第 5 卷◆第 04 期◆版本 1.0◆2023 年
文章类型：论文|刊号（ISSN）：2705-0637(P) / 2705-0645(O)

人脸识别技术在智慧公安系统中的应用

祝大海
杭州悉点科技有限公司
DOI：10.12238/ems.v5i4.6408

[摘　要] 在刑事司法中，人脸识别技术适用核查个体身份、研判身份背景、实时追踪与追捕追逃三种权利干预程度渐次提升的应用场景。在助力惩治犯罪的同时，人脸识别技术也具有错误干预公民人身自由、强化刑事司法执法偏见、突破程序法定原则的潜在风险。我国在构建人脸识别技术综合法律规制框架时，忽视了刑事司法领域的需求，导致从人脸数据采集、比对数据源获取、人脸数据存储管理到识别结果使用均缺乏适用规范性。为此，应建构刑事司法领域人脸识别技术的场景化规制路径，构建敏感人脸数据管理制度、限缩人脸比对数据源范围、构建人脸识别证据的直接举证规则，并赋予被识别主体知情权、更正权等权利。
[关键词] 人脸识别；智慧公安；系统应用

Application of Face Recognition Technology in Intelligent Public Security System

Zhu Dahai
Hangzhou Xidian Technology Co., Ltd

[Abstract] In criminal justice, facial recognition technology is applied in three scenarios where the degree of intervention in individual identity verification, identification background analysis, real-time tracking, and pursuit and escape rights is gradually increasing. While helping to punish crimes, facial recognition technology also carries potential risks of mistakenly interfering with citizens' personal freedom, strengthening criminal justice enforcement bias, and breaking through the principle of procedural legality. When constructing a comprehensive legal regulatory framework for facial recognition technology in our country, we have neglected the needs of the criminal justice field, resulting in a lack of applicability and standardization in facial data collection, comparison of data sources, storage and management of facial data, and use of recognition results. Therefore, it is necessary to establish a scenario based regulatory path for facial recognition technology in the criminal justice field, establish a management system for sensitive facial data, limit the range of facial comparison data sources, establish direct evidential rules for facial recognition evidence, and grant the identified subject the right to know and correct.
[Keywords] facial recognition; Smart Public Security; System application

引言

近年来，随着深度学习技术的发展，人脸识别技术已成为人工智能技术发展产业化最成功的案例。人脸识别技术广泛应用在安防、金融、教育、应急、电子商务等各领域，其在给人们工作、生活和学习带来便利的同时，也存在技术滥用、数据泄露、贩卖等安全风险，易引起公民隐私受侵、财产损失，甚至威胁国家安全。本文介绍了目前人脸识别应用中数据信息安全管理的情况，分析了应用的安全风险，并提出防范应用安全隐患的有关对策，为行业发展提供参考。

1人脸识别技术的规制必要性

1.1 人脸识别技术侵权风险大

人脸识别信息采集具有隐蔽性和强制性，具备识别功能的摄像头随处可见。在手机软件上，当我们在不知情的情况下被拍照进而采集人脸识别信息，告知和同意程序就被需置进而引发一系列法律问题。在信息技术发达的现代社会，人脸识别信息已成为重要的数据资源。在实践当中，从人脸识别信息收集、转卖到违法使用，已经逐渐形成一个产业链。人脸识别信息泄露风险的危害往往更严重，因泄露往往具有隐蔽性，信息所有者难以得知其信息被泄露的情况，造成持续且不可逆的损害。郭兵诉杭州野生动物世界案被喻为我国“人脸识别第一案”,起因是由于杭州野生动物世界在未经郭兵同意的情况下将原定的指纹入园验证方式变更为人脸识别入园方式，并且将郭兵办理会员时留下的照片进行活化处理以用于人脸识别验证。在郭兵多次要求恢复指纹入园验证并且在其人脸识别系统中删除个人照片未果后，将该动物园告上法庭。2021 年 4 月，杭州市中级人民法院进行二审宣判，要求动物园赔偿郭兵合同利益损失及交通费，并删除其办理指纹年卡时提交的包括照片在内的面部特征信息和指纹识别信息。有学者在评论该案件时指出，生物识别信息是敏感个人信息，深度体现自然人的生理和行为特征，具备较强的人格属性，一旦被泄露或非法使用，可能导致个人的人身、财产安全受到危害，因此应谨慎处理并严格保护。由此可见，如果人脸识别技术应用的场景与个人的合理预期不相符合，极易产生侵权的风险。

1.2 民法和行政法保护力度不足

我国民法对人脸识别信息的保护主要是将人脸识别信息作为敏感个人信息而进行保护。《民法典》第 1034 条第二款规定个人信息包括生物识别信息，人脸识别信息属于生物识别信息范畴。民法对个人信息的保护主要是通过对处理个人信息进行限制，自然人享有事前同意权、事中知情权以及事后删除请求权和损害赔偿请求权。但是，在多数情况下，当事人不知情的情况下人脸识别信息已经被采集，导致当事人的同意权得不到保障。人脸识别信息处理过程中，由于信息处理专业性和独立性，当事人一般不参与信息的处理，在信息处理者未充分履行告知义务的情况下，当事人知情权同样受限。在当事人的权益受到侵害的情况下，请求侵权损害赔偿需要受害人证明加害人的违法加害行为、受害人遭受了可救济的损害、加害行为与损害有因果关系和加害人对损害的发生具有过错。受害人处于弱势地位且《民法典》侵权责任编并未就个人信息侵权损害赔偿作出具体的规定，仅靠个人进行救济存在困难。

1.3 涉人脸识别犯罪难以遏制

近年来，应用人脸识别技术侵犯公民个人信息犯罪处于高发态势，而且与电信网络诈骗、敲诈勒索、绑架等犯罪呈合流态势，社会危害严重。通常来讲，鉴于人脸识别技术的应用范围较广,对该技术应用的规制过于严格会阻碍其发展，只有在情节严重的情况下才会选择通过刑法进行规制。在比较法的视野当中，域外对于人脸识别信息的保护局限在生物识别信息的范畴内，而对于涉人脸识别犯罪也未在定罪和量刑方面进行专门的突出强调。美国对于人脸识别技术的规制在刑事司法上没有具体的规定，美国国会通过的《防止身份盗窃及假冒法》将人脸识别信息解释为身份证明材料，部分州将破解人脸识别技术的行为认定为“身份盗窃”，在执行过程中却受限于商事领域，缺乏统一性。欧盟具有代表性的是《一般数据保护条例》（GDPR），同样将人脸识别信息解释为个人敏感数据进行保护，但是对人脸识别信息的保护趋向于谨慎。我国现行刑法对于人脸识别技术犯罪主要涉及侵犯公民个人信息罪、破解人脸识别信息系统罪和侵犯公民人格尊严、财产安全的犯罪，并未对人脸识别技术进行强调并且在定罪、量刑等方面存在现实困境，导致难以针对人脸识别犯罪进行有效规制。

2人脸识别技术法律规制的预防行政属性

2.1 作为风险预防原则调整对象的人脸识别技术

风险预防原则虽起源于环境法领域，但随着社会上愈来愈多的风险不确定性和不可预测性出现，风险预防原则亦被用于处理这些风险。对人脸识别技术而言，法律面临着安全与利用价值的权衡，立法者面临着是否需从偏重后果规制至正视风险预防的规制理念与调控手段的转变。

2.2 人脸的二重属性

人脸是“生物性的通用标识符”，不可隐匿，易采集而不易更改，具有肖像和身份的双重属性。在《个人信息保护法》出台前，人脸图像首要便与肖像权相关。肖像权是非物质性人格权，亦是标表型人格权，其本质为一种“受尊重权”而非“支配权”，是一种消极权利而非积极权利，这决定了肖像权的保护往往只能发生在遭遇权益侵害型不当得利时。《民法典》第 1019 条进一步扩张了肖像权的保护范围，以丑化、污损的形式或者利用信息技术手段伪造他人肖像等行为都属于侵害他人肖像权。由此可知，除了肖像的商业化利用外，对于绝大多数普通人，通常只有在未经本人同意，对方以侮辱性、伪造等不法方式使用“人脸”时，才构成侵害肖像权的行为。人脸的第二重属性为个人的“身份”。人脸识别技术可实现高度精确性，通过对个人肤色、五官等相貌特征的识别，锁定个人身份。这里的身份强调的是社会身份而非自然身份。正如马克思所言，人是先在市民社会中生活，后才在政治国

家中生活。而人作为自然存在的个体，不是一蹴而就进入政治社会中的，这中间的一个环节是一个人成为社会意义上的人。个人的自然属性只有被“看见”、被“听见”，被他人“意识到”、被社会“考量”，才能体现个人在社会关系网络中的坐标位置。因此，相比于自然身份，强调将社会属性集合于人身的社会身份更具意义。那么，人脸识别起到身份认证的功能，成为激活各类社会身份与活动的钥匙。人脸识别不侧重于相貌的自然身份识别，而是重在识别的基础上进行社会身份分析，亦即将纯粹的身份识别转换为身份分析，分析个人在社会关系网中的所处位置。

2.3 人脸识别技术风险预防的行政权定位

对于如何防治人脸识别的危害，有两种应对方式：一种是传统的私法保护进路，等待已发生损害结果再去采取措施，提起侵权损害赔偿诉讼这一事后救济方式。另一种是通过一系列措施使人脸识别技术处于安全状态，对个人不产生影响，亦即风险的控制。人脸识别技术法律规制面临着如上的选择，本文认为，零风险的预防性原则并不适用于人脸识别技术。但是，从人脸识别技术的后果控制到风险预防是必然趋势，这亦是国家作为个人信息保护义务主体从被动走向主动的必由之路。

通过对人脸识别技术风险特征的分析可知，人脸识别技术的风险来源是与个人之间存在持续性不对称关系、对个人实施压迫性监视的权力，且此种权力的行使有着极大的安全性欠缺之可能。由于人脸识别技术的隐蔽性特征，监视与生活的界限并不明晰，当发现损害结果时，个体难以判断侵权发生的时间点、危害程度与后果，这决定了人脸识别技术侵权的私法保护进路存在困境。

3人脸识别技术刑法规制的具体路径

为切实保护好人脸识别信息、人身财产安全，同时为了促使人脸识别技术的向善发展，刑法作为最后的救济方式应当对人脸识别技术进行合理规制，把握好人脸识别信息保护和人脸识别技术发展之间的平衡。

3.1 明确刑法规制人脸识别的限度

对于人脸识别技术刑法规制的限度应当合理化，需要保持刑法规制的谦抑性，在确有必要的情况下进行合理规制。应当防止刑法过多介入人脸识别技术的发展，为人脸识别技术的发展人为制造不合理的框架；另一方面，当人脸识别技术的发展给人民的人身和财产造成重大影响时由刑法对其进行合理限度内的规制。

3.2 为民法和行政法预留空间

刑法应当保持谦抑性，在违法行为轻微的情况下刑法不应当介入，应当发挥民法和行政法的作用。对于通过人脸识别技术侵犯个人的人身、财产安全时，违法行为具有针对性，并且由个人信息处理者证明自己没有过错，属于过错推定责任原则，从而减轻受害人的举证责任。行政执法部门作为主管部门，对于违法使用人脸识别技术的企业具有监督管理职责，应当尽快建立完善的合规审计体系，对于违反法律规定，拒不改正的给予罚款等行政处罚。当违法行为严重，民法和行政法等法律部门难以提供有效救济的情况下，应当由刑法进行规制，在明确的入刑标准下，形成民法、行政法和刑法共同配合的规范体系。

3.3 明确刑法入罪标准

人脸识别信息属于敏感个人信息，相比较行踪轨迹信息、通信内容、征信信息和财产信息具有不可更改性、人身依附性等，对方的姓名、住址可能不得而知，但一看脸就能识别出对方的身份。而在陌生人社会中，即使能够获取姓名、住址等信息，往往也需结合人脸才能识别到特定的人。应当就人脸识别技术的入刑标准进行进一步明确的规定，就非法获取、出售、提供人脸识别信息的条数、违法所得数额、违法经营额等方面进行具体明确的规定。在这一过程中需要把握好限度，有学者提出将人脸识别信息的入罪条件设置为“非法获取、出售或者提供生物识别信息 5 条及以上”，这一解释属于对兜底条款的误用，不符合人脸识别技术规制的合理化限度，入罪标准较低。在其他罪名中，也应当将“情节严重”即关于人脸识别犯罪的入罪标准进行合理规定，根据人脸识别信息的重要程度并借鉴现有个人信息犯罪的相关规定，设定为 50 条以上较为合适。

3.4 明确个人信息范畴

为了扩展刑法规制的维度，在公民个人信息的范畴进行进一步解释，《刑法》第二百五十三条之一中规定的公民个人信息应明确包括人脸识别信息，不仅是作为生物识别信息进行规制，还应通过突出人脸识别信息对其进行更加明确的保护。人脸识别信息范围应当包括用于人脸识别的静态的图片和动态的视频以及已经经过分析处理的人脸识别特征。

结语

科学技术是把双刃剑，如火如荼的人脸识别技术也不例外。人脸识别产业行稳致远需要政府部门、科技企业、用户等各方共同参与，共建共治共享，促进人脸识别产业健康发展和数据安全应用，构建良性的应用生态。多方发力，深度参与人脸识别应用安全治理，将其可能带来的潜在风险降至最低，确保技术服务于人们的生产生活，为人们创造美好的生活提供技术保障，让技术应用方向始终向善向美。

[参考文献]

[1]肖军.人脸识别技术在追逃工作中的应用现状与展望[J]刑事技术 2016（2）：137－141