

doi:10.16104/j.issn.1673-1883.2021.01.011

人脸识别技术的应用风险及其法律规制 ——以《个人信息保护法》的制定为契机

夏金莲

(贵州民族大学法学院, 贵州 贵阳 550025)

摘要:人脸识别技术通过对人脸图像进行特征提取、分类识别,从而达到身份鉴别的目的,其具有识别的自动性、自然性和风险防控的复杂性等特征。人脸识别技术应用场景众多,根据应用目的的不同,可以将其划分为基于公益目的的应用和基于私益目的的应用。人脸识别技术的应用具有侵犯个人隐私、贬损个人人格尊严、侵害个人财产权益等风险,法律规制无力是这些风险产生的主要原因。《个人信息保护法》的制定是治理人脸识别技术应用的良好契机,未来可以以《个人信息保护法》为基础,渐次推导出适用人脸识别技术的规范,明确人脸识别技术应用的法律原则以及使用者的义务,并区分不同应用场景下法律规制的重心。

关键词:人脸识别;应用场景;应用风险;《个人信息保护法》

中图分类号:D922.16 **文献标志码:**A **文章编号:**1673-1883(2021)01-0055-08

Risk in the Application of Face Recognition Technology and Its Legal Legislation: From the Perspective of the Enactment of the *Personal Information Protection Law*

XIA Jinlian

(Law School, Guizhou University for Nationalities, Guiyang, Guizhou 550025, China)

Abstract: Face recognition technology can serve the purpose of identification by extracting and classifying face images, which has the characteristics of automatic recognition, naturalness and complexity in risk prevention and control. This technology can be applied to many occasions. According to different purposes of application, it can be divided into the application for public welfare purpose and the application for private interest purpose. The application of face recognition technology bears the risks of infringing personal privacy, derogating personal dignity and infringing personal property rights and interests which haven't been effectively subjected to laws and regulations. The enactment of the *Personal Information Protection Law* is a good opportunity for better regulating the application of face recognition technology. In the future, based on the legal framework provided by the *Personal Information Protection Law*, we can gradually draw up the norms applicable to face recognition technology, clarify the legal principles of face recognition technology and the obligations of users, and shift to different legal focuses under different application scenarios.

Keywords: face recognition; application scenarios; application risk; *Personal Information Protection Law*

从一夜火遍社交网络又迅速没落的换脸软件 Zao,到人脸识别进入校园,再到“国内人脸识别第一案”,关于人脸识别技术的讨论在 2019 年集中爆发,并一直持续到现在。长时间的激烈讨论体现了公众对人脸识别技术的恐惧与担忧。人脸信息具有唯一性且难以改变,生活中为确保账户安全人们可以频繁更换密码,但若要频繁“换脸”却是难以实现的。人脸信息一旦发生泄露,就不仅仅只是隐私

泄露的问题,甚至还会给当事人的人身和财产安全带来不可估量的风险。但是科技不断向前发展是不可逆转的社会潮流,恐惧和担忧不该变成阻碍科技进步的理由,将人脸识别技术善加利用并施以有效引导和规制才是唯一正确的选择。遗憾的是,我国目前尚未出台专门规制人脸识别技术及其应用的法律法规,关于个人信息收集、使用和处理的规定散见于《民法典》《网络安全法》《消费者权益保护

收稿日期:2020-12-09

作者简介:夏金莲(1995-),女,贵州盘州人,硕士研究生,研究方向:宪法学与行政法学。

法》《刑法》等多部法律以及相关司法解释中,而且这些规定大都是原则性的,可操作性较弱。现行立法所呈现出的分散性和原则化不利于对人脸识别技术的规制。经过多年酝酿,2020年10月13日《个人信息保护法(草案)》终于在常委会第二十二次会议上迎来第一次审议,《个人信息保护法(草案)》为个人信息保护和个人信息处理构建了整体性的法律框架。人脸信息是个人信息的一种,《个人信息保护法》的制定将为人脸识别技术的法律规制提供相对具体的法源支持,但是人脸信息毕竟属于个人信息的下位概念,而且有其自身的特殊性,在适用《个人信息保护法》的过程中,还需结合特定主体和场景进行细化解,以符合“场景正义”。

一、人脸识别技术概述

(一) 人脸识别技术的概念

随着科学技术的发展,越来越多的生物特征识别技术被开发出来,如人脸识别、指纹识别、语音识别、虹膜识别等等。近年来,人脸识别越来越受到人们的重视,并且逐渐从众多生物特征识别技术中脱颖而出,大有占据自动检测识别技术首要位置的态势。何谓人脸识别?人脸识别技术的应用过程一般包括三个步骤:第一步是面部信息采集,即通过摄影、视频录像等方式获取自然人面部图像,并以此建立人脸数据库;第二步是特征提取,即利用计算机技术对数据库中的人脸进行分析,并通过一系列数字代码将面部特征信息表征出来;最后一步为身份识别,即将待识别人脸信息与数据库中的人脸特征进行对比分析,根据两者的相似度判别分类,从而达到身份确认或者身份查询的目的。综上所述,所谓的人脸识别技术可以理解为:通过机器对静态或视频中的人脸图像进行特征提取、分类识别,以达到身份鉴别的目的^[1]。

(二) 人脸识别技术的特征

与指纹识别、语音识别、虹膜识别等识别技术相比,人脸识别在应用上有其自身独特性,主要体现在:识别的自动性、自然性和风险防控的复杂性。

1. 识别的自动性。身份识别技术从密码验证发展到短信验证,再到生物特征识别技术,几乎每一种都需要被识别对象积极配合,主动进行相关操作,大多数生物特征识别技术也不例外。密码验证和短信验证需要手动输入密码和验证码,语音识别必须要发出语音才能进行声波识别,指纹识别需要用手指在识别器上进行按压或触摸以获取指纹的形状,虹膜识别则需要将眼睛准确对上识别器才能

实现精准识别。相比之下,人脸识别的自动性要高得多,其可以在被识别对象不与设备接触甚至无所察觉的情况下完成识别工作,整个过程无须被识别对象主动配合。

2. 识别的自然性。每一个自然人都有区别于其他个体的自然特征,比如面部特征、指纹特征、声音特征等,我们对某一个体与其他个人进行区分时所依据的就是这些自然特征。虽然人人都有五官,但是一眼望去却大不相同,因此区分不同个体的面部特征成为我们识别其他个体最直观、最自然的方式,我们辨别他人的第一感知就是通过眼睛的感官传递回大脑^[2],人脸识别技术正是应用了这一自然性原理。此外,人脸识别技术通过分析被识别对象的自然面部特征就可以达到识别和区分不同个体的目的,无须被识别对象再提供其他物体特征。因此,相较于其他的生物识别技术人脸识别技术在使用和体验上更加自然。

3. 风险防控的复杂性。在人脸识别技术的应用过程中,其引发的风险防控极为复杂。人脸识别技术的应用以大数据、云计算、人工智能等高端科学技术手段作为基础保障,在获取人脸信息后,信息控制者需要应用上述技术手段对所掌握的信息进行分析和处理,并在此基础上做出风险预判,从而确定应当采取的风险防控策略。但是在实际应用中,很多技术使用者的风险防控能力都不足,在信息储存和处理等环节,存在安全隐患和系统性技术风险。另外,人脸识别技术风险所具有的隐蔽性也加剧了对其防控的复杂度。如前所述,人脸识别技术的应用具有自动性,无须被识别对象的主动配合,这同时促使它具备了隐蔽性。近年来,大量的人脸信息被非法使用和贩卖,但是作为信息所有者的个人却对自身信息是在何种情况下被采集的毫不知情,这使得公众对人脸识别技术的风险防范变得极为困难。不得不说的是,在互联网时代下,信息传播具有速度快、范围广的特点,这使得对人脸识别技术风险进行防控的复杂度又进一层。

二、人脸识别技术应用的不同场景

结合物联网、大数据和人工智能等新兴科学技术,人脸识别技术在生活中的很多场景都有应用,为公权力机构、企业组织以及个人都提供了不少便利。对政府而言,人脸识别技术在维护公共安全和进行公共管理上有着不可替代的作用;对企业来说,人脸识别技术是研发、推广产品和服务的重要手段;对公众而言,人脸识别技术为日常活动提供

了许多便利。根据应用目的的不同,可以将人脸识别技术的应用场景分为基于公益目的的应用和基于私益目的的应用。

(一) 基于公益目的的应用

随着人脸识别技术日趋成熟,可操作性和便捷性逐渐增强,其被越来越多的公权力机构和公共事业性组织应用到日常的管理工作中,涉及的领域包括以下几种。

1. 罪犯追踪。由于人脸识别可以隐蔽操作,其在罪犯监控与抓逃工作中发挥着不可替代的作用^[3]。公安机关通过建立档案系统存储个人人脸信息,当以合法的手段获得犯罪嫌疑人照片或者面部特征信息时,将其与档案系统储存的原始信息进行比较,可以快速查找到犯罪嫌疑人。得益于人脸识别技术的应用,公安机关侦查案件的效率大幅提升。

2. 出入境识别。在机场出入境时,乘客在人脸识别门的机器上扫描机票后,机器将即时拍摄照片,并与乘客信息进行比较,确认是否为其本人。人脸识别自动门的应用,提高了边境工作人员的工作效率,同时也缩短了旅客在机场出入境的等待时间。

3. 治安防控。在治安防控工作中人脸识别技术应用较多的形式有两种,即视频监控系统 and 门禁系统。例如不少政府部门、银行、高等院校、图书馆、机场、火车站等公共服务机构和公共场所都会设有全天运作的视频监控系统,如果监控过程中发现异常情况或者可疑人员,就需要对其进行实时追踪和识别。又如在新冠疫情防控过程中流行起来的小区人脸识别门禁,为严格管控小区人口的出入,北京、武汉、成都等多地为小区装上人脸识别门禁系统,通过智能识别避免非小区人员随意进入并对本小区人员的进出进行监管,从而实现保护广大住户居住安全的目标。

4. 交通管制。如从2017年4月开始深圳市将人脸识别技术应用到对违法闯红灯行为的监管工作中,当十字路口出现闯红灯的车辆时,该技术将自动锁定行为人的信息,并将相关信息在十字路口的显示屏上予以公示,该技术的应用对制止公民违法闯红灯效果明显。

5. 涉及社会公益的其他领域,如人口管理、医疗卫生等。

(二) 基于私益目的的应用

除了公权力机构和公共事业性组织,越来越多

的企业也开始将人脸识别技术应用于日常经营活动中,市场营销、付款结账、休闲娱乐、身份认证等众多场景中不断被引入人脸识别技术。例如,中国两大巨头支付宝和微信都在其线上支付服务中推出了人脸识别,客户只需对准手机摄像头露出面部并做出眨眼、摇头等小动作就可顺利完成付款。而在线下支付市场中,支付宝和微信也相继推出“蜻蜓”和“青蛙”两款刷脸支付设备,并在众多城市部署。又如,总部位于印度的FaceX提供了目前最为先进的智能人脸识别系统,该系统通过实时捕捉入店客户的人脸来识别客户的年龄、性别、到店次数等信息,从而帮助零售商设计针对性广告以实现精准营销。再如,2019年陌陌公司推出的一款游戏软件Zao,客户只需要在该软件上上传一张符合要求的照片,就能即刻将自己替换成影视作品中的人物,由于可以帮助人们实现多年的“明星梦”,这款软件一经推出就吸引了大量用户。在身份认证领域,Android拥有一款被叫作Smart Lock的人脸识别应用程序,应用该程序用户只需将人脸贴近智能手机的屏幕就可以完成解锁手机的操作。除此之外,Apple为IOS设备开发的名为Face ID的安全登录系统也应用到人脸识别技术。

随着人脸识别技术的广泛应用,购物付款从现金支付、刷卡支付转向刷脸支付,手机解锁从密码、指纹解锁转向人脸识别智能解锁,人们也不再满足于繁杂又费时的手工修图,越来越偏向于选择省时省力的“一键美颜变妆”。对于商家和消费者个人而言人脸识别技术的商业化应用带来的似乎是一种双赢的局面,其在给企业带来低成本、高效率的同时,也为消费者提供了便捷、新奇的生活体验^[4]。

三、人脸识别技术的应用风险及其产生的原因

(一) 人脸识别技术的应用风险

1. 侵犯个人隐私

对人脸信息的收集极有可能造成对个人隐私的侵犯。根据《民法典》的规定,隐私是自然人的私人生活安宁和不愿为他人知晓的私密空间、私密活动、私密信息。我们每天出入各种场合,并且多数情况下并不对面部进行遮掩,因此从隐私定义的角度来看,人脸信息并不属于个人隐私的范畴。虽然人脸本身称不上隐私,但是利用数据挖掘、图像处理等科技手段,却可以从人脸信息中分析出个人的年龄、性别、种族、健康状况、情绪状况等多种隐私。此外,当特定的人脸与其出现的时间、空间相结合

时,也可能形成隐私^[5]。人脸识别技术的应用可能侵犯公民隐私权以及民主自由这是不少西方学者的观点^[6]。学者们有这样的观点不难理解,公民享有集会和公开讨论所持观点的权利是民主得以实现的基础,而该项权利的实现又依赖于公民的行动不受他人监视。然而,当人脸识别技术与互联网、人工智能大数据等科学技术结合时,政府却能够实现对任意地点任意个人的二十四小时的持续监视。强大的监控系统很大程度上改变了公众在公共场合的活动方式,并且在一定程度上阻碍了公众开展公开集会、抗议等民主活动。

在人脸识别技术被广泛应用的今天,公共场所的每一个角落都存在监控探头的踪影,虽然安装这些设备的目的是维护社会治安,保护公众的人身和财产安全。但是当公民信息被政府部门、企业组织等大量收集时,如果收集到的信息发生储存或使用不当的情况,公民隐私将面临巨大威胁。我们并不否定人脸识别带来的便捷和改变,但是人脸识别技术背后隐藏的风险也警示着我们它并不是百无一害。人脸信息一旦被泄露或盗取,那么公民的隐私将无所遁形。

2. 贬损个人人格尊严

人格尊严指作为一个“人”所应有的最起码的社会地位并且受到社会 and 他人最基本的尊重。人格尊严是人类最为重视的价值之一,有时人类对人格尊严的追求甚至超过对生命的追求。在法律规范中,人格尊严的价值也得到了认可和确定,我国《宪法》^①和《民法典》^②中都有相关规定。然而,在某些情况下,人脸识别技术的应用却直接侵犯到个人人格尊严。“脸”作为人身体的一部分,其生理层面的重要性不必言说,除开生理功能,“脸”还是一个人的名片,是人与人之间相互区别的重要标志,而且终生不可更改。正是由于个人面部所具有的唯一性和不变性,人们才可以轻易做到观其脸,知其人。不仅如此,“脸”还反映着一个人的内在精神,并与一定的稳定人格形成联系,或直接或间接的表征着一个人的人格^[7]。

目前我国个人信息收集以同意机制为基础,但是在现实中,很多人都是在不知风险或者迫于压力的情况下表示同意的。这样的同意虽然形式上符合法律的规定,但实质上却没有真正体现信息主体的自由意志,无论是哪种情况都是对知情同意原则的违反。在人脸识别技术盛行的时代,个人的人脸信息在被摄像镜头捕捉以后又被编写成一连串的数据和编码,最终用以识别身份的真伪,在这个过

程中,人脸信息已经沦为一种工具。在这样的事实之下,未获得信息主体真正知情同意的人脸识别应用更是对人格尊严的贬损,人脸所蕴藏的人格因素及其所承载的尊严价值被忽视甚至刻意抹去。人脸识别技术以新型技术作为分析手段,成功地将人脸所表征的独立人格转换成一系列的数字和编码,将活生生的人转化为一行行数据,此时,识别的是人脸,得到的是数据,失去的或被贬损的则是人的主体性及其尊严^[8]。随着人脸识别技术的广泛应用,公民人格尊严受损的程度将会继续加深,如人脸信息成为买卖的商品,据《光明日报》报道,在互联网平台上,花几元钱就能买到上千甚至上万张人脸照片^[9]。

3. 损害个人财产权益

人脸信息的收集和应用有可能给个人的财产安全带来巨大风险。“业主刷一下脸,房子就被过户”^③,这是 2020 年发生在广西南宁市的一起诈骗案件,在这起案件中诈骗分子就利用了人脸识别。房屋中介韦某某以房屋查档为由,要求当事人在“甞 e 登”App^④上进行刷脸认证,然而完成刷脸认证后房产却在当天被转移到买方名下,并被买家抵押给第三方。据报道,从 2020 年 6 月到 10 月,在韦某某以同样的方式实施的诈骗活动中,受害人超过 10 人,受骗总额超过 1 000 万元。

由于经济与数据之间存在天然的紧密关系,人脸识别技术被广泛地应用到经济活动中。目前腾讯微众银行应用人脸就可以为客户开户,支付宝、微信也开通了线上和线下的刷脸支付功能,越来越多的企业将人脸识别技术应用到日常业务办理中。无疑人脸识别在经济领域的应用为经济行业的发展造就了新推力,但是其给个人财产安全带来的风险也不容小觑。首先,人脸信息被银行、网络金融机构获取后,无法确保这些信息不被泄露,而且这些机构的网络安全设施、相关人员的网络安全意识和技术等也难以保障人脸信息长期处于安全状态,人脸信息一旦被非相关主体获取并使用,可能会对信息主体的账户安全造成巨大隐患。其次,随着科技发展,仿真头套、全息投影、人脸跟踪等高科技攻击手段不断涌现,人脸识别的攻击成本将不断降低,在线上不可控的环境中,不法分子将很容易伪造人脸视频通过身份认证。斯坦福大学的研究团队研发了一款名为 Face2Face 的人脸跟踪软件,通过摄像头拍摄用户的面部表情和动作后,可以应用这款软件促使视频中选定的物体做出与先前拍摄的完全相同的表情和动作,让人无从辨别真伪。

2020年10月,《楚天都市晚报》就报道了一起诈骗团伙通过人脸识别仿真,登录被害人微信进行转账的案件^⑤。案件中诈骗分子通过远程盗取受害人微信后,从微信里找出受害人的自拍照,利用软件做出眨眼、张嘴的动图通过人脸识别验证,从而顺利转走受害人在微信中绑定的银行卡里的钱。真伪鉴别手段与视频伪造技术始终是悬在人脸识别技术商业应用头上的“达摩克利斯之剑”^[10]。

(二) 人脸识别技术应用风险产生的法律原因

任意一项科学技术的普遍应用都需要社会管理者以法律规范的形式做出回应,一方面应该当通过法律规范对科学技术的合法性予以确认,确定技术价值的社会意义;另一方面还要应用法律规范对科学技术加以规制,防止出现技术滥用的现象。在这两个方面中,后者是法律回应科学技术应用的关键所在。法律规范应当最大限度地反映社会需要和愿望,保障公众的合法权益不受非法侵害。在面科学对科学技术这种利弊兼具的调整对象时,更应该规范其发展,将其可能对公众的人身、财产等权益带来的风险和损害降到最低。反观我国现行相关立法,其对人脸识别技术应用的规制力度明显存在不足。

2016年制定的《网络安全法》,虽然涉及个人信息保护,但也只是停留在个人信息这一层面上,并没有具体到个人信息的下位概念。新颁布的《民法典》在《网络安全法》的基础上更进一步,明确将生物识别信息纳入个人信息的范围之内。但令人遗憾的是,《民法典》并没有凸显生物识别信息的特殊性,也未对其进行特别保护。我国目前对于人脸信息等生物识别信息的专门规定主要体现在软法规范当中。2020年3月新修订的《信息安全技术个人信息安全规范》将生物识别信息与一般个人信息区分开来,将其划入个人敏感信息的范畴,并且对个人敏感信息规定了严于一般性个人信息的保护措施,比如传输和存储个人敏感信息时,应当采取必要的安全措施;个人生物识别信息应与个人身份信息分开储存;等等。除此之外,我国还出台了与人脸识别技术或生物特征识别信息的相关国家标准,如《公共安全人脸识别应用图像技术要求》《信息技术生物特征识别应用程序接口》。但是这些标准,包括《信息安全技术个人信息安全规范》均属于软法的范畴,其主要是对个人信息、使用和处理等行为提供指导,并无强制性,无法形成有效的约束力。

由此可以看出,目前我国关于个人信息保护的法律法规具有硬法和软法兼具的特征,但是硬法规定过于分散和笼统,无法形成系统的保护,也很难

对人脸识别技术的应用提供明确指引;而软法又因缺乏强制力,不论是对司法机关、还是人脸识别应用者来说其约束力都不强,这就导致了法律对人脸识别技术规制无力的现状。人脸识别技术应用所带来的侵犯个人隐私风险、贬损个人人格尊严、损害个人财产权益等风险,很大一部分原因即在于现行法律的规制无力。

四、人脸识别技术应用的法律规制

如何通过立法来防范人脸识别技术所带来的风险,或将成为未来个人信息保护领域的一个重要课题。2020年10月21日《个人信息保护法(草案)》在中国人大网公布,草案对个人信息保护进行了较为全面的规定,内容包括个人信息处理规则、个人在个人信息处理活动中的权利、个人信息处理者的义务等等。《个人信息保护法》意在为个人信息保护提供一个基本的制度框架,其战略高度决定了它无法做到面面俱到、细致入微,很多法律条文在具体应用中需要通过法规、规章的形式予以细化。人脸识别技术应用风险防范是个人信息保护的一个特殊领域,未来对人脸识别技术的规制应当以上位法——《个人信息保护法》为基础,渐次推导出适用于人脸识别技术的具体规范,明确人脸识别技术应用的法律原则以及技术使用者的义务,并区分不同应用场景中法律规制的重心,为规制人脸识别技术应用,防范其应用风险提供实际可行的法律指引。

(一) 明确人脸识别技术应用的法律原则

法律原则是历经长时间的发展和反复验证所形成的科学的法律规范,在相应领域内具有普遍指导意义。根据《个人信息保护法(草案)》的规定,处理个人信息应当采用合法、正当的方式,具有明确、合理的目的,并且应当限于事先处理目的的最小范围内,除法律规定的情形还应取得信息主体的同意。这是合法性原则、狭义比例原则和知情同意原则在个人信息保护领域的应用,是个人信息利用的安全底线。人脸信息作为个人信息的下位概念,在对其利用的过程中理应遵循上述原则。但是《个人信息保护法》属于狭义的法律,条文规定较为笼统,为增强其可操作性,在对人脸人别技术进行规制的过程中还需将其具体化。

第一,人脸识别技术的应用应当符合合法性原则。在基于公益目的应用中,审查技术使用者的行为是否合法应根据宪法和法律的相关规定,从内容

和程序两个方面进行。在内容上主要考察不同主体是否在法定职权和职责范围内应用人脸识别技术,如考察应用对象是否属于管辖范围和权限;在程序方面,公权力机构和公共事业性组织应当依照相关法律法规规定的程序实施应用行为,不同的应用场景可能有不同的程序标准,但基本要求是要符合法定程序。在基于私益目的的应用中,技术应用者与信息主体双方为平等主体,人脸识别技术的应用必须以双方的真实意思表示为基础,而且不得违反法律规定,损害公共利益和他人合法权益。

第二,人脸识别技术的应用应当遵循知情同意原则。知情同意原则旨在维护个人自主性,体现了对公民个人信息自决的尊重。^[11]通过确立知情同意原则,可以有效防范对人脸信息的滥用。在知情同意原则框架下,任何主体收集、利用和处理人脸信息都应当将收集目的、使用范围、存储期限、救济途径等内容告知信息主体,并取得信息主体的同意。为避免知情同意原则流于形式,应当规定告知书应当以书面的形式作出,并且应当以合理的方式让信息主体从实质上知晓同意书的内容和如果同意可能存在的风险;此外,还应规定信息主体的同意须以明示的方式作出,即信息主体应当明确表示同意对方收集、使用、处理自身人脸信息,单纯的沉默不能推定为同意,同时还应允许数据主体随时行使撤销权。

第三,人脸识别技术的应用应符合狭义比例原则。狭义比例原则表达了一种适度、均衡的理念和思想^[12],其强调通过考量手段与目的之间的关系来实现伤害最小化、利益最大化。在人脸识别技术应用中,狭义比例原则要求使用者必须仔细考量下列问题:人脸识别技术的运用是否是必需的?应用人脸识别技术所获取的利益是否大于公众因此而遭受的损害值?在确实无法避免危害结果发生时,应当如何将损害降低到最小?比例原则是信息保护的具化标准,也是实现价值多元和利益平衡的重要手段。当前人脸识别技术尚有不成熟之处,在应用过程中存在诸多不确定的风险,在这样的现实之下既要风险防范,又要实现效益获取,以狭义比例原则作为价值指引,显得尤为重要。

(二) 明确人脸识别技术使用者的义务

目前的个人信息收集遵循知情同意原则,在该框架下,信息主体一旦表示同意,随后的信息收集、使用、处理就完全交给了信息控制者,信息主体无法参与后续环节也难以进行监督。而且,只要在收集信息前征得同意,之后所有环节的风险将大部分

转由信息主体承担。实际上这是极不公平的,因为在人脸识别技术的应用中,最大的获益者是技术的使用者,与技术使用者相比,信息主体获得的利益是微不足道的,在一项科学技术的应用过程中让明显获利较少的一方承受较大的风险显然不符合公平的法治理念。此外,如前文所述,由于信息主体的同意多是在不了解情况和不得已的情况下做出的,以同意机制对人脸识别技术应用进行规制更显得无力。因此,对滥用人脸信息行为的规制,在强调信息主体理性的同时,也应该关注技术使用者的义务配置,这样既能平衡信息主体与技术使用者之间存在的 unfair 现象,同时也能倒逼技术使用者自觉保护自身所掌握的人脸信息。

《个人信息保护法(草案)》以专章的形式对个人信息处理者的义务做出规定,个人信息处理者负有采取必要措施保障个人信息安全、信息发生泄露时立即采取补救措施等义务。对于人脸识别技术使用者义务的具体设定,在不违反我国《个人信息保护法》的前提下,可以借鉴经济合作发展组织的《隐私保护和个人数据跨境流动指南》规定的责任原则,通过法律授权个人信息的监管者制定相应的规则,规定数据控制者在使用、储存人脸信息的过程中应当履行的义务、采取的安全措施以及不履行相关义务应当承担的法律责任。如规定信息控制者应当制定人脸信息保存、安全管理等方面的管理制度和操作规程,明确岗位职责,完善内控制度,保障人脸信息的安全。在法律责任设置上不妨严厉一些,只要技术应用者未履行法定义务,就应当承担相应的法律责任,即使未对人脸信息主体造成不利后果。明确的规则下,技术应用者为了更好地维护自身权益将会严格遵循法律的规定,采取相关措施,保障人脸信息免受泄露或被无关主体随意利用。通过这样的制度设计,可以确保人脸信息的安全性,且符合公共利益和公序良俗。

(三) 区分不同应用场景下法律规制的重心

如前所述,根据人脸识别技术应用范围的不同,可划分为基于公益目的的应用和基于私益目的的应用,不同场景下的应用,法律规制的重点应该有所侧重。对基于公益目的的人脸识别技术应用应当以事前规制为重点,这是因为在基于公益目的的应用中,个人利益必须忍受重大公共利益的限制,个人对于人脸技术的应用一般没有拒绝的权利,一旦法律赋予公权力机构或者公共事业性组织应用人脸识别技术的权利,公众就必须得接受这一事实。为了防止人脸识别技术被滥用,损害公民权

益,必须对公权力机构和公共事业性组织应用人脸识别技术进行严格把关。因此,对于基于公益目的的人脸识别技术应用应当将规制的重心放在技术应用前的审批流程上。也就是说对于公权力机构和公共事业性组织使用人脸识别技术应当设置事前审批制度,有权机构应对申请主体的使用目的、范围、必要性等事项进行严格审查,对于符合条件的申请单位应当予以批准使用,任何公权力机构、公共事业性组织未经有权机构批准同意,不得使用人脸识别技术。

基于私益目的的人脸识别技术应用应以事后规制为主。与基于公益目的的应用不同,在基于私益目的的应用中,个人与企业组织之间属于平等主体关系,企业能否对某一个人使用人脸识别技术由双方自主协商决定,如果个人认为人脸识别技术的应用可能对自身带来不利后果,可以拒绝。在个人对人脸识别技术的应用有自主决定权的情况下再设置事前审批意义并不大。此外,如果企业等私主体使用人脸识别技术也需要获得有关机关批准,可能会给企业造成极大的负担,而且极有可能会遏制科技的创新和发展。为激发企业活力,促进科技创新,不宜对企业组织应用人脸识别技术设置过高门槛。对基于私益目的的人脸识别技术应用的规制可以将重心放在事后的追责上,通过设置严格的问责制度倒逼企业组织遵守相关法律规定,从而规避人脸识别技术应用可能产生的风险。当然,事后规制需以健全的法律责任制作为基础,只有法律明确规定企业组织违反相关法律规定应用人脸识别技术应当承担的法律责任,执法部门才能通过事后追

责进行有力监督,也只有这样受害人才可以通过事后的民事诉讼依法维权。

需要说明的是,不论是基于公益目的的应用还是基于私益目的的应用,事中的监督都是不可或缺的,政府有关部门应当切实履行监督义务,对于在应用人脸识别技术过程中有违法行为的主体,应该及时查处。公众如果发现相关主体有违法违规行为,或者自身权益已经遭受侵害的,应积极投诉、举报或者提起诉讼。公众监督对规制人脸识别技术的应用起着重要作用,为鼓励公众积极参与监督,可以采取一定措施,如对主动投诉、举报者予以表扬或奖励等。

五、结语

科学技术的应用并非只有益处,利弊共存是所有科学技术都具有的特性,人脸识别技术作为尖端科技的一种,与其他科学技术一样充满了不确定性风险,然而一项技术的产生究竟是会造福人类还是会祸害百姓并不取决于技术本身,而在于我们自己如何应用。面对人脸识别技术的迅速普及,我们要保持包容开放的态度,同时也要积极防范其可能带来的风险。人脸信息具有唯一、不可改变的特点,并且表征着个人的人格,我们应当对其谨慎应用。《个人信息保护法》的制定是治理人脸识别技术应用的良好契机,未来对人脸识别技术的应用进行治理时,应当对《个人信息保护法》的相关规定进一步细化,制定相应的法规、规章,明确人脸识别技术应用的法律原则、使用者的义务,并区分不同应用场景中法律规制的重心。

注释:

- ① 《中华人民共和国宪法》第38条:“中华人民共和国公民的人格尊严不受侵犯。禁止用任何方法对公民进行侮辱、诽谤和诬告陷害”。
- ② 《中华人民共和国民法典》第109条规定:“自然人的人身自由、人格尊严受法律保护”。
- ③ 细思极恐! 业主毫不知情,仅刷一下脸,房子就被过户[EB/OL]. [2020-12-10]. <http://m.people.cn/n4/2020/1210/c676-14616414.html>
- ④ “邕e登”App是一款面向南宁市的不动产登记综合服务平台,通过该平台用户可以随时了解各种不动产相关资讯以及政策信息,同时还可以直接通过手机在线进行查询、登记等一系列业务办理。
- ⑤ 人脸识别被破解,登录微信就能转账,诈骗团伙将照片做成能眨眼的小动图[EB/OL]. (2020-12-07) [2020-12-08]. <http://wx.qq.com/cmsid20201017A01X1300? f=newdc>.

参考文献:

- [1] 徐竞泽,吴作宏,徐岩,等.融合PCA、LDA和SVM算法的人脸识别[J].计算机工程与应用,2019(18):34.
- [2] 蒋福明,曾慧平.人脸识别技术应用中的隐私伦理问题及其消解路径[J].山西高等学校社会科学学报,2020(9):19.
- [3] 司绍寒.人脸识别技术在司法行政领域的应用前景[J].犯罪与改造研究,2019(3):58.
- [4] 李国鑫.人脸识别技术的发展与应用[J].科技传播,2018,10(19):102-103.
- [5] 郭春镇.数字人权时代人脸识别技术应用的治理[J].现代法学,2020(4):24.
- [6] 洪延青.人脸识别技术的法律规制研究初探[J].中国信息安全 2019(8):86.

- [7] 徐艳东.“脸”的道德形而上学——阿甘本哲学中“脸、人、物”思想研究,哲学动态,2015(2):16.
- [8] 郭春镇.数字人权时代人脸识别技术应用的治理[J].现代法学,2020(4):27.
- [9] 张焱.为便利让渡个人隐私存在安全隐患[N].光明日报,2019-11-20(002).
- [10] 商希真.生物特征识别信息商业应用的中国立场与制度进路——鉴于欧美法律模式的比较评价[J].江西社会科学,2020(2):207.
- [11] 田野.大数据时代知情同意原则的困境与出路——以生物资料库的个人信息保护为例[J].法制与社会发展,2018(6):111.
- [12] 郑晓剑.比例原则在现代民法体系中的地位[J].法律科学,2017(6):101.

(上接第 54 页)

- ⑦ 克智:是彝族民间流传相当广泛、具有竞赛性质的口头文学形式。其内容涵盖天文地理、古今历史,用语朴实、生动活泼、感染力强。

参考文献:

- [1] 王俊青.两汉的移风易俗[J].黑龙江史志,2010(23).
- [2] 高寿仙.洪武时期的社会教育与移风易俗[J].明史研究,1999(1).
- [3] 王岚.凉山形象扶贫——一场移风易俗的革命[J].西南民族学院学报.哲学社会科学版,1998,19(S1).
- [4] 习近平.在中央扶贫开发工作会议上的讲话[M]//十八大以来重要文献选编.中央文献出版社,2018:37.
- [5] 陈寒非.风俗与法律:村规民约促进移风易俗的方式与逻辑[J].学术交流,2017(5):108-117.