ISSN：3105-0085
EISSN：3105-0093

人脸识别信息的刑法保护问题研究

李思宇 王 慧 甘瑞丰 *

大连海洋大学海洋法律与人文学院，辽宁 大连 116023

摘 要：人脸识别信息因具有身份唯一性、采集便捷性和不可匿名化等特质，已成为公民个人信息体系中的核心要素。目前，适用侵犯公民个人信息罪规制相关行为时，存在入罪标准模糊、行为规制范围过窄、量刑情节界定不清等问题，导致司法保护存在漏洞，难以有效应对数字时代的个人信息安全风险。为解决上述问题，应从立法层面系统推进以下改革：首先，明确将“人脸识别信息”列为重点保护对象，赋予其与其他敏感信息同等的法律地位；其次，将非法储存行为纳入刑法规制，弥补现行法对行为类型覆盖的不足；再次，区分作为与不作为的入罪标准，避免“一刀切”认定，实现罪责刑相适应；最后，在量刑层面强化从业禁止的适用，完善罚金刑裁量规则，并增设数据整改从宽及知情同意免责情节，构建多层次处罚与激励体系，全面强化人脸识别信息的刑法保护。

关键词：人脸识别；个人信息；刑法保护路径

DOI：10.64649/yh.shygl.2026020019

1 问题的提出

作为具有高度敏感性与身份唯一性的生物识别数据，人脸识别信息直接关联公民的人身识别与财产安全核心权益，其一旦被非法获取、使用或泄露，可能引发身份冒用、财产损失等连锁危害。目前，民法在规制侵犯人脸识别信息行为时，存在处罚力度偏轻、惩戒威慑不足的局限，难以形成有效震慑，更无法充分应对新技术迭代带来的新型风险挑战。从刑法保护维度来看，人脸识别信息显然属于侵犯公民个人信息罪所保护的敏感个人信息范畴，但其特殊性尚未在立法层面得到明确凸显。我国现行《刑法》及相关司法解释，尚未针对侵犯人脸识别信息的行为作出专门性规定，导致司法实践中存在认定标准不统一、规制力度不足等问题，难以充分发挥刑法作为“社会保护最后防线”的功能。

2 人脸识别信息刑法保护的必要性

有部分学者认为，人脸识别技术虽在身份核验、场景智能化等方面作用显著，但其背后的风险不能轻视，因此有必要引入风险预防理论进行规制[1]。不过，也有学者提出了不同看法。他们认为，若因过度担忧人脸识别技术的风险，就主张让刑法提前介入规制，甚至一味将相关行为“罪过化”，这种思路有待进一步探讨。在他们看来，人脸识别技术本身并无价值倾向，是客观中立的工具，从推动科技进步的角度出发，不应对这类中立技术施加过于严苛的约束[2]。需要明确的是，人脸识别信息既带有不可替代的人身专属属性，又具备可转化的财产关联价值，属于权益高度复合化的敏感个人信息，对其的规制确实需要更精准的平衡。鉴于此，对人脸识别信息的法律保护不能依赖单一部门法，而需构建前置法与刑法协同发力的体系化保护机制。

2.1 法益保护的优先定位

人脸信息天然携带能锁定个人身份的唯一性标识，这种特性使其一旦遭遇非法获取或被违规滥用，信息主体的隐私就会直接面临泄露风险。在个人信息权益体系中，存在一项核心权利——信息自决权，它具体指信息主体对自身信息享有控制、支配的权利，以及自主决定信息如何被使用的决策权利[3]。人脸识别技术已深度渗透生活场景，从日常购物的自助结账到小区的门禁管理，应用场景日益广泛。但信息主体常陷入到不提供人脸信息就无法享受服务的被动局面，对于自身人脸信息的保存时长、保存范围，以及具体使用场景、是否会共享给第三方等关键事项，其知情权与许可权往往难以得到有效保障。随着网络技术的成熟，人脸识别数据与消费记录、浏览偏好等商业数据的融合不断加深。企业可借此串联消费者在不同平台、不同时段的消费行为，甚至精准推测其消费需求与习惯。精准描绘消费画像，进而开展定向广告投放与推销活动。

2.2 安全与发展的动态权衡

人脸识别技术在生活中提供诸多便利，从交通出行的刷脸检票到日常消费的刷脸支付，极大简化了生活流程。但与之配套的法律规制仍存在明显短板，难以完全覆盖技术应用中出现的新问题。由于人脸信息既直接关联个人隐私与人格尊严，又能为企业带来商业流量与经济利益，二者深度绑定的特性使其一旦遭遇滥用或被恶意利用，不仅会侵害个体权益，还极易滋生数据黑市、精准诈骗等各类社会问题。

ISSN：3105-0085
EISSN：3105-0093

而构建一套权责清晰、惩戒有力的刑法规制体系，正是实现技术创新发展、个人合法权益保障与社会秩序稳定三者动态平衡的关键。将情节严重的侵犯人脸识别信息行为纳入刑事立法，是筑牢公民权益保护防线的必要之举。唯有以刑事手段划定红线，方能倒逼企业合规采集、严管数据，让技术回归“便民”初心，才能在数字时代重塑公众对“刷脸”的安全感与信任感。

2.3 刑法机能的最终实现

《民法典》虽已从法律层面明确规定，信息主体在个人信息处理活动中依法享有同意权、知情权以及在权益受损时的损害赔偿请求权，但在具体的司法实践场景中，由于证据固定难度大、责任认定流程复杂等现实因素，信息主体作为受害人，其合法权益的维护往往面临诸多阻碍，维权之路仍存在不少困难。在生活中，人脸识别系统常未经同意便安装启用，当事人拒绝则无法享受服务或进入场所，同意权沦为形式。同时，《个人信息保护法》虽对监管部门职责与处罚方式有规定，但部门职责分工未细化，影响保护工作推进；且记入档案等行政处罚力度，远低于信息处理者非法获利，难以形成有效威慑。而现有民事与行政救济难以应对技术带来的风险，因此需完善刑法规制体系。

3 人脸识别信息的刑法保护困境

3.1 侵犯人脸识别信息的入罪界限模糊

司法工作人员因对技术及法律属性的认知差异，在案件定性、罪责界定上易产生分歧，侵犯人脸识别信息的入罪标准存在模糊性。构成侵犯公民个人信息罪需满足“情节严重”，《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》（以下简称《解释》）第 5 条虽按信息类型设定了量化标准，但受立法滞后性影响，未对人脸识别信息的保护层级作出规定。若参照我国法律对其他类型个人信息的入罪标准，通常需达到非法处理 5000 条以上才会被认定为“情节严重”；但对于行踪轨迹信息、通信内容这类敏感度极高的核心信息，入罪门槛大幅降低，仅需非法处理 50 条即可构成“情节严重”。而人脸识别信息既包含面部特征这一不可变更的生物识别数据，又常与身份、行为等信息关联，兼具高敏感性与强关联性，如何结合其数据特性科学设定合理的入罪数量标准，在精准打击违法犯罪与保障技术合理应用之间实现罪责平衡，这一问题仍需学界、司法界进一步深入探讨。

3.2 侵犯人脸识别信息的行为类型缺漏

在人脸识别信息犯罪的完整链条中，不法分子通常会通过隐蔽拍摄、数据窃取等方式，从公共场所、APP 应用或数据库中获取大量人脸数据，为后续犯罪活动奠定基础；随后，这些非法收集的人脸信息会进入流通与处理环节，具体表现为非法出售给第三方机构、向他人违规提供以牟取利益，或是进行数据清洗、格式转换等加工操作；最终环节是非法使用行为，比如将人脸数据用于虚假身份认证、精准诈骗、非法监控等，直接对公民的人身财产安全与信息权益造成侵害[4]。普通信息处理机构在依法获取人脸识别信息，并顺利完成用户明确授权范围内的各项信息处理事宜后，其对该类核心生物特征信息的合法持有基础便已丧失，相应的持有资格也随之终止。若此类机构明明具备删除信息的技术条件、人力支持与执行能力，却故意拖延或明确拒绝履行数据删除义务，反而长期持续非法储存大量包含公民不可替代生物特征的人脸识别信息，这种消极放任的不作为行为已构成典型的不作为式非法持有，严重违反了个人信息保护领域相关法律法规及监管要求。

3.3 侵犯人脸识别信息的量刑标准不明

我国《刑法》中关于侵犯公民个人信息罪的量刑情节缺乏明确、具体的界定标准，相关条款的表述较为原则化，这一立法现状直接导致司法实践中此类案件的量刑尺度难以统一，普遍存在偏轻的问题。这种轻缓化的量刑结果，既未能充分发挥法律应有的威慑作用与惩戒效能，也难以从根本上遏制侵犯公民个人信息行为持续蔓延的态势，亟需结合当前个人信息保护的现实需求与司法实践经验进行优化调整。《刑法》第 253 条第 2 款针对“在履行职责或者提供服务过程中”侵犯公民个人信息的行为设置了加重处罚条款，以期加大对特殊场景下侵权行为的规制力度，但在司法实践中，由于“履行职责”“提供服务”的边界界定缺乏清晰指引，行为主体是否处于该特定状态的认定存在明显困难，导致该加重处罚条款的适用率偏低，未能充分发挥其立法初衷。多数具有特殊身份的主体都隐去了本人身份，实质上却利用了身份带来的各种影响达成非法侵犯目的[5]。这会导致规制效果难以达至理想状态。

4 人脸识别信息刑法保护的完善路径

4.1 扩容侵犯公民个人信息罪的行为边界

在当前侵犯公民个人信息犯罪已形成完整产业链的背景下，现行《刑法》第 253 条主要规制非法获取与使用行为，尚未将非法存储纳入管辖，存在明显的规制盲区。《刑法》中的作为义务主要包括对危险源的监管义务和对法益对象的保护义务[6]。后者来源于职务、业务

ISSN：3105-0085
EISSN：3105-0093

或制度规定。《个人信息保护法》第 47 条设定的信息删除义务，为刑法中认定不作为型的非法持有提供了法律依据。在刑事责任认定上，应严格遵循不作为犯的构成要件，即行为人负有法定作为义务、能够履行却未履行，并因此产生或可能产生严重后果。考虑到单纯持有与主动出售、提供等行为在主观恶性和社会危害性上存在差异，其入罪标准应作区分处理。建议将非法持有人脸识别信息的入罪数量设定为 5000 条，既体现罪责刑相适应原则，也有助于强化对该类敏感信息的司法保护。

4.2 界定人脸识别信息的刑事入罪标准

关于入罪标准，现行《解释》按信息敏感度将“情节严重”划分为三个数量层级。若将人脸信息置于第三层级（5000 条以上），则因门槛过高导致处罚范围过窄，难以实现有效规制。有学者建议，将侵犯人脸识别信息归入《解释》第 5 条第 10 项 “其他情节严重的情形”，并将非法获取、出售或提供生物识别信息 5 条及以上的行为入罪 [7]。但此举可能违反罪刑法定原则的明确性要求。较为合理的路径是借鉴行踪轨迹、通信内容等信息的保护逻辑，将人脸识别信息纳入第一层级（50 条以上）。该信息与个人人身、财产权益高度关联，其泄露可能引发严重后果，将其列为第一层级既符合现有规范体系，又能体现其特殊的法益保护需求，实现罪刑均衡与技术风险之间的制度调适。

4.3 优化个人信息犯罪的惩戒与处遇体系

为完善侵犯公民个人信息罪的处遇体系，建议从以下四方面进行优化：第一，优化罚金刑适用标准。除依据违法所得倍数外，应结合信息保护层级、犯罪情节及危害后果等因素设定阶梯式罚金标准，并设立最低罚金数额以增强适用性。对无力支付者，可适度加重自由刑以实现刑罚相当。第二，将数据整改明确为减轻处罚情节。对于在经营中主动履行风险防控、侵害发生后积极配合调查、有效弥补漏洞并落实整改措施的企业，可在量刑时予以从宽处理，以此激励主体责任落实与系统防护提升。第三，以信息主体知情同意作为免除处罚情节 [8]。处理信息前已明确告知处理目的、方式与范围，并取得信息主体有效同意的，可阻却刑事违法性。该同意须基于真实意愿、不损害公共利益，且以单次授权为限。第四，强化从业禁止制度的适用。对利用职务或业务便利实施犯罪的特定从业人员，在刑罚执行完毕后依法施加从业限制，防止其再犯，增强刑法在敏感行业中的威慑与预防效能。

5 结语

当前人脸识别信息的刑法保护面临入罪标准模糊、行为规制缺漏及量刑机制失衡三重困境。为有效应对，需构建层次化的保护体系：在立法层面明确其敏感信息地位并将非法储存行为独立入罪；根据信息特性与行为危害性设置差异化入罪标准，建议纳入《解释》第一层级；同步完善处遇措施，通过优化罚金规则、引入数据整改激励机制及强化从业禁止适用，实现惩罚与预防并重。这一系统性完善路径既能强化个人信息安全保障，亦为技术发展划定必要法律边界，最终实现权益保护与科技创新之平衡。

参考文献：

[1] 张勇 . 个人生物信息安全的法律保护——以人脸识别为例 [J]. 江西社会科学 ,2021,41(05):157-168+255-256.

[2] 邢会强 . 人脸识别的法律规制 [J]. 比较法研究 ,2020,(05):51-63.

[3] 沈朝阳 . 论人脸识别信息应用的法律规制进路 [J]. 西部金融 ,2022,(07):74-79.

[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(01):72-83.

[5] 李娜 . 人脸识别信息的刑法保护研究 [D]. 中国人民公安大学 ,2023.

[6] 张明楷 . 刑法学 [M].6 版 . 北京 : 法律出版社 ,2021:198-204.

[7] 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(02):133-143.

[8] 苏雄华 , 刘忠福 . 人脸识别信息刑法保护的问题检视与路径完善 [J]. 福建警察学院学报 ,2025,39(02):46-54.

作者简介：李思宇（1998.02—），女，汉族，辽宁省鞍山市，研究生，研究方向：刑法学。
通讯作者：甘瑞丰（1982.06—），男，汉族，博士，讲师，研究方向：刑法学。