人脸识别信息隐私侵犯与刑法保护

冯敏

贵州财经大学法学院，贵州贵阳，550025；

摘要：随着信息技术的飞速发展，技术创新衍生出大量新型人工智能技术，其中人脸识别技术应用范围最为广泛、应用价值最高，受到社会各界的强烈关注。人脸识别技术自开发应用以来，便以极快的速度渗入社会公众的日常生活，给公众生活带来便利的同时，技术的不规范使用也对个人信息保护提出了挑战，侵犯人脸识别信息的违法犯罪案件也在逐年递增。本文聚焦于人脸识别信息在当今数字化时代所面临的隐私侵犯问题及其刑法保护机制。首先阐述了人脸识别技术的广泛应用现状以及由此引发的隐私风险，分析了隐私侵犯的多种表现形式。接着探讨了现行刑法在保护人脸识别信息方面的相关规定及适用困境。最后提出了完善刑法保护的路径，包括明确法律概念、细化入罪标准、加强行刑衔接以及提升公众意识等，旨在构建更为有效的刑法保护体系，以应对人脸识别信息隐私面临的严峻挑战，维护公民的基本权利与社会的信息安全秩序。

关键词：人脸识别信息；隐私侵犯；刑法保护

DOI：10.69979/3029-2700.25.05.068

引言

随着科技的飞速发展，人脸识别技术已广泛渗透到社会生活的各个角落，从智能手机解锁、门禁系统到金融支付、公共安全监控等领域，其便利性和高效性显著提升了社会运行效率。然而，人脸识别信息作为一种极具敏感性的个人生物识别数据，其隐私保护问题也日益凸显。一旦遭受侵犯，不仅会对个人的人格尊严、财产安全和隐私权益造成严重损害，还可能引发一系列社会安全隐患。刑法作为保护公民权利的最后一道坚实防线，在人脸识别信息隐私保护中承担着至关重要的角色。

1 人脸识别信息概述

人脸识别信息是随着人脸识别技术的广泛应用而产生的新型信息种类，其具有独特的价值与特征。从常义上理解，人脸识别信息就是把“人脸”信息数据化并加以利用。从法律概念的意义上讲，人脸识别信息作为公民个人信息的类型之一，是识别特定自然人身份的重要信息数据。明确人脸识别信息的概念，准确界定其法律属性，剖析其本质特征，是构建人脸识别信息刑法保护体系的出发点。

1.1 人脸识别信息的概念

人脸识别是一种基于人的脸部特征信息进行身份识别的一种生物识别技术。它通过摄像机或摄像头采集含有人脸的图像或视频流，自动在图像中检测和跟踪人脸，如眼睛、鼻子、嘴巴等的位置和形状信息，然后将这些特征与已存储的人脸数据库进行比对，从而确定身份。人脸识别技术主要包括人脸检测和人脸对比两个过程。首先，通过人脸检测技术确定图像中是否存在人脸，并标定出人脸的位置和大小；然后，通过人脸对比技术提取人脸的特征信息，并将其与已知的人脸特征进行对比，从而识别每个人脸的身份。

1.2 人脸识别信息的特征

第一，唯一性。基于基因多样性，不同主体面部特征不会完全相同，且人脸识别信息可变性低，个体成年后面部特征变化多在识别技术能力范围内，较为稳定。所以，计算机识别系统能精准区分肉眼难辨的相似主体。尽管同卵双胞胎因器官结构相似带来识别挑战，但计算机系统仍可凭借精确识别，使人脸识别技术得出唯一验证结果。

第二，便宜采集性。与传统个人信息录入（需手动登录）、指纹等生物识别信息提取（需主动参与）不同，获取人脸识别信息无需信息主体配合，设备能远距离自动抓取，采集快速高效。凭借这一特性，乘车安检、游园检票、等公共场所广泛应用人脸识别技术，既能节省人力成本，又能提高工作效率，有效应对客流高峰时的拥堵。

第三，高度敏感性。人脸识别信息不仅可以用于精确追踪信息主体，还能迅速与信息主体的其他个人信息相连接，在网络环境中可以轻易用数据刻画出信息主体的完整形象。

第四，不可匿名性。个人信息匿名化是信息披露交流的合理形式，能切断信息与主体联系，实现去主体化。但含人脸识别信息的生物识别信息匿名化是伪命题，人脸识别信息因唯一性和表现形式无法去识别化，匿名处

理会致其失去应用价值，这表明此类信息一旦泄露，危害更严峻 。

2 刑法对人脸识别信息保护的现状与困境

2.1 相关罪名及规定

目前刑法中与人脸识别信息保护相关的罪名主要包括侵犯公民个人信息罪。根据相关规定，非法获取、出售或者提供公民个人信息，情节严重的行为将受到刑法处罚。人脸信息作为公民个人信息的一种重要类型，在理论上可适用该罪名进行保护。然而，在实际司法实践中，对于人脸识别信息的界定、何为“情节严重”等问题的判断存在一定的模糊性。例如，对于非法采集少量但具有特殊价值的人脸识别信息是否构成犯罪，以及如何衡量其情节严重程度，缺乏明确的标准。由此可见，刑法对人脸识别信息的规定缺位导致司法实践中无法直接援引刑法相关规定对人脸识别信息进行明确保护，尽管当前能够运用解释方法将人脸识别信息纳入刑法保护范围，但明确予以规定仍是解决问题的根本。

2.2 适用困境

2.2.1 罪名界定模糊

目前，我国刑法及相关司法解释在涉及人脸识别信息方面的规定尚未明确，与其他类似个人信息的界限难以准确区分。这遗漏了一个不断增长并被广泛使用的个人信息种类，难以为针对其侵权行为的量刑提供明确规范。人脸信息不仅涉及个体的健康生理特征，更有可能关联到个体的安全、隐私和经济利益，从而该信息的滥用和泄露潜在的危害极大。刑法规定了侵犯公民个人信息罪，司法解释侵犯公民个人信息罪中的“公民个人信息”进行定义，但该定义并未明确将人脸识别信息列为侵犯公民个人信息罪中的“公民个人信息”，《解释》第 1 条在列举个人信息类型时，姓名、身份证件号码等信息被明确提及，但并未包括人脸识别信息，这一做法可能存在合理性问题。

2.2.2 入罪标准不明确：

我国现行《刑法》及其相关司法解释并未就侵犯人脸信息达到多少条时构成“情节严重”、是否成立侵犯公民个人信息罪作出答复，未对人脸信息给予特殊保护。在涉及人脸识别信息的案件中，对于信息数量、获取方式、使用目的、造成的危害后果等因素如何综合考量以确定是否达到入罪标准，尚无统一规范。这可能导致一些具有严重社会危害性的人脸识别信息侵犯行为因不符合现有模糊的入罪标准而无法被追究刑事责任，或者一些情节较轻的行为被过度入罪，影响司法公正和刑法的权威性。

3 人脸识别技术中隐私侵犯的表现形式

3.1 数据过度收集

第一、许多应用或服务提供商在收集人脸识别信息时，往往超出了实现其业务功能所必需的范围。例如，社交娱乐应用注册时，额外收集面部表情细节等信息；商业机构会员注册，除人脸图像，还大量收集姓名、身份证号等个人信息。第二、一些不良商家或不法分子采用隐蔽手段收集人脸识别信息。他们可能在用户不知情的情况下，通过在公共场所设置隐藏摄像头、在应用程序中植入恶意代码等方式，悄然获取用户的人脸图像或视频流。例如，如商场、酒店被安装非法监控设备，秘密采集过往人群信息用于盗窃、诈骗等。

3.2 未经授权的收集和使用

在很多场合，个人的人脸信息被未经授权地采集和使用。部分应用程序或设备在用户不知情的情况下，擅自开启摄像头收集人脸信息。例如，部分商场擅自利用人脸识别摄像头收集消费者的人脸信息，分析消费者的性别、年龄等。有人以牟利为目的，利用 AI 换脸软件非法处理他人人脸信息，将他人人脸与部分视频中的人脸进行替换合成，制作虚假的换脸视频和图片。甚至存在一些不法分子通过恶意软件或网络攻击手段，窃取他人的人脸信息，并将其用于诈骗、盗窃等。

3.3 数据存储不安全

人脸识别技术中的人脸信息存储环节隐患重重。人脸信息多储存于计算机数据库或云存储系统，这些系统易出现软件漏洞，黑客借此发动网络攻击，入侵系统窃取信息。部分机构和企业对数据加密不够重视，加密技术落后，加密密钥强度低、算法过时或加密过程有缺陷，都会导致人脸信息易被黑客破解。此外，数据存储的物理环境不容忽视，一些数据中心建设管理时对物理访问控制不严，不法分子可非法闯入，获取信息或破坏存储设备，造成数据丢失损坏。

3.4 身份冒用与欺诈

人脸信息具有较高的商业价值，一些不法分子可能会滥用或非法交易人脸信息。不法分子通过获取他人的人脸信息，利用人脸识别技术的漏洞或伪造身份验证手段，冒用他人身份进行各种违法犯罪活动。例如，在金融领域，冒用他人身份进行贷款申请、信用卡办理或盗刷；在网络社交平台，冒用他人身份进行虚假信息传播、诈骗等行为，严重损害了被冒用者的财产安全和个人声誉，给个人和社会带来经济与安全风险。

4 完善刑法保护的路径

4.1 明确法律概念

在对个人信息的种类进行列举时，应当将人脸识别

信息明确加以列举，防止司法实践中司法机关对人脸识别信息保护的忽视。实践裁判中，人脸识别信息不应与其他危害性更低的个人信息采取统一批量认定的方式进行定罪量刑，应当对人脸识别信息进行单独分类评价认定，以达到保护效果。对于人脸识别信息这类敏感个人信息，其本身往往与信息的用途或者行为人获取、利用信息的目的有关，对于不同种类公民个人信息的定罪量刑条款的适用，应当结合定性标准，动态的界定不同场景下公民个人信息的合理利用范围和法律保护范围，对于人脸识别信息应当明确给予层次更高的保护。

4.2 细化入罪标准

进一步明确侵犯公民个人信息罪中关于人脸信息的界定、收集、使用的合法界限以及“情节严重”的具体标准。对于非法获取计算机信息系统数据罪，应根据人脸识别技术的特点，细化非法侵入和获取数据的行为方式及定罪量刑标准。在侵犯商业秘密罪方面，应明确人脸信息作为商业秘密的具体认定条件和保护范围，以便更好地打击相关犯罪行为。综合考量人脸识别信息侵犯行为的各个方面因素，制定详细的“情节严重”入罪标准。通过这种多维度的细化规定，使入罪标准更加科学合理、具有可操作性，确保刑法能够精准打击严重的人脸识别信息隐私侵犯行为。

4.3 加强行刑衔接

建立健全行政监管与刑事司法之间的衔接机制。行政机关在日常监管过程中，如发现涉嫌侵犯人脸识别信息的行为，应及时进行调查处理。对于情节较轻尚不构成犯罪的，依法给予行政处罚；对于涉嫌犯罪的，应迅速将案件移送司法机关，并提供相关证据材料和调查情况说明。司法机关在办理此类案件时，应加强与行政机关的沟通协作，对于行政机关移送的案件及时审查立案，在案件审理过程中充分参考行政机关的前期调查成果，确保行政监管与刑事司法形成合力，共同打击人脸识别信息隐私侵犯行为，避免出现处罚漏洞或重复处罚的情况。

4.4 提升公众意识与技术保障

4.4.1 公众意识方面

通过广泛的宣传教育活动，提高公众对人脸识别信息隐私保护的认识。利用媒体、网络平台等多种渠道，向公众普及人脸识别技术的应用风险以及如何保护个人人脸识别信息的知识。增强公众的自我保护意识和隐私维权意识，从源头上减少人脸识别信息被侵犯的可能性。通过宣传教育活动，提高公众对人脸识别技术隐私侵犯风险的认识，增强公民的自我保护意识。同时，加强对相关企业和从业人员的法律培训，使其了解人脸识别技术应用中的法律责任和义务，自觉遵守法律法规，合法合规地开展业务活动。

4.4.2 技术保障方面

用技术保障人脸识别信息，能增强安全性，保护个人隐私不被泄露与滥用；还能提高识别准确率，减少错误识别的情况发生；同时，有助于在安防、金融等领域可靠地确认身份，推动行业健康发展，增强社会信任。因此应该鼓励企业和科研机构加大对人脸识别技术安全保障方面的研发投入。研发先进的加密技术、访问控制技术等，用于人脸识别信息的存储和传输过程，确保信息的安全性。

5 结论

人脸识别信息的隐私保护在数字化时代面临着前所未有的挑战，刑法保护作为其中的关键环节，需要不断适应技术发展和社会需求进行完善。通过明确法律概念、细化入罪标准、加强行刑衔接以及提升公众意识与技术保障等多方面的努力，构建更为严密、科学、有效的刑法保护体系，能够更好地防范和打击人脸识别信息隐私侵犯行为，切实保障公民的人格尊严、隐私权益和社会的信息安全秩序，促进人脸识别技术在合法合规的轨道上健康发展，为构建数字社会的法治基石贡献力量。现行刑法在一定程度上对人脸识别技术中的隐私侵犯提供了保护，但仍存在一些不足之处。通过细化犯罪构成要件、加大刑罚力度、加强行刑衔接等多方面的完善措施，可以在充分发挥人脸识别技术优势的同时，有效地保护个人隐私，促进人脸识别技术的健康发展。

参考文献

[1]马梦萍.人脸识别信息的刑法保护研究[D].扬州大学,2009.
[2]张展悦.侵害人脸识别信息行为刑法规制研究[D].山东财经大学,2010.
[3]徐韩榆.大数据时代加强人脸识别信息刑法保护的困境与完善建议[J].市场周刊,2024(13):158-161.
[4]杨成,梁祝花.非法使用人脸识别信息的刑法应对[J].湖南警察学院学报,2023(04):59-66.
[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]巩欣.人脸识别信息的刑法保护[D].西北政法大学,2021.