

人脸识别信息刑法规制的困境与出路

朱安娜, 吴 若

西南民族大学法学院, 四川 成都

收稿日期: 2026年6月28日; 录用日期: 2026年7月29日; 发布日期: 2026年8月10日

摘 要

数字时代下, 人脸识别技术广泛普及, 但其依托的人脸生物识别信息滥用、泄露、非法交易等违法犯罪问题日益突出, 传统法律规制体系的短板持续凸显。人脸信息具备唯一性、不可更改性与终身关联性的特殊属性, 属于高度敏感个人信息, 一旦被非法利用会造成不可逆的法益损害。最高人民法院指导性案例192号明确了人脸信息的刑法属性, 填补了司法认定空白, 但当前我国人脸信息刑法规制仍存在诸多现实困境。本文以该指导性案例为核心依托, 结合司法实践典型案例, 引入风险社会理论与域外规制经验, 采用“提出问题 - 分析问题 - 解决问题”的逻辑框架, 系统梳理人脸识别信息刑法规制的现实难题, 深入剖析困境产生的法理与实践成因, 最终构建适配人脸识别技术特性的刑法规制完善路径, 兼顾公民个人信息权益保障、网络秩序维护与数字技术良性发展。

关键词

人脸识别信息, 刑法规制, 侵犯公民个人信息罪, 司法适用

The Dilemma and Solutions of Criminal Law Regulation on Face Recognition Information

Anna Zhu, Ruo Wu

Law School of Southwest Minzu University, Chengdu Sichuan

Received: June 28, 2026; accepted: July 29, 2026; published: August 10, 2026

Abstract

In the digital era, face recognition technology has gained extensive popularity. Nevertheless, illegal and criminal acts including abuse, leakage and illicit trading of facial biometric information that underpins such technology have become increasingly prominent, and the deficiencies of the traditional legal regulation system keep coming to the fore. Featured by uniqueness, immutability and lifelong relevance, facial information falls into the category of highly sensitive personal information,

and its illegal utilization will inflict irreversible damage to legal interests. Guiding Case No. 192 promulgated by the Supreme People's Court defines the criminal law nature of facial information and fills the gap in judicial adjudication. However, the criminal law regulation of facial information in China still faces multiple practical dilemmas at this stage. Taking this guiding case as the core foundation, combined with typical judicial practice cases, this paper introduces the risk society theory and extraterritorial regulatory experience, and unfolds its research following the logic of "problem raising, problem analysis, problem solving". It systematically sorts out practical difficulties and probes into the underlying causes, and finally constructs an optimized path of criminal law regulation tailored to the characteristics of face recognition technology, so as to strike a balance among the protection of citizens' personal information rights and interests, the maintenance of network order and the sound development of digital technology.

Keywords

Face Recognition Information, Criminal Law Regulation, Crime of Infringing Citizens' Personal Information, Judicial Application

Copyright © 2026 by author(s) and Hans Publishers Inc.

This work is licensed under the Creative Commons Attribution International License (CC BY 4.0).

<http://creativecommons.org/licenses/by/4.0/>



Open Access

1. 人脸识别信息刑法规制的现实困境

随着大数据、人工智能技术的迭代升级,人脸识别技术凭借精准高效、便捷适配的特点,全面渗透到民生支付、门禁安防、政务服务、网络登录等各类社会场景,成为数字社会智能化建设的核心支撑技术。技术赋能社会治理与便民服务的同时,也催生了完整的人脸信息黑色产业链,非法窃取、贩卖、滥用人脸信息的犯罪行为频发,不仅严重侵害公民人格尊严、人身与财产安全,更极大地扰乱了数字网络空间的秩序稳定。与姓名、手机号、居住地址等普通个人信息不同,人脸识别信息属于核心生物识别信息^[1],具备终身稳定、不可篡改、唯一识别的特殊属性,无需依托其他辅助信息即可精准定位特定自然人,一旦泄露或被非法利用,将产生长期、不可逆的损害,法益侵害风险远高于普通个人信息,亟须刑法提供特殊、严苛的兜底保护。

目前我国已构建起《中华人民共和国民法典》《中华人民共和国个人信息保护法》《中华人民共和国网络安全法》等前置民事、行政法律与《中华人民共和国刑法》(以下简称《刑法》)协同保护的个人信息保护体系,形成了层级递进的规制框架。但在司法实践中,人脸识别信息的刑事司法保护仍存在明显短板,规制漏洞与裁判乱象尚未彻底解决。此前刑法理论与司法实践长期存在认知分歧,部分观点以刑法条文未单独列明人脸识别信息为由,否定其属于侵犯公民个人信息罪的规制范畴,导致刑法对人脸信息的保护力度远滞后于前置法,法律体系衔接不畅。最高人民法院发布的指导性案例 192 号,正式明确人脸识别信息,包含原始采集信息与 3D 人脸模型等衍生信息,属于刑法意义上的公民个人信息,统一了人脸信息刑法属性的认定标准,为司法裁判提供了核心指引¹。但该案例仅解决了基础属性认定问题,并未彻底化解司法实践中的各类争议。

结合近年司法判例来看,人脸识别信息刑法规制的实践困境愈发凸显。以内蒙古乌兰浩特市法院审理的陈某虎、杨某侵犯公民个人信息案为例,二被告人利用通信行业工作与代理权限,非法获取 588 套

¹参见最高人民法院指导性案例 192 号:李开祥侵犯公民个人信息案,法〔2022〕177 号。

包含人像照片、身份证信息的完整人脸数据, 违规用于电话卡实名认证, 为境外电信诈骗团伙提供技术支撑, 最终因行为人主观明知信息用于违法犯罪, 被直接认定为“情节严重”并定罪量刑^[2]。该案例充分暴露了当前规制体系的核心问题: 《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》²(以下简称《个人信息刑事解释》)基于普通个人信息设置的入罪标准, 与人脸信息的高敏感属性严重不匹配, 常规数量入罪门槛过高, 仅能依托“明知用于犯罪仍提供信息”的特殊条款定罪, 无法规制单纯非法获取、储存人脸信息的高危行为。与此同时, 司法实践中还存在非法获取行为边界模糊、关联罪名竞合处断混乱、刑行衔接不畅等一系列问题, 导致部分危害性极大的人脸信息侵犯犯罪行为难以得到有效追责, 刑法的威慑与兜底作用未能充分发挥, 构建专项化、精准化的人脸信息刑法规制体系已成为当下司法实践的迫切需求。

2. 人脸识别信息刑法规制困境的深层成因

人脸识别信息刑法规制的各类司法困境, 并非单一制度缺陷导致, 而是法律概念适配、司法解释标准、罪数适用规则、法律体系衔接等多重因素叠加的结果。结合刑法基础理论与司法实践现状, 可从法律属性与概念衔接、入罪标准适配性、罪名适用规则三大维度, 深度剖析困境的核心成因。

首先, 刑法与前置法的概念适用分歧与行为边界模糊, 是规制混乱的基础成因。在个人信息法律保护体系中, 人脸识别信息已被《个人信息保护法》明确列为高敏感生物识别信息, 纳入核心民事保护范畴, 但刑法领域长期存在概念适用争议, 学界形成“范围差异说”与“范围统一说”的对立观点。“范围差异说”主张前置法规制范围更广, 刑法作为最后保障法, 仅规制严重危害行为, 个人信息认定范围应窄于前置法; 而“范围统一说”基于法律体系统一性, 强调部门法同一法律概念应解释一致, 避免法律适用矛盾^[3]。长期以来, 司法实践中部分裁判采纳“范围差异说”, 将人脸信息排除在刑法核心保护范围之外, 造成前置法保护与刑事保护脱节, 出现“民事侵权规制、刑事无法追责”的法律漏洞。同时, 侵犯公民个人信息罪中“以其他方法非法获取”的行为边界认定模糊, 进一步加剧了司法乱象。司法实践中对“窃取”行为的认定清晰, 但对于职务、服务场景下的越权获取行为界定标准不一, 部分行业从业者依托合法工作权限采集人脸信息, 后续超越授权范围流转、滥用信息的行为, 是否属于非法获取范畴, 缺乏统一裁判标准, 导致大量行业内人脸信息黑产行为难以被精准打击^[4]。

其次, 现有司法解释入罪标准适配性不足, 是罪责刑失衡的核心成因。当前司法实践中, 人脸信息犯罪统一适用普通个人信息的“情节严重”认定标准, 未结合人脸信息的高敏感特性设置差异化规则, 存在明显的制度滞后性。根据《个人信息刑事解释》第5条规定, 行踪轨迹、征信等极高敏感信息入罪门槛为50条, 健康生理信息为500条, 普通个人信息为5000条, 但人脸识别信息无法归入上述任一专项范畴, 只能适用5000条的普通信息入罪标准。从风险社会理论的视角审视, 数字时代生物识别信息泄露属于典型的技术性社会风险, 具有损害不可逆、传播范围广、后果潜伏期长的特征, 传统刑法以实害结果为核心、以信息数量为核心标尺的入罪逻辑, 本质上是工业时代的回应型规制模式, 难以适配数字风险的扩散性与隐蔽性^[5]。对人脸识别信息沿用普通个人信息的数量门槛, 低估了人脸信息“单条即高危”的特殊属性, 即人脸信息具备唯一性与不可替代性, 少量信息泄露即可引发精准诈骗、身份冒用、洗钱等次生犯罪^[6]。导致刑法介入时点滞后, 无法发挥预防性规制功能。虽可依托“明知他人犯罪仍提供信息”条款兜底定罪, 但该规则仅适用于上下游关联黑产情形, 适用范围有限, 最终导致司法裁判尺度不一、罪责刑不相适应。

最后, 关联罪名竞合处断规则混乱与刑行衔接缺位, 是规制效能不足的关键成因。人脸识别相关犯

²<https://www.court.gov.cn/zixun/xiangqing/43942.html>

罪多为复合型网络犯罪, 行为人实施犯罪时往往同时触犯侵犯公民个人信息罪、非法获取计算机信息系统数据罪、盗窃罪、诈骗罪等多个罪名, 但目前学界与司法实务界尚未形成统一的罪数处断标准, 裁判乱象突出。司法实践中存在单一定罪、数罪并罚、牵连犯从一重处断三种裁判模式, 部分裁判仅评价目的侵财行为, 遗漏对人脸信息权益、网络安全法益的独立保护, 导致量刑畸轻、法益评价不全。学界对此也争议不断, 数罪并罚说、牵连犯处断说、目的行为吸收说各有依据, 未形成统一适用规则, 严重影响司法公信力[7]。与此同时, 刑事法律与民事、行政法律的衔接机制不完善, 前置监管与刑事追责断层问题突出。日常人脸信息违规采集、流转行为多由行政机关以行政处罚方式处置, 行刑移送机制不健全, 大量涉嫌刑事犯罪的案件被以罚代刑, 未能及时纳入刑事司法程序, 导致人脸信息黑产的上下游链条无法被彻底斩断, 难以形成常态化、全链条的打击震慑格局。

从全球范围看, 域外主要经济体均已针对生物识别信息构建专门化规制体系, 而我国当前仍沿用普通个人信息的统一规制模式, 制度供给的针对性不足进一步放大了上述困境。

3. 人脸识别信息刑法规制的完善路径

针对当前人脸识别信息刑法规制的各类困境, 结合体系解释理论与司法实践需求, 需立足人脸信息的特殊法益属性, 借鉴域外成熟规制经验, 从法律解释规则、司法解释标准、罪数处断规则、法律体系协同四个维度, 构建精准化、系统化、层级化的刑法规制体系, 实现权益保障、秩序维护与技术发展的动态平衡。

第一, 统一法律解释规则, 夯实部门法体系衔接基础。首先, 坚守法律体系统一原则, 确立刑法与前置法个人信息概念统一解释规则, 以体系解释为核心, 明确人脸识别生物识别信息属于刑法法定公民个人信息范畴, 彻底消除部门法概念冲突[8]。依托指导性案例 192 号的司法指引效力, 将原始人脸采集信息、动态人脸数据、3D 人脸衍生模型等全类型人脸信息纳入刑事保护范围, 统一全国司法认定标准, 杜绝同案不同判现象。其次, 明确非法获取人脸信息的行为边界, 结合同类解释与目的论解释双重逻辑, 界定“以其他方法非法获取”的核心内涵, 将职务、服务场景下超越授权范围采集、储存、流转人脸信息的行为, 购买、接收非法流转人脸信息的行为, 全部纳入非法获取的规制范畴, 精准打击行业内人脸信息黑产犯罪[9]。

第二, 细化差异化入罪标准, 破解罪责刑失衡难题。突破传统单一“数量导向”的入罪模式, 针对人脸信息高敏感、高风险的特性, 构建“数量 + 危害 + 情节”三位一体的综合入罪认定体系。域外立法普遍对生物识别信息采取分层级特殊保护模式: 欧盟《通用数据保护条例》(GDPR)将生物识别数据明确列为“特殊类别个人数据”, 原则上禁止处理, 仅在严格限定的例外情形下方可实施, 并配套了高额行政罚款与刑事追责衔接机制; 美国在政府部门使用人脸识别技术的规制方面, 主要采取三种模式: 一是严格禁止模式; 二是特许授权模式; 三是任意使用模式。禁止使用制度为美国旧金山市所首创, 并被美国不少城市所效仿, 在目前备受关注[10]。我国可借鉴域外分层保护经验, 在现有司法解释基础上增设生物识别信息专项入罪条款, 大幅降低人脸信息刑事入罪的数量门槛, 明确非法获取、贩卖、储存一定数量人脸信息, 足以造成公民人身财产安全风险、诱发网络诈骗等次生犯罪的, 即可认定为“情节严重”。同时设置行业从重处罚规则, 对于通信、物业、互联网平台等依托职务、服务权限非法获取人脸信息的从业者, 适用从重处罚标准, 压实行业主体合规义务。拓宽“情节严重”的认定范围, 不再局限于上下游犯罪关联情形, 将单纯批量囤积、倒卖人脸信息、多次实施人脸信息违法行为等情形纳入入罪范畴, 全方位提升刑法对人脸信息的保护力度。

第三, 规范罪数处断规则, 实现法益全面评价。明确人脸识别复合型犯罪的罪数认定标准, 厘清牵连犯、吸收犯的适用边界, 确立“多重法益、独立评价”的司法裁判原则。区分《刑法》第 287 条的适

用场景,明确该条款仅适用于手段行为无独立社会危害性的情形,对于破解人脸识别系统、非法获取人脸信息、侵入计算机系统、实施网络侵财的复合型犯罪,若手段行为与目的行为分别侵害个人信息权、网络安全、财产权等独立法益,均具有独立可罚性,应当依法数罪并罚,杜绝单一罪名评价导致的法益保护缺位。通过统一罪数处断标准,彻底解决司法裁判尺度混乱问题,严格贯彻罪责刑相适应原则,实现对各类法益侵害结果的全面追责。

第四,健全刑行协同机制,构建全链条规制体系。完善“民事救济、行政监管、刑事追责”层层递进的立体化保护体系,强化前置法与刑法的有效衔接。行政监管部门强化日常执法监管,重点整治各类违规采集、滥用人脸信息的行业乱象,完善人脸信息处理合规审查机制,从源头遏制违法行为。健全行刑衔接案件移送机制,明确行政违法与刑事犯罪的边界标准,对于批量非法处置人脸信息、情节恶劣、涉嫌刑事犯罪的案件,坚决杜绝以罚代刑,及时移送司法机关启动刑事追责程序。通过行政监管前置、刑事兜底保障的协同模式,全方位斩断人脸信息黑色产业链,形成常态化、全覆盖的违法犯罪打击格局。

数字技术的创新发展离不开法治的规范护航,人脸识别技术的良性发展,必须以公民个人权益保障为底线。当前我国人脸识别信息刑法规制体系虽已初步建立,但仍存在解释规则模糊、入罪标准失衡、裁判尺度混乱等诸多问题。未来需持续依托指导性案例的司法指引作用,吸收域外先进规制经验,优化法律适用规则、细化司法认定标准、完善协同规制体系,在严厉打击人脸信息违法犯罪、保障公民人格与财产权益的同时,合理规划技术创新的法律边界,实现个人权益保护、网络秩序治理与数字经济高质量发展的动态平衡,为数字社会法治化建设提供坚实的法治支撑。

参考文献

- [1] 张新宝.《中华人民共和国个人信息保护法》释义[M].北京:中国法制出版社,2021.
- [2] 王明平.两男子窃取588套公民人脸数据,被用于电话卡实名认证后成电诈帮凶 两人双双获刑[EB/OL].
<https://www.toutiao.com/article/7639654735494103594/>, 2026-07-18.
- [3] 喻海松.“刑法先行”路径下侵犯公民个人信息罪犯罪圈的调适[J].中国法律评论,2022(6):121-131.
- [4] 李瑞.非法获取型侵犯公民个人信息罪中“其他方法”的规范判断[J].湖南警察学院学报,2023,35(5):118-128.
- [5] [德]乌尔里希·贝克.风险社会[M].何博闻,译.南京:译林出版社,2004.
- [6] 王德政.针对生物识别信息的刑法保护:现实境遇与完善路径——以四川“人脸识别案”为切入点[J].重庆大学学报(社会科学版),2021,27(2):138.
- [7] 周光权.涉人脸识别犯罪的关键问题[J].比较法研究,2021(6):13-29.
- [8] 雷达,郑旭江.法秩序统一视野下“个人信息”的认定——从侵犯公民个人信息罪切入[J].北京科技大学学报(社会科学版),2023,39(3):310-319.
- [9] 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.
- [10] 邢会强.人脸识别的法律规制[J].比较法研究,2020(5):51-63.