

# 人脸识别技术应用中的隐私伦理问题 及其消解路径

蒋福明, 曾慧平

(南华大学 马克思主义学院 湖南 衡阳 421001)

**摘 要:** 人脸识别技术是一种基于人的脸部特征进行身份识别的现代技术,这一技术极大地方便了人们的日常生活,但也带来了一些由知情同意缺乏和信息自主失效引发的隐私伦理问题。这些隐私问题在一定程度上侵犯了人类的尊严与自由。出现这一窘况的主要原因在于信息主体隐私保护意识薄弱、信息获取要求配合度低以及行业监管缺失与相关立法滞后。只有加强公民隐私保护方面的宣传教育、健全人脸识别隐私保护机制、完善人脸识别相关法律法规建设,才能有效消解人脸识别技术应用的隐私困境。

**关键词:** 人脸识别; 隐私伦理; 隐私困境; 知情同意; 信息自主

**DOI:** 10.16396/j.cnki.sxgskxb.2020.09.005

**中图分类号:** B82-057 **文献标识码:** A **文章编号:** 1008-6285(2020)09-0019-06

时代变迁,技术赋能。人脸识别技术作为新兴科技产物,给人们的生活带来了极大的便利,开启了人脸“技术识别”的新时代。然而,随着人脸识别技术在金融、公共安全、军事、教育、交通等领域的广泛应用,出现了企业、媒体、公共机构等对人脸的非法收集、滥用、泄露等问题,这给个人隐私安全和群体隐私安全带来了一定的隐患。

## 一、人脸识别技术应用中隐私伦理问题的表现

人脸识别技术(Face Recognition Technology)通常也叫人像识别或面部识别,是一种基于人的脸部特征进行身份识别的生物识别技术,即用摄像机或摄像头采集含有人脸的图像或视频流,并自动在图像中检测和跟踪人脸,进而对检测到的人脸进行脸部识别<sup>[1]</sup>。与其他身份识别技术相比,人脸识别技术具有自动记录、统计、成图及分析功能,因而其判别结果更精准、高效和便捷。也正因如此,在人脸识别技术面前人们变得愈发透明,每一个人的面部信息都可能被非法收集、恶意加工、恣意传递和散播。人脸识别技术的应用依托于人脸信息的获取、加工、储存、传播与使用,如果以人脸信息为媒介去窃取更多的他人隐私信息,用于敲诈勒索、非法经营、倒卖

牟利等行为,将会对人们造成严重伤害。并且,由于生物特征信息的敏感性、信息处理过程的复杂性、技术能效的有限性等因素的影响,人脸识别技术应用中的隐私伦理问题在影响范围或影响效果上都与一般的隐私问题不同。一些西方国家因担忧人脸识别技术对公民隐私和自由的损害,对该技术的应用持谨慎态度,甚至颁布了限制或者禁止人脸识别技术社会应用的法令。

隐私一般是指个人的、不愿他人知晓与干涉的私人事务。罗斯科·庞德(Roscoe Pound)曾指出:“隐私权是产生于今天越来越拥挤的社会生活条件下的一种现代性需要,……把纯属个人性事务中的有关私人问题予以公开是对人格权的伤害。”<sup>[2]</sup>从法律层面上看,“隐私权指自然人享有的私人生活安宁与私人信息依法受保护,不被非法侵扰、知悉、搜集、利用和公开的一种人格权”<sup>[3]</sup>。从伦理层面上看,它是个体享受私人事务被保护的一种权利,表达了对不伤害、自主自愿的伦理追求,是人类自由、尊严的表达,是人之为人的精神体现。无论是从道德层面还是从法律层面上看,隐私权作为人类生活的现代性需要,是基本的人格权利,应与人类其他基本权利一样受到尊重与保护。因此,指出并分析人脸识别技术应用中存在的隐私伦理问题,探索解决

收稿日期: 2020-05-27

基金项目: 湖南省研究生科研创新项目“人脸识别技术应用的伦理考量”(CX20200914)之阶段性成果。

作者简介: 蒋福明(1970—),男,湖南衡阳人,南华大学副教授,硕士,硕士生导师,从事伦理学研究。

曾慧平(1994—),女,湖南祁东人,南华大学硕士生,从事伦理学研究。

其隐私困境的有效路径,是当前事关人脸识别技术健康发展与社会和谐的紧迫任务。一般来说,人脸识别技术应用过程中存在的隐私伦理问题主要表现在知情同意缺乏和信息自主失控两个方面。

#### (一)“知情同意缺乏”侵犯意志自由

知情同意作为一项伦理原则诞生于医疗领域,最初主要用于保护病患的自主表达,现在已经成为生命伦理学的一项基本伦理准则,它体现了尊重、不伤害和公正等伦理精神。人类具有尊严,而尊严来自主体的意志自由,来自其自主选择的能力。中国传统伦理学推崇人的意志自由,孔子认为“三军可夺帅也,匹夫不可夺其志也”。他认为人有道德的自主自由性,并进一步提出“为仁由己,而由人乎哉”,其实质是肯定道德主体的意志自由、自主性。康德认为“只有当生命作为自主的可能性之条件时,才有尊严”。当代政治哲学家罗纳德·德沃金(Ronald Myles Dworkin)指出“即使国家实施改善公共设施、使其成员获得便利的举措,也不能对个人的权利进行干涉或侵入。”<sup>[4]</sup>因此,尊重人的尊严,就必然要尊重人的自主性,尊重人的意志自由。

随着社会发展,知情同意原则已延伸至各个领域。在当今信息时代,知情同意原则作为隐私保护的第一道防线,是当事人行为道德选择的前提与基础,是对人类尊严和人格利益维护的彰显。我国于2020年3月发布的最新版《信息安全技术 个人信息安全规范》(GB/T35273—2020,以下简称“规范”)在2017版的基础上对个人生物信息的收集与储存进行了完善与细化。规范指出“在收集个人信息时,应向个人信息主体告知收集、使用个人信息的目的、方式和范围,并获得信息主体的授权同意;在收集个人生物识别信息前,应单独向个人信息主体告知收集和使用个人生物识别信息的方式、范围、存储时间和目的等,并且征得个人信息主体的明示同意。”<sup>[5]</sup>

然而,在人脸识别技术应用中大量私自收集、加工、分析与使用个人信息的行为正在侵蚀公民的隐私权。当前,大多商用人脸识别在收集人脸信息时并未就其收集方式、范围、目的、存储时间等做任何告知,更遑论征求人脸主体的同意。日前,“中国人脸识别第一案”<sup>[6]</sup>的被告方杭州野生动物园就因使用人脸识别技术作为入园检测手段,被消费者以未提前告知与征得同意而私自收集人脸信息为由诉诸法庭,引发了多方关注。Facebook也曾面临未经同意而滥用伊利诺伊州人脸数据的350亿美元集体诉

讼案。在人脸识别技术应用过程中的人脸信息储存、使用等环节,信息控制者为减少支出或避免冲突,在很大程度上会忽视信息主体的知情同意诉求。此外,大数据时代网络数据的流转速度使得信息控制者在客观上也无法达到信息主体的“知情同意”要求。这些均使得信息主体的知情同意权处于被动状态。

#### (二)“信息自主失控”妨碍人的主体性

自古以来,关于“人是什么?”的问题一直是思想家们探究的核心,他们从不同维度论证了人的特征,直到现在,这一问题仍是哲学界探讨的热点。在前人研究成果的基础上,当代学者从新的角度对这一问题做出了回应。甘绍平认为人是一种二元存在,是文化精神和自然生物的统一体,从伦理学上看,人的本质就在于这种精神性的体现,而人的精神性首先体现为人的自由。换言之,人的自由、自主决定的能力是人之为人的本质体现<sup>[7]</sup>。所谓自由和自主就是当事人可以基于自身的决断来行事,做自己的主人,而不是受他人意志的驱使。在人脸识别技术应用生活化的今天,个人信息自主更应该成为隐私保护的重要举措。

然而,从2019年“ZAO—逢脸造戏”APP(以下简称ZAO)的AI换脸风波、利用人脸信息帮助无法完成账号实名认证的人群完成实名认证以获取非法利益的过脸产业,以及近期福建一银行APP人脸识别技术被破解等一系列事实来看,人脸识别技术的广泛与非理性应用严重侵扰了人们的信息自主。在人脸识别技术应用过程中,个人肖像的公开使得主体失去了对它的控制<sup>[8]</sup>,信息很可能被非法使用(这其中不仅仅包括人脸信息,亦可能包含其他的个人隐私,譬如家庭住址、行踪轨迹、通讯方式、财产信息、身份证号码、健康生理信息等个人敏感信息)。并且,在当前网络信息时代背景下,隐私信息经过上万次甚至千万次的传播与流转,信息主体对于自身信息所向何处、为谁所用、所用为何根本无法控制,个人信息自主完全没有保障。

另外,个体信息自主的损害与丧失不仅影响自身,对群体隐私利益也存在严重威胁。人脸识别技术的研发与使用离不开人脸数据库的支撑,但这些数据库中的人脸模型信息却不是信息主体能够掌控的。2019年有多起新闻报道了人脸数据泄密的问题,最引人注目的就是一家安防领域的人工智能企业的大规模数据泄露事件,该企业因内部数据库的安全防护缺失导致250余万公民个人信息数据被不

受限制访问。一种基于 DNA 的新的人脸识别方法将探针 DNA 图谱与已知的面部图谱数据库相匹配,可以从已知身份的 3D 面部形状中预测 DNA 信息,在验证模式下其实质性正确(83%~80%)超过错误(17%~20%)匹配<sup>[9]</sup>。如果群体成员中的核心或重要人物的 DNA 信息通过 3D 人脸图像被预测得知,其后果的严重性不言而喻。美国圣母大学的 Sheri A. Alpert 探讨了个体基因与其血亲基因和所在种群基因间的关系,并指出“在任何情况下,所有基因信息不仅与任何一个个体有关,而且与他(她)的血亲有关,还可能与他(她)所在的种群有关,任何群体中一小部分人的信息都可以(正确地或不正确地)包含该群体所有成员的信息。”<sup>[10]</sup>与基因信息同属生物信息的人脸信息不仅包含着单个个体生物特征,也包含了其所在群体的整体生物特征。如若数据库中的人脸图谱被作为预测群体基因信息的样本,那么,不管作为样本的那一小部分人的信息能否准确地预测群体基因,我们都应该重新考虑人脸识别技术应用对隐私的挑战与威胁,避免其成为基因武器。

综上所述,隐私权作为人权的组成部分,体现了人对基本权益的共同需求。而人权作为一种全球性、跨文化、跨民族的道德秩序,具有道德权利与法律权利的双重属性,是对人的根本利益的维护,是不同社会文化和社会生活方式的共同需求。保护隐私权在内的人权所表达的不伤害理念体现了道德规范的根本性内容。人脸识别技术对人类隐私的侵犯,导致对人类意志自由和信息自主的伤害,这足以体现人脸识别技术伦理问题的普遍性和严峻性。

## 二、人脸识别技术应用中隐私伦理问题的归因

产生人脸识别隐私困境的根源是多维度的,总的来说可以概括为信息主体隐私保护意识薄弱、信息获取配合度要求较低、行业监管缺失与相关立法滞后等三个方面。

### (一) 信息主体隐私保护意识薄弱

受社会发展和多元价值观的影响,人们的个人隐私观日益开放,个人可接受的隐私泄露底线逐渐向前推移,我们已进入到一个“弱隐私”时代。如今,通过各种网络途径向他人分享自己的生活、经历已成为人们日常生活与社交的一部分,而这些数据往往涉及个人隐私,如家庭住址、生活轨迹等,为隐私问题的滋长提供了土壤。这些信息是以数字化信息的形式存贮的,而数字化信息的特点是极易传播

和扩散。信息主体隐私保护意识薄弱,甚至忽视隐私泄露的风险,有可能导致大量的个人信息碎片被积聚、关联,形成完整的个人数字画像,最终将会暴露出个人的深度隐私。

人脸识别技术的生活化应用大大削弱了人们的隐私防护意识。国际权威调研机构市场洞察(Gen Market Insights)发布的《2018 年全球人脸识别设备市场研究报告》显示,近年来人脸识别设备市值不断攀升,预计其市值将会以 26.80%/年的速度增长,在 2025 年达到 71.7 亿美元,这充分显示了人脸识别行业旺盛的生命力。报告还指出,中国是人脸识别设备最大的消费区域,2017 年消费额占全球比例为 29.29%,2023 年将达到 44.59%,在 2018—2023 年复合年增长率为 29.53%<sup>[11]</sup>。当前我国真正地进入了“刷脸时代”,各大商场、酒店、车站、学校、小区等地都设有人脸识别,从日常进出小区、乘坐地铁、取快递,到线下支付、领养老金、身份审核等,人脸识别技术贯穿我们的衣食住行和娱乐消遣,成为日常生活的普遍形式。人们对于人脸信息被收集的行为也习以为常,并认为理所当然。个人隐私防护意识逐渐被这种“习以为常”和“理所当然”攻破,人脸信息等个人隐私被泄露、滥用的风险也在这种麻痹大意中悄然而至。

### (二) 信息获取配合度要求较低

传统的生物识别技术在提取特征信息过程中对信息主体的配合程度要求较高,否则可能导致无法获取特征信息或无法获得高质量特征信息,从而影响识别率。譬如,指纹识别在指纹提取过程中需要信息主体提供纹路清晰的手指并按要求移动手指以保证所采集指纹的完整性;虹膜识别则需要使用特定的机器对人的整个眼部进行拍摄,并且在特征提取过程中不能眨眼。

与传统的生物识别技术相比,人脸识别技术获取人脸特征信息的方式相对便捷。一方面,人脸识别技术特征信息提取配合度要求低。它不仅可以近距离获取人脸特征信息,也可通过摄像头或者遍布大街小巷的监控探头,在无需信息主体配合的情况下远距离抓取人脸生物特征而不被信息主体察觉。另一方面,星罗棋布的网络式监控是人脸识别技术获取或侵犯信息主体隐私的“抗辩理由”。巴拉巴西在其著作《爆发:大数据时代预见未来的新思维》中指出“我们正处于一种不断变化但却日趋精密的被监视状态中,……正是这些记录的存在引爆了个人隐私危机,而这一问题的严重性再怎么夸大也

不为过。”<sup>[12]</sup>

安全感一直是人类生存过程中所追寻的。随着时代的发展,安全防护技术大大提升,安全防护措施也更加严密。当今社会,监控已成为人类日常生活安全防护的常态,随处可见。然而,监控摄像给人们带来“安全感”的同时,也在一定程度上充当了人脸识别技术隐私风险的“加速器”。监控摄像大量地记录着人们的相貌特征、行为特征、生活轨迹等信息,尽管人脸识别时非接触性的无感收集已经简化了采集程序、降低了信息采集难度、加快了采集进度、减弱了对被采集者的配合要求,但其利用监控海量收集人脸信息,不仅增加了个人面部信息被非法采集的风险,在心理上也更容易使信息主体忽视其背后蕴藏的隐私风险。

### (三) 行业监管缺失与相关立法滞后

行业监管不力、标准参差不齐、数据安全防范不足,从而导致人脸信息泄露,这是人们抵触人脸识别技术大范围应用的重要原因之一。目前有关人脸识别技术的行业标准尚未成体系,仅存在一些对人脸识别技术中的部分技术的统一标准。在人脸识别技术商用过程中人脸信息的采集和保管全靠商家自律,因此,在人脸识别技术应用实践中保护人脸信息主体的信息安全存在诸多障碍。

相较于人脸识别技术进步与突破的速度,有关人脸识别技术应用以及人脸信息保护的立法明显出现滞后。当前涉及人脸信息隐私保护的窘境在于:对人脸识别技术的应用场景,人脸信息的采集、存储、使用环节以及权力归属还没有严格的法律限制。造成这种状况的原因有三:其一,面对巨大的使用人群、海量的数据信息以及多元的价值观念,建立一套完备的法律体系绝非易事;其二,高科技技术更新周期短,面对多变的立法诉求与瞬息万变的新问题、新情况,整合相关的法律规则与调整方案绝非一日之功;其三,我国的立法程序严格,一部成熟适用的法典必须经过反复斟酌与检验,不可不慎。

## 三、人脸识别技术应用中隐私伦理问题的消解路径

要维护人脸识别技术的良性运用,就要加强对公民隐私保护的宣传教育、完善人脸识别技术相关法律法规、健全人脸识别隐私保护伦理约束机制,以明晰技术与隐私的边界,缓解两者矛盾。

### (一) 加强隐私保护方面的宣传教育

人的行为一方面取决于自身情感机制的判定与

认知上的权衡,另一方面受社会文化因素的影响。就如同德性论的观点,最高的道德标准就是作为内在规范的道德品格。加强对公民隐私保护宣传教育的目的就在于利用情感、认知与行动之间的联动性,从个体的内部塑造其形态,在人的内心形成一个理性认知与习惯,继而外化于行,规范与引导自身的伦理实践。

信息主体的隐私观念淡薄是隐私问题产生的重要原因之一,要维护自身隐私不受侵犯还需依靠信息主体隐私安全防护意识的提升。人工智能时代的隐私风险呈现出与传统隐私风险相异的复杂性、多样性以及多变性,因此只有针对其表现特征的隐私保护措施才能行之有效。第一,加强潜在隐私风险教育。当前人们的生存、生活实践范围出现了跨越式的扩展和延伸,网络信息的发展、各项智能产品的发明拓宽了人们认识世界、改变世界的道路,同时也增加了隐私泄露的风险,譬如,非必要场合的人脸信息读取、网站注册中的详细个人信息填写、智能软件中的多种权限请求,等等。因此,在实际生活中,要认清各种行为背后潜藏的隐私风险,从源头杜绝个人隐私的泄露,对于有争议或不信任的软件,尽量做到少用或不用。第二,加强数据遗忘与数据销毁意识宣传。隐私信息的数据化是当今时代的一种常态,人们的生活轨迹、行为偏好等产生的信息都能以数字形式存储,若是被大量存储与整合,那后果将不可估量,因此数据销毁与遗忘十分必要。

### (二) 强化责任伦理意识培养

如今,人们在享受人脸识别技术带来的高效与便捷的同时,其带来的矛盾与冲突已慢慢成为人类生活的新常态。随着人脸识别技术对人们生活工作的深远影响,所引发的一系列问题已变成当今社会必须面对的问题,这也是人脸识别技术发展中不可回避的问题。在这个充斥着技术风险的时代,以塑造和培育人们责任意识为目的的责任伦理培养是应对人脸识别技术风险的有效策略。

首先,明确责任的主体维度及其责任分担是与人脸识别技术应用相关的隐私伦理研究中的一个重要问题。与传统单一的技术责任主体不同,现代技术责任主体已转变为类、群体等整体性主体,风险后果的承担也呈现出链条化、联动性的特征,形成一个利益共同体。在人脸识别技术使用过程中,商家、企业、社会都各自承担着不同的责任。譬如,企业在数据库的管理方面有制定严密管理措施、维护数据安全的责任;社会有承担建设安全、平等、可信、和谐的

数据环境的责任。各主体对自身行为责任的回应,不仅是对自身利益的维护,也是一种道德要求。

其次,在行为后果的责任承担时间维度方面我们应该树立一种前瞻性责任观。尤纳斯(Hans Jonas)的责任原则便是对这种后果特征的一种回应,他提出“每个人都应当有这样的行为,以便你的行为效果与地球上真实的人类生命的永久持存相适应。”他强调我们需要关注的不仅仅是当下行为后果的责任,更要关注该行为对未来影响的责任。在当今交流和联系日益紧密的社会共同体背景下,人脸识别技术带来的伦理风险在时间与空间上都显示出“广延性”的特征。因此,加强人们的前瞻性责任伦理意识培养,明确自身道德行为的责任后果,树立风险与利益相平衡的责任伦理观,是避免人脸识别技术的福音转化为威胁的道德呼吁。

### (三) 健全人脸识别技术隐私保护机制

首先,增加人脸识别技术设计阶段的伦理建构。从本质上看,人脸识别是携有不确定性风险的实践活动。并且,人脸识别技术已经不是纯粹单一的技术探索,而往往与企业、国家等利益群体间的博弈相关,其风险诱因也变得复杂。因此,为保障其更好地为人类服务,在尊重其发展规律的基础上,可在人脸识别技术设计阶段建构技术设计伦理原则,使之成为人脸识别技术的内在维度。譬如,不伤害、公正、尊重、审慎等。

其次,尝试建立人脸信息使用伦理审查系统。为数据库人脸信息集设置守门人,建立一个用于审查人脸数据集访问与使用的系统,以此保护数据库中人脸数据主体的安全与权益,进一步规范人脸信息的使用行为。系统主要关注请求者使用该数据的场合与目的,并要求数据使用者遵循数据使用的伦理合理性;如若隐瞒或者歪曲意图,则需要承担相关责任,譬如,失去数据库的访问与使用权限、赔偿巨额罚款等。这就使得你无论决定要做什么时,都把前因后果考虑进去。

最后,寻求与发展人脸识别新业态。尽管人脸识别技术已初具人类视觉的基本样态,但人类视觉功能的复杂性是单一的人脸识别技术无法比拟的。随着不断出现的新的需求与变化,人脸识别技术在精准识别中难以达到人们的理想目标,很可能出现错误识别的状况。在识别过程中,人脸识别技术不如人类视觉器官的最大原因就是人类大脑拥有比人脸数据库更全面的目标特征信息,它包含但不限于声音、体型、习惯等,人类视觉器官正是在这些基础

上进行识别判定。基于此,我们可以模仿人类大脑的功能,在人脸数据库的基础上增加其他特征的数据库,发展集人脸识别、声音识别、指纹识别等于一体的复合识别技术。当前,蚂蚁金服就是采用了复合型生物识别技术来保障客户的资金安全。

### (四) 完善人脸识别相关法律法规建设

技术效用能否顺利实现,技术的正向价值能否得到保证,不仅受技术应用主体素质限制,还取决于社会立法与规范等外部环境的影响。因此,规范技术的良性发展与应用、维护人的隐私与尊严,这个观念不能仅仅停留在人们的头脑中,而必须经过严谨的立法程序,使之成为整个社会必须遵循的行为规范,以及人脸识别技术正向价值得以实现的保障。

首先,设立人脸识别技术应用禁区。通过立法明确规定何以为可,何以为不可,避免侵入性过强的举措。遵循“必要且有限”原则,对信息采集的范围及所收集的人脸数据使用场景作出严格限制,以防止数据的滥用。

其次,高度重视人脸数据收集和使用的知情同意。2003年10月16日联合国教科文组织大会通过的《国际人类基因数据宣言》(International Declaration on Human Genetic Data)规定:获取人类遗传数据、蛋白质数据或活检数据,以及随后由公共或私人机构进行的处理、使用和保存,均应在缔约方自由、知情和明确同意的情况下进行<sup>[13]</sup>。对于人脸识别技术的使用,收集方应参照上述规定,在采集人脸信息前必须就相关信息与风险做明确充分的告知,确保被收集人的知情同意权。只有切实执行这些要求,才能维护人脸信息使用与个人隐私保护之间的平衡。

最后,明确相关主体的权责规定。第一,明确规定人脸识别技术应用者(商家、企业等)的权利与义务。相关企业与商家在经营过程中若需使用人脸识别技术应到相关部门申报,获得批准的商家与企业在不侵犯顾客权益的前提下有权对顾客使用人脸识别技术,但也应该承担妥善保管顾客人脸信息的责任,并承诺不得将所采集的人脸信息另作他用。第二,明确规定对商家与企业违规的处罚标准等,以此提高信息外泄成本,降低风险。欧盟《通用数据保护条例》(简称GDPR)在数据的控制者和处理者违规处理个人数据的后果方面就制定了严苛的惩罚标准:使用、销售和转让数据的企业,轻者处以罚款1000万欧元或前一年世界销售额的2%,重者处以罚款2000万欧元或前一年世界销售额的4%<sup>[14]</sup>。惩罚的目的是

敦促商家及企业妥善保管用户隐私信息。

人脸识别技术的良性发展不仅受制于公共政策和法律的协同治理,也受制于人类道德观念的提升。我们应该正确看待人脸识别技术与社会、人脸识别技术与人本身之间的关系,形成正确的、合理的科学技术社会观,在技术发展、个人隐私以及公共福祉三者之间寻求平衡,让人脸识别技术在安全、持续有序的语境下为人类服务。

#### 参考文献

- [1] 秦鸿,李泰峰,郭亨艺,等.人脸识别技术在图书馆的应用研究[J].大学图书馆学报,2018(6):49-54.
- [2] 庞德.法理学:第3卷[M].廖德宇,译.北京:法律出版社,2008:45.
- [3] 李正风,丛杭青,王前.工程伦理[M].北京:清华大学出版社,2016:255.
- [4] 德沃金.认真对待权利[M].北京:中国大百科全书出版社,1998:6.
- [5] 国家市场监督管理总局,国家标准化管理委员会.信息安全技术 个人信息安全规范:GB/T 35273—2020[S].北京:中国质检出版社,2020.
- [6] 毕玉谦,洪霄.民事诉讼生成权利规制探析:以“人脸识别第一

案”为切入点[J].法学杂志,2020(3):53-62.

- [7] 甘绍平.伦理学的当代建构[M].北京:中国发展出版社,2015:2-5.
- [8] 王俊秀.数字社会中的隐私重塑:以“人脸识别”为例[J].探索与争鸣,2020(2):86-90.
- [9] SERO D,ZAIDI A,LI J,et al. Facial recognition from DNA using face-to-DNA classifiers[J]. Nature Communications,2019(10):2557.
- [10] ALPERT S A. Protecting medical privacy: challenges in the age of genetic information[J]. Journal of Social Issues,2003(2):301-322.
- [11] GEN MARKET INSIGHTS. Global face recognition device market research report 2018[EB/OL]. [2020-03-26]. <https://genmarketinsights.com/report/global-face-recognition-device-market-research-report-2018/41637/>.
- [12] 巴拉巴西.爆发:大数据时代预见未来的新思维[M].马慧,译.北京:中国人民大学出版社,2012:8.
- [13] 刘宏恩.人群基因数据库法制问题之研究:国际上发展与台湾现况之评析[J].律师杂志,2004(303):71-94.
- [14] 张虹,熊澄宇.用户数据:作为隐私与作为资产?——个人数据保护的法律与伦理考量[J].编辑之友,2019(10):74-79.

[编辑 张红霞]

## Ethical Issues Relating to Privacy in the Application of Face Recognition Technology and Solutions

JIANG Fuming ZENG Huiping

(School of Marxism, University of South China, Hengyang 421001, China)

**Abstract:** Face recognition technology is a modern technology for identity recognition based on human facial features. It greatly facilitates people's daily life, but there still arise some ethical issues relating to privacy due to the lack of informed consent and autonomous failure of information, which violate dignity and freedom of human to a certain extent. The main reasons for the situation are the weak privacy awareness of information subjects, the low degree of coordination of information access requirements, the lack of industry supervision and the lagging of relevant legislation. As a result, only by strengthening the publicity and education of citizens' privacy protection, perfecting the privacy protection mechanism of face recognition, and improving the construction of laws and regulations related to face recognition, can we effectively resolve ethical dilemmas about privacy in the application of the technology.

**Key words:** face recognition; ethics of privacy; privacy dilemma; informed consent; information autonomy