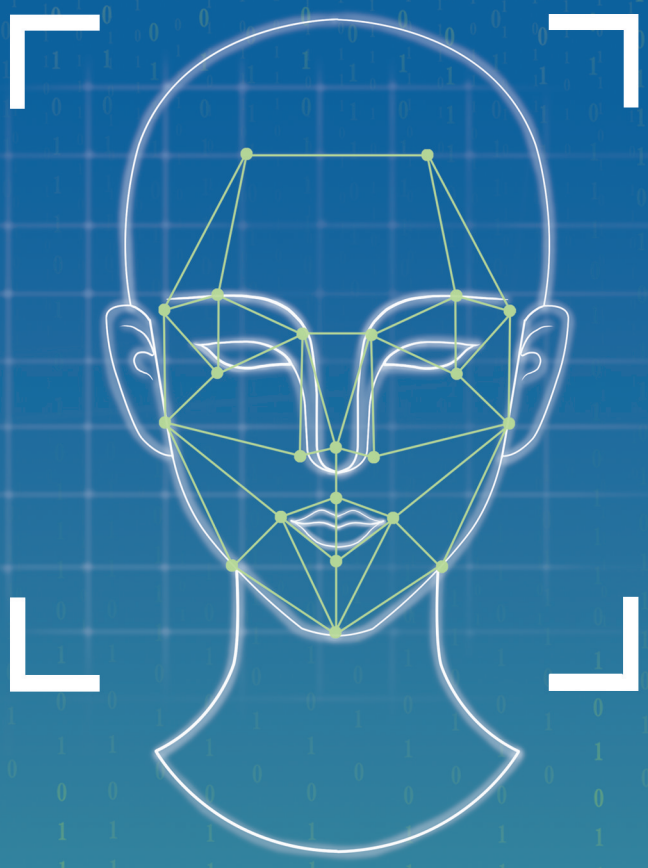
日前,国家互联网信息办公室、公安部联合公布的《人脸识别技术应用安全管理办法》(以下简称《办法》)将于今年6月1日起施行。在个人信息保护法、网络安全法、数据安全法已构建起我国数据安全与个人信息保护基本框架的同时,《办法》的出台填补了相关法律空白,针对人脸识别技术的应用也提出了系统性的规范指引。近日,新快报记者与法律界人士对话,共同探讨《办法》的亮点以及给普通百姓生活带来的改变。

■采写:新快报记者 毛毛雨 高京 通讯员 广互宣

新规明确:6月起你有权拒绝刷脸!

《人脸识别技术应用安全管理办法》三大亮点保障、保护个人隐私



亮点1 不强制

人脸识别需取得个人同意

随着计算机视觉技术和深度学习算法的优化,以人脸识别技术为代表的人工智能有了飞速的发展,但是有关"人脸识别"的争议也从未停止。

在广州互联网法院综合审判三庭的王蕾法官看来,人脸因其独特的生物特征和可直接识别性,属于最重要的个人敏感信息之一。一旦被泄露或滥用,会对个人人身和财产安全造成极大危害。

在王蕾看来,《办法》的亮点之一就是重申了"单独同意"原则,强调基于个人同意处理人脸信息的,需在个人充分知情的前提下获得自愿、明确的同意。同样,《办法》提供了场景化指引,允许个人拒绝刷脸,但个人需提供其他验证方式,明确"自主选择权"边界。如此一来,既避免"一刀切"影响数字化服务,又推动技术在"安全与效率"两方面平衡发展。

浙江恒霁律师事务所律师卢琼认为,《办法》体现了对个人意愿的尊重,避免在未经个人明确同意的情况下擅自使用人脸信息,与《个人信息保护法》处理敏感个人信息需要取得单独同意相一致。

在未成年人层面,《办法》对人脸数据设置更高保护标准:基于个人同意处理不满十四周岁未成年人人脸信息的,应当取得未成年人的父母或者其他监护人的同意。

对此,汉盛律师事务所高级合伙人李旻表示,未成年人认知和判断能力有限,更易受到误导、侵害,信息易泄露、被滥用,对其特殊保护体现了立法的人文关怀。

亮点2 需告知

人脸识别须有显著提示标识

《办法》对公共场所安装人脸识别设备作了规定,其核心就是,设备应当为维护公共安全所必需,依法合理确定人脸信息采集区域,并设置显著提示标识。

除法律、行政法规规定可以不向个人告知的以外,应用人脸识别技术处理人脸信息前,应当真实、准确、完整地向个人告知信息处理者的名称和联系方式,包括处理目的、方式及人脸信息保存期限等内容。

北京浩天(广州)律师事务所合伙人张万隆表示,当消费者在线支付、会员注册时会碰到需要验证的情况,消费者有权选择其他验证方式,从而避开人脸识别。同样,当消费者在酒店办理入住涉及刷脸验证,若有验证方式,商家不得强制刷脸,消费者也有权拒绝刷脸。

那么,一些小区物业、企业安装了人脸识别的门禁或者打卡系统,如何判断是否违规?李旻认为,首先要考虑设备安装前是否向居民或员工充分告知并取得明确同意,其次设备是否遵循必要性,是否将人脸识别作为唯一验证方式。物业应允许住户选择门禁卡、密码等,公司应提供指纹打卡、纸质签到等方式。若拒绝提供,则存在违规风险。最重要的是,要查看物业或企业是否对信息进行加密存储、是否限制了信息的访问权限等。

卢琼提到,市面上有一些App以"不同意刷脸就无法使用服务"要求进行人脸识别,这种模式使人无法单独对人脸信息作出自愿同意。App这种强制索取非必要个人信息的行为,属于违法违规。一旦遇到,可以向网信部门、公安机关或者12345热线投诉举报。

VCG/图

■腾讯元宝AI生成

小区刷脸系统违规吗?

小区物业安装了人脸识别的门禁或者打卡系统,应向居民充分告知并取得明确同意。其次物业应允许住户选择门禁卡、密码等方式开门。若拒绝提供其他方式,则存在违规风险。

亮点3 防私密

情节严重 最高可判7年有期徒刑

《办法》明确规定,任何组织和个人不得在宾馆客房、公共浴室、公共更衣室、公共卫生间等公共场所中的私密空间内部安装人脸识别设备。人脸识别技术应用系统也应当采取数据加密、安全审计等措施保护人脸信息安全。

对此王蕾分析,新规对人脸识别技术的应用场景提出了原则性要求,也给技术发展保留空间。在验证个人身份方面,鼓励优先使用国家人口基础信息库、国家网络身份认证公共服务等渠道,减少对人脸信息的收集和存储,针对人脸识别技术在生活中的典型应用场景,提供了清晰具体的操作指南。

随着"AI"换脸技术使用日益广泛,也将涉及人脸数据处理,生成或替换的人脸图像常用于视频编辑、娱乐等,也有不法分子利用"AI换脸"制作虚假视频,实施网络诈骗。卢琼认为,新规将推动AI换脸技术在合法、安全的框架内发展,保护公众利益。

《办法》要求处理人脸信息应遵循特定目的、充分必要及对个人权益影响最小原则,且实施严格保护措施,这确保了"AI换脸"技术在合法合规框架内应用,防止过度收集和滥用信息,降低人脸信息被窃取、篡改的风险,也避免因强制刷脸带来的信息泄露风险。

另外,《办法》还要求商业机构需要建立数据安全管理制度,并可能面临备案要求。如果处理人脸信息达到一定规模(超过10万人),需向相关监管部门备案。

值得注意的是,根据不同的违规情节,企业将面临民事、行政、刑事三方面处罚。卢琼表示,窃取"人脸信息"情节严重的,构成"侵犯公民个人信息罪",相关负责人将会被依法追究刑事责任,最高可被判7年有期徒刑。

典型案例

制作虚假人脸视频获利 支付赔偿金+公开道歉!

从2020年9月开始,郑某利用某即时通信软件组建群组。任某、戴某、陈某通过上述群组先后向郑某购买公民个人信息,制作虚假人脸动态识别视频,用于解封账号、验证App的实名认证,从中非法获利。

据悉,四被告自认非法处理个人信息2000余条,违法所得103000余元。其间,四被告利用某软件阅后即焚功能删除大量信息和交易记录,受害人数量、身份、信息去向、用途均无法核实。

另外,郑某、任某、戴某、陈某已经生效刑事判决书认定构成侵犯公民个人信息罪。

2022年1月,广州市越秀区人民检察院以郑某等4人行为侵害社会公共利益,依法向广州互联网法院提起个人信息保护民事公益诉讼。

裁判结果:四被告注销用于侵权的互联网账号、解散或退出用于传授犯罪方法的通信群组;向法院支付公益损害赔偿金13000元-30000元不等;四被告在省级以上媒体或具有同等影响力的互联网媒体上公开发表经法院认可的赔礼道歉声明。在本判决生效之日起一年内,通过与个人信息保护相关的警示教育、公益宣传、志愿服务等方式进行行为补偿。