责编:郭星宇
制版:高如哈
内蒙古法制报

人脸数据泄露和滥用造成的危害不可逆

斩断伸向人脸的黑手

“刷脸”正变得无处不在,无疑给人们带来了诸多便利,但在各类数据没有牢固的“保险”的情况下,人们更接近于在信息世界“裸奔”。“人脸数据泄露和滥用最大的问题在于造成的危害是不可逆的,与密码不同,人脸信息不可重置。”

人脸识别视频最低0.5元/套,质量较高的100多元/套,其中,质量较高的可通过大部分APP验证的消息令人胆战心惊。“刷脸”时代到来了,老百姓该如何保护好自己的“脸”?

一场关于人脸数据的“争夺战”正在打响,一边是不少移动互联网应用程序(APP)在人脸数据等领域疯狂“攻城略地”,不少APP甚至采用“霸王”条款,比如不进行人脸识别就不能寄快递、投简历、上厕所,甚至还有个别企业安装摄像头“偷”人脸数据……另一边是公众对人脸信息等个人信息保护的强烈呼吁以及监管部门不断重拳出击。

4月23日,《信息安全技术人脸识别数据安全要求》国家标准的征求意见稿开始面向社会公开征求意见,提出刷脸必须征得明示同意,并不得用于预测个人经济状况。

并且,今年5月1日,《常见类型移动互联网应用程序必要个人信息范围规定》也将正式实施。其中明确了APP运营者不得因用户不同意收集非必要个人信息,而拒绝用户使用App基本功能服务。

工信部信息通信经济专家委员会委员、联合国世界丝路论坛数字经济研究院院长、浙江大学教授王春晖表示,对个人必要信息的范围进行划线,填补了人脸识别应用领域的空白。这一次,不断伸向“人脸”的“黑手”能否被斩断?

不“刷脸”就不能买票、寄快递

“必须要我的人脸信息才能登录吗?”3月28日,来自北京的孙斌(化名)通过身份证号等信息登录了一直在使用的某航空公司官方购票APP购买机票,却显示账号存在风险,需进行身份验证。孙斌通过APP提供的“银联验证”进行验证,却被告知“暂时不支持此验证方式”。孙斌说,“这唯一的方式也是形同虚设。”

随后,孙斌致电该航空公司,客服告诉他,系统认定该账号安全等级过低从而“冻结”了他的账号,并称“这是为了您的账户安全着想”。而“解冻”的唯一方式则是完成人脸识别。孙斌表示,这明显是强制“刷脸”。

与孙斌的遭遇如出一辙,高茗茗(化名)也被强制要求“刷脸”。她用快递柜寄件时却被告知:根据快递条例要求,寄件需要验证本人身份,唯一的验证方法也是人脸识别。下单前,她已在官方微信公众号上通过了实名认证。

2018年5月1日起施行的《快递暂行条例》对实名收寄快递作出了规定,收寄快件时,应对寄件人身份进行查验,并登记身份信息,寄件人拒绝提供身份信息或者提供身份信息不实的,经营快递业务的企业不得收寄。其中,对是否使用人脸识别并未明确规定。

北京观韬中茂律师事务所合伙人王渝伟表示,寄送快递达不到采集人脸信息的必要性,这里要求人脸识别是假借了身份查验的由头。人脸信息并非不能应用于寄送快递的身份查验,问题在于不应该是唯一手段,应给予消费者选择权。

当前,小区安防和智慧零售是人脸识别安全风险发生的重灾区。在王渝伟看来,人脸识别的安全风险主要是应用太过泛滥。“最让人担心的是不知道这些信息泄露到了哪里,甚至有可能是境外。”

通过一张脸掌握一个人的消费习惯

“刷脸”正变得无处不在,无疑给人们带来了诸多便利,但在各类数据没有牢固的“保险”的情况下,人们更接近于在信息世界“裸奔”。并且,各类APP的信息获取从个人位置到照片,再从通讯录到人‘脸’信息,对个人信息的挖掘速度不断加快,深度也在不断增加。

“人脸信息的背后是一个人的住址、喜好以及消费习惯等信息,掌握了这张‘脸’,就掌握了一个人的各种习惯。”王春晖表示,很多APP不断在人脸识别领域布局,是为了方便对用户有针对性地“画像”,从而精准定位和营销,实现更大的商业价值。

事实上,人脸识别相关产业正在不断发展壮大。据亿欧智库发布的《2019计算机视觉人脸识别市场研究报告》显示,2018年中国计算机视觉人脸识别市场规模为151.7亿元,预计今年将达到530亿元。

然而,与人脸识别相关的风险问题也越来越凸显,比如个人信息泄露、滥用等。一些企业因管理不到位、应用方式不规范以及安全保障技术不过关等因素导致人脸信息、行踪轨迹等个人敏感信息泄露。

人脸等个人信息采集、售卖甚至已经形成了一条成熟的黑色产业链。近期,在部分社交平台和网站上,不少卖家将人脸识别视频明码标价,100元一套,其中包括身份证正反面照片、以及手持身份证照片和点头、摇头张嘴等诸多视频。并且,卖家还打包票称所售验证视频,能通过大多数APP平台验证流程。

据媒体报道,个别卖家透露,如今市面上流通的身份证照片大多是在小额贷款平台和公司野蛮发展期间泄露出来的;有些则是各个行业以人脸识别技术开发和系统测试为名采集而来。

其中,不乏通过技术伪造的人脸识别视频。王春晖观察到,人脸识别技术在不断发展,相关的“伪造技术”也在不断迭代。甚至有人用身份证照片就可以进行模拟人脸识别需要的张嘴、眨眼等动作,甚至可以骗过许多技术等级不高的人脸识别平台。

“信息之所以被伪造核心在于个别企业的人脸识别技术不太行。”王渝伟表示,如果一个企业的核心算法够强,伪造的难度就很大,伪造成功率也很低。

当前,人脸识别的技术提供商很多,但水平参差不齐,有的企业没有能力支撑人脸数据安全保障。企查查数据显示,目前,我国共有人脸识别相关企业7404家,并且,相关企业注册量已连续3年突破1000家。近年来,各类人脸识别系统也层出不穷,据统计,我国人脸识别相关专利目前共1.37万件。

王渝伟也观察到,当前,人脸识别市场竞争激烈,不少企业为了争夺市场份额,低价出售人脸识别技术或者设备,行业内甚至在一定程度上打起了“价格战”。王渝伟说,在这种情况下,人脸识别技术变现难,一些企业将盈利的可能性聚焦在数据上,“很多企业只是希望拿到人脸数据。”

监管逐渐进入“深水区”

人脸数据十分特殊而敏感,监管刻不容缓。王渝伟表示,“人脸数据泄露和滥用最大的问题在于造成的危害是不可逆的,与密码不同,人脸信息不可重置。”

事实上,监管方面也一直在发力。比如,近期发布的《常见类型移动互联网应用程序必要个人信息范围规定》明确了39种常见类型APP的必要个人信息范围。

“现在监管迈出了一大步,逐渐进入了‘深水区’。”王渝伟表示,这里对每类APP可以采集的个人信息作了详细规定,行业的标尺更为明确,监管的效率也将更高,这也意味着对人脸信息安全的保护能力可能将会提高一大截。

与此同时,一些地区也开始出台相关规定,明确物业不得强制业主进行人脸识别。日前,经四川省人民政府第64次常务会议讨论通过并提请四川省人大常委会第二十六次会议审议的《四川省物业管理条例(修订草案)》(以下简称《条例》)明确,物业服务人不得强制业主通过指纹、人脸识别等生物信息方式使用共用设施设备。给予业主选择权的同时,也保护业主的隐私。

当前,人脸数据被泄漏、滥用后,老百姓维权的难度依然很大。今年4月,备受关注的“人脸识别第一案”迎来了终审判决。被告杭州野生动物世界被判删除原告郭兵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,并于判决生效之日起10日内履行完毕。当事人郭兵在接受央视采访时表示,诉讼收益小,百姓维权动力不足,以及违法成本低,处罚力度不够是人脸识别滥用仍频发的原因。

个人信息安全受到侵犯该怎么办?郭兵建议,可以让相关机构提起公益诉讼,这相对于个人举证会多一些优势。

王春晖建议,将APP使用的个人必要信息的范围纳入法律范畴,给予更高的法律位阶,比如纳入《中华人民共和国个人信息保护法(草案)》。王渝伟也表示,人脸识别技术发展日新月异,新问题层出不穷,他建议,将人脸识别的相关法律同人脸识别相关的国家标准、行业标准进行有效衔接,这样既与时俱进,可操作性也更强。

同时,王春晖还建议,加大对违法违规获取、提供个人信息行为的惩罚力度。并且,拓宽消费者维权的路径,一旦发生侵权事件,消费者可以尽快向监管部门反映和举报。

在企业端也需加大事前审批监管的力度。王渝伟表示,可以借鉴行政审批的模式,对提供人脸识别底层技术支持的企业,进行资质审核,必须达到相应的安全保障能力,获得相应的资格认证,才能从事相关的技术。

同时,也应对后续人脸数据信息存储作出更为详细的规定。王渝伟说,比如不存储人脸的原始图片,并规定数据存储期限等。

当前,我国人脸识别技术走在世界前列。王渝伟表示,面对出现的新问题,对人脸数据安全的保护再严厉都不为过,但监管也不能“一刀切”,亦要给予行业一定发展空间。

(赵丽梅)