脸识别技术的使用场景、数据处理方式及个人信息保护的具体要求，确保法律规范的针对性和有效性。比如在公共安全、金融支付等必要且合理的场景使用人脸识别技术的同时，严格限制其在非必要、侵犯隐私的场合的应用。第二，为确保法律适用的全面性和公正性，

必须明确法律的时间效力，即何时开始实施及是否溯及既往；空间效力，即法律适用的地域范围；以及对人的效力，即哪些主体需受法律约束。消除法律适用的模糊地带，确保个人信息得到法律保障。最后，加强法律解释工作。通过司法解释、指导性案例等方式，对人脸识别技术相关的法律条款进行细化与明确，为司法实践提供具体指导，减少法律适用的不确定性和争议，为人脸识别技术下个人信息的保护提供清晰的法律边界和依据。

4.3. 强化行政监管能力

“技术本身是双向的，监管也是双向的，从监管技术向技术监管转变，不仅是监管理念的深刻变化，更是国家治理体系和治理能力现代化的需要”([5]: p. 129)。强化行政监管能力是保护人脸识别技术下个人信息的有力保障和支持，这要求行政机关在立法与执法层面构建一套全面、高效的监管体系，以应对人脸识别技术带来的隐私侵犯和数据安全风险。首先，强化行政监管机构的职责与能力。成立专门的监管机构或部门，负责对人脸识别技术的全链条监管，包括技术应用的审批、事中事后的监督检查以及违法行为的查处。这些机构应具备专业的技术能力和丰富的执法经验，以有效应对技术更新带来的监管挑战。其次，建立健全有效的监管机制。实施人脸识别技术备案审查制度，要求企业在使用前向监管部门提交详细的技术方案和数据保护计划，经审查合格后方可投入使用。在行政监管过程中，运用大数据、人工智能等现代技术手段，对人脸信息处理活动进行实时监控和风险评估，及时发现并纠正违规行为。此外，还应完善信息安全应急响应机制，一旦发生数据泄露或滥用事件，能够迅速响应并采取有效措施加以处理。最后，要加强行政监管的透明度和公众参与度。建立信息公开制度，定期发布监管报告和典型案例，确保监管工作的有效性和公正性，提高公众对人脸识别技术监管的认知度和信任度。同时，畅通投诉举报渠道，鼓励公众积极参与到监管过程中来，形成社会共治的良好局面。

4.4. 加强人脸识别行业自律

除了以上途径之外，加强人脸识别行业自律对于个人信息的法律保护也具有重要意义，有助于构建健康、可持续的行业生态。第一，需推动建立行业自律组织，作为行业内部自我监管、自我约束的平台。这些组织应制定行业规范、行为准则和伦理标准，明确企业在收集、使用、存储和传输人脸信息时应遵循的原则和底线，确保技术应用不侵犯用户隐私、不损害公共利益。第二，强化行业自律监督与惩罚机制。自律组织应设立独立的监督机构，对成员企业的行为进行定期检查和评估，对违反行业规范的行为进行公开曝光、警告乃至剔除出组织等惩罚措施。同时，鼓励企业之间建立相互监督机制，共同维护行业秩序和良好形象。最后，加强行业自律教育与培训，提升对公民个人信息保护的主动性、自觉性。通过组织专题研讨会、培训班、讲座等形式，提升行业从业人员对个人信息保护的认识和重视程度，增强他们的法律意识和职业道德水平。

5. 结语

人脸识别技术的快速发展无疑为现代社会带来了前所未有的便利与效率，但其对公民个人信息的潜在威胁亦不容忽视。面对这一技术双刃剑，法律与政策的及时跟进显得尤为关键。对此，面对人脸识别技术下个人信息保护的法律困境，需要进一步完善隐私权保护指导原则，明确法律适用范围，强化行政监管能力以及加强人脸识别行业自律。让人脸识别技术在法治轨道上健康、有序地发展，构建一个既促进技术创新又保障个人信息安全的和谐生态。

参考文献

[1] 张翠平, 苏光大. 人脸识别技术综述[J]. 中国图象图形学报, 2000, 5(11): 885-894.

[2] 邢会强. 人脸识别的法律规制[J]. 比较法研究, 2020(5): 51-63.

[3] 贾萨诺夫. 发明的伦理: 技术与人类未来[M]. 尚智丛, 田喜腾, 田甲乐, 译. 北京: 中国人民大学出版社, 2018: 104-109.

[4] 梁逸兰. 基于人脸识别技术的公民个人信息法律保护探究[J]. 西部学刊, 2024(12): 92-95.

[5] 倪楠, 王敏. 人脸识别技术中个人信息保护的法律规制[J]. 人文杂志, 2022(2): 121-131.

[6] 于品显, 韩雨欣. 人脸识别个人信息保护法律问题研究[J]. 唐山师范学院学报, 2024, 46(2): 122-126.

[7] 马腾飞, 冯晓青. 政府数据开放背景下人脸识别法律规制研究[J]. 中国政法大学学报, 2023(3): 180-191.