

“人脸识别”入法 “颜面何存”无忧

“刷脸”解锁、“刷脸”支付、“刷脸”进小区、“刷脸”入景区……近年来,生活中的“刷脸”应用越来越常见。但人脸识别技术在便利人们生活的同时,也带来不少问题。8月8日,国家网信办就《人脸识别技术应用安全管理规定(试行)(征求意见稿)》(以下简称“意见稿”)公开征求意见,引发广泛关注。它一旦开始实施,真的能保护我们的这张脸吗?将会带来哪些改变?

数读人脸识别

●2021年,我国人脸识别市场规模为**56亿元**,按照现在年均超过**20%**的增速,预计到2024年市场规模将突破**100亿元**,10年内市场规模有望达到**千亿元**级。

●全国信息安全标准化技术委员会等机构发布的《人脸识别应用公众调研报告》显示,在两万多名受访者中,**94.07%**的人表示用过人脸识别技术,**64.39%**的人认为人脸识别技术有被滥用的趋势,**30.86%**的人表示已经因为人脸信息泄露、滥用等遭受损失或者隐私被侵犯。

使用泛滥遭到严监管

随着人脸识别毫无节制地泛滥,其应用范围问题也不断被推上舆论的风口浪尖。近年来,欧美多地针对人脸识别技术出台禁令,而国内也逐渐显示出“严监管”信号。

例如,英国信息专员办公室(ICO)就曾对一家名为Clearview AI的美国公司发出警告,该公司通过Facebook等社交网络或其他网络公开平台收集了大量英国公民的人脸照片,而且这些照片可能是在人们不知情的情况下获取的,已“涉嫌严重违反”该国的数据保护法。

根据Clearview AI官网信息,该公司创建了有着超过100亿张图片的人脸数据库,主要服务于警察局等执法机构。据相关媒体报道,一些英国警察曾试用该公司提供的服务,但目前这一做法已经停止。

此次意见稿对于人脸识别的“大数据杀熟”和“过度标签化”等滥用的可能,可以起到一定的遏制作用。例如,2021年“3·15”晚会曝光了多家知名企业的线下门店,安装一款名为“万店掌”的摄像头,非法抓取客户人脸信息进行标记。客人一旦去了A

店,再光顾B店,就绝对不会得到比A店低的价格,也就是大家都很熟悉的“大数据杀熟”。这样对人脸信息的使用明显侵害了当事人的权利,而类似这种“大数据杀熟”从线上到线下都如此普遍。

又如,有超市在出入口安装的摄像头,会通过人脸比对,为部分消费者打上“疑似小偷”的标签,有“可疑人员”到来会自动报警。这不仅涉及过度标签化,也有隐性歧视的成分,而且,这种在当事人不知情的情况下做出的人脸信息采集和过度分析,明显侵害了当事人的权益。

为此,意见稿首次提出了针对远距离、无感式人脸识别技术的场景使用规范,明确在公共场所、经营场所使用人脸识别技术远距离、无感式辨识特定自然人,应当为维护国家安全、公共安全或者为紧急情况下保护自然人生命健康和财产安全所必需,并由个人或者利害关系人主动提出。也就是说,这种在当事人不知情的情况下采集人脸信息并进行“分析”的行为,都将被禁止。

会否冲击刷脸支付?

众所周知,科技公司是最早劝说用户使用刷脸技术的一批人。自从苹果公司首度在全球范围内发布了成熟的人脸识别“刷手机”之后,支付宝、微信等小消费型科技公司纷纷开通了刷脸支付的功能。

那么,对于这份即将出台的指导文件,会否冲击刷脸支付?

8月8日,接近微信官方的知情人士表示,新规对其影响不大。目前大平台使用的人脸识别技术,其后台都是通过

公安系统调用的,自身并不会存储用户的面部数据。

“至于要求刷脸必须征求用户同意。大公司在开通刷脸支付的时候,也都是会获得用户同意的。”该人士表示。

专家对此分析,从行业角度看,新规对于支付宝、微信、网贷公司等没有太大影响,因为这套规则实际上之前已经开始运行,很多互联网企业已经完成了用户同意授权,也给出了其他的认证方式,技术上并没有实质性的困难。当然,人脸识别技术使用者不得保存人脸原始资料这一点,可能会要求未来一些互联网公司在认证人脸的时候对接政府部门的人像识别库,这也是一个技术上的小对接。

04

●目前,人脸识别技术不规范应用主要集中在3个领域:
一是商场、健身房、景区等商业场景的应用;
二是以居民小区、写字楼等为主物业门禁系统的应用;
三是部分线上平台或者应用软件,通过拒绝使用软件的方式强制索取用户人脸信息。

最少使用

征求意见稿提出,只有在具有特定的目的和充分的必要性,并采取严格保护措施的情形下,方可使用人脸识别技术处理人脸信息。实现相同目的或者达到同等业务要求,存在其他非生物特征识别技术方案的,应当优先选择非生物特征识别技术方案。使用人脸识别技术验证个人身份、辨识特定自然人的,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权威渠道。

遵循自愿

征求意见稿要求,使用人脸识别技术处理人脸信息应当取得个人的单独同意或者依法取得书面同意。法律、行政法规规定不需取得个人同意的除外。个人自愿选择使用人脸识别技术验证个人身份的,应当确保个人充分知情并在个人主动参与的情况下进行,验证过程中应当以清晰易懂的语音或者文字等方式即时明确提示身份验证的目的。

最小存储

征求意见稿指出,除法定条件或者取得个人单独同意外,人脸识别技术使用者不得保存人脸原始图像、图片、视频,经过匿名化处理的人脸信息除外。使用人脸识别技术处理人脸信息应当尽量避免采集与提供服务无关的人脸信息,无法避免的,应当及时删除或者进行匿名化处理。

物业强制要求“刷脸”进入 业主可否拒绝?

案例:张女士所在小区要求所有业主前往物业完成人脸信息采集,并告知业主通过人脸识别进入小区将成为唯一进入方式,如不配合采集和录入工作,将无法进入小区。

解读:《最高人民法院关于审理使用人脸识别技术处理个人信息相关民事案件适用法律若干问题的规定》(以下简称《规定》)第10条第1款载明:“物业服务企业或者其他建筑物管理人以人脸识

别作为业主或者物业使用人出入物业服务区域的唯一验证方式,不同意的业主或者物业使用人请求其提供其他合理验证方式的,人民法院依法予以支持。”

根据这一规定,物业管理者如使用人脸识别门禁系统,在录入和使用人脸信息时,应当征得业主或者物业使用人的明示同意,对于不同意将人脸识别信息作为唯一验证方式的,小区物业应当提供替代性验证方式。

被非法使用人脸信息 可以主张哪些财产损失?

案例:某购物应用软件在未征得赵先生同意的情况下擅自采集其人脸信息,并通过分析其性别、年龄、心情等采取不同营销策略。赵先生发现后,起诉要求该应用软件运营者删除人脸信息并支付律师费。

解读:《规定》第8条第2款明确,“自然人为制止侵权行为所支付的合理开支,可以认定为民法典第一千一百八十二条规定的财产损失。合理开支包括该自然人

或者委托代理人对侵权行为进行调查、取证的合理费用。人民法院根据当事人的请求和具体案情,可以将合理的律师费用计算在赔偿范围内。被侵权人为制止侵权行为所支付的合理开支以及合理的律师费用可作为财产损失请求赔偿。”

因此,受害人可主张的财产损失除了实际损失、侵权人因此获得的利益之外,还包括为制止侵权行为所支付的合理开支以及合理的律师费用。

意见稿明确这些要求

普法课堂