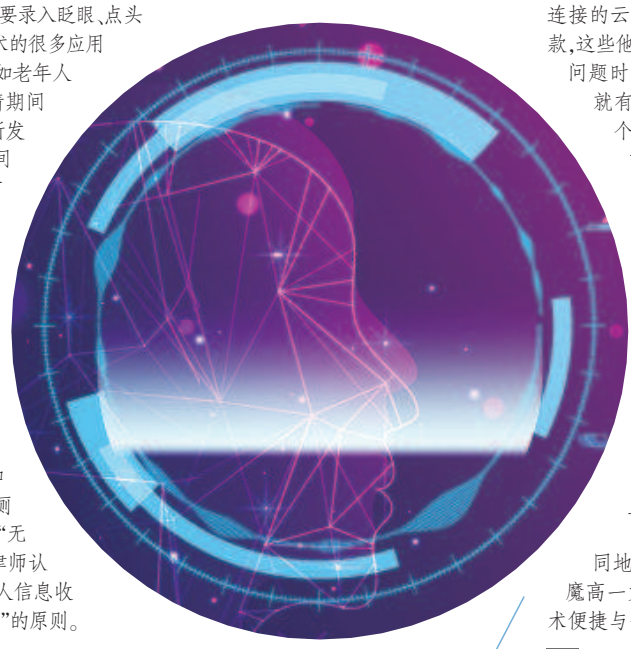
脸面上的事,你我的大事

本报记者 **姜燕**



“人脸识别 依法使用 不能滥用”

天津市和平区鞍山道168号,一座环境清幽、翻新过的老小区,新刷过赭红色涂料的墙体上攀附着陈旧的暖气管道和电缆线,进出大多是老年人。

岁末年初,这个平静的角落突然成了焦点,因为小区使用3年的“人脸识别”门禁系统受到了挑战。

一 用,还是不用?

《天津市社会信用条例》是2020年12月初表决通过的,当中的第十六条特别引人注目,它规定了“市场信用信息提供单位不得采集自然人的宗教信仰、血型、疾病和病史、生物识别信息以及法律、行政法规规定禁止采集的其他个人信息”。

按照它第九条的界定,市场信用信息是指“信用服务机构、行业协会、商会及其他企业事业单位等市场信用信息提供单位,在生产经营、提供服务或者行业自律管理活动中产生、获取的信用信息”。根据相关国家标准,个人生物识别信息包括个人基因、指纹、声纹、掌纹、耳廓、虹膜、面部识别特征等。

虽然有律师指出,此条例只限于征信体系范畴,但天津市和平区鞍山道168号的文化村居委会敏感地察觉到法律层面对人脸识别的关注,迅速以微信群、贴通告和小区广播等方式通知全体居民,在12月31日前决定是否继续使用人脸识别进出,还用的就去居委会签字,不用的,在年底前拿之前发的门禁卡去重新授权。

600户居民80%以上都选择了去签字,因为刷脸太方便了,尤其对爱忘带门禁卡的老年人。小区里几位老人都说,通知一出,家里也没商量啥,直接就去把字签了,一人签字代表全家。82岁的孙爷爷说,身上带张门卡,要用的时候都不知道放在哪个口袋里了,用“这个”,照下脸就进来了,至于信息安全,孙爷爷说“信息早就到处飞了,自己加点小心,不贪就行了”。截至2020年12月24日,小区共有50户居民表示不再使用人脸识别门禁系统。

二 “刷脸”刷了屏

2020年末,“挑战”人脸识别的新闻层出不穷。

11月、12月,浙江理工大学特聘副教授郭兵起诉杭州野生动物世界“人脸识别第一案”的一审宣判、二审开庭;

11月20日前后,一则戴着头盔去售楼处看房的视频在网上流传,事主公开回应说“被售楼部人脸识别系统拍到是自然到访客户,就只能按正常价格买,无法享受渠道优惠”,而从网络评论看来,不少人有过类似遭遇;

12月1日,《天津社会安全信用条例》出台;

2020年早些时候,北京大学法学教授劳东燕所在的小区准备安装人脸识别门禁,要求收集业主房产证、身份证、人脸识别等信息,她认为物业没有权利收集人脸信息,即使是公权力部门收集个人敏感信息,也需要有相应的法律依据或明确的法律授权。最后物业表示业主进出小区,可以在门禁卡、刷手机、人脸识别三种方式中自愿选择。

每一桩案例都引起网络热度,评论几乎一边倒地质疑人脸识别过度使用,对政府出台规定约束叫好。

人脸识别技术在我国投入商业应用的年头不长,专家将它的应用分为三类:人证比对如乘飞机、高铁、住酒店;人脸解锁如手机使用、考勤等;活体检测包括银行支付时需要录入眨眼、点头等信息。人脸识别技术的很多应用是非常值得称道的,如老年人护理、缉捕逃犯、疫情期间的流调防控等。最新发布《2021年春运期间交通运输疫情防控方案》中,也包含使用人脸识别技术加强疫情防控。

但它和其他网络时代的产品一样,短短三四年里,就迅速“攻城略地”,在越来越多的生活场景中应用,如小区门禁、公园和会所年卡,甚至上公厕都要跟风,几乎到了“无处不在”的地步,有律师认为,这早已超出了个人信息收集“合法、正当和必要”的原则。

三 “滥用”让人忧

它的便捷让人无可抗拒,但带来的个人信息安全问题也让人产生隐忧。

普通人对人脸识别安全性的担忧体现在感知阶段。40多岁天津出租车驾驶员宋先生说,他开通了支付宝刷脸支付后,用了两次就取消了,原因是“太快了,犹豫的时间都没有,我只轻轻看了手机一眼,钱就付掉了”。168号小区一个年轻的女士则曾经把她老公从睡梦中喊醒,趁他刚一睁眼,就拿他的手机对着他,“‘唰’地一下,手机就开了,太恐怖了!”

在央视新闻直播间人脸识别专题节目中,清华大学孵化的一个技术团队尝试攻破人脸识别系统,在给人戴上特殊的眼镜后,他就被系统识别为另一个人,并为一台不属于他的手机解锁。也有受访者表示,自己曾被系统判定为另一个人而通过门禁防控。

涉及人脸识别的案件近年也有发生,如厦门00后攻破银行人脸识别系统注册假账户并出售获利的案件,浙江一女子被犯罪分子诈骗开设银行账户并存钱,但人脸信息通过视频电话被录取,导致财产损失等。

全国信息安全标准化技术委员会等机构成立的App专项治理工作组去年10月发布了一份《人脸识别应用公众调研报告(2020)》,显示九成以上的受访者都使用过人脸识别,具体用途当中“刷脸支付”最为普及;六成受访者认为人脸识别技术有滥用趋势,还有三成受访者表示,已经因为人脸信息泄露、滥用而遭受到隐私或财产损失。在某些网络交易平台上,只要花2元钱就能买到上千张人脸照片,而5000多张人脸照片标价还不到10元。

除了技术本身和使用上的危险,它的存储也同样是很多人包括如劳东燕和郭兵在内的法律界人士最为担忧的环节。

四 安全,不安全?

在技术人员看来,人脸识别应用有风险,但并不比指纹或密码更不安全。一名在芯片公司工作多年的技术人员Eric说,如果对方要攻破银行账户系统,人脸信息并不是必需的,甚至有时银行的人脸识别系统还能够帮助识别犯罪行为。

Eric说,以人脸识别门禁系统为例,有没有信息泄漏安全隐患关键取决于采集机构。如果采集单位和广告公司或互联网公司有互动,确实存在风险。“如果是小公司,在财务发生问题时,开放数据是他们最快、最容易获得利润的途径。”Eric说,无论对于出售方还是购买方,采取攻破个人银行账户违法获利的时间成本和金钱成本,都远比直接出售信息和根据获取到的个人购物数据推送广告高得多。

华东师范大学数据科学与工程学院副研究员陆雪松也说,人脸信息包含更多的活体信息,比指纹更加安全,也有更好的利用场景。它还是很难被用模型和照片去复制的。如果有人拿到了生物信息特征,非常暴力地去和系统里已经采集到的数据库里的信息匹配并解锁,技术上存在这种可能,“但要在系统和应用上通过层层封锁,代价是比较高的。而且这种攻击行为是网络安全面临的普遍问题,并非人脸识别所特有”。

但郭兵指出,人脸识别等生物识别技术收集个人信息时,往往还同时收集个人其他身份信息,这些信息如果打包出售,后果不堪设想。Eric说,一般出售中的数据会做一些脱敏处理,互联网公司或网络商家获得的个人信息,可能会丢失关键字段,如注册信息等,对他们有价值的是人脸购物信息,足以提供他们推送广告的依据。“但也有不脱敏直接卖的。”他透露。

对于存储上的问题,Eric说如果将采集到的数据存储在自身的服务器,被攻破的例子是有的;租用公有云存储数据的相对安全,云服务提供商一般不会和第三方广告和互联网公司有协议,也有防范的手段,不大会被攻破。在存储方面与政府部门连接的最安全,但需要确认其真实性。

“如果我住的小区要上人脸识别,我会索取供应商信息,包括他的资质、使用的芯片、采集设备里所有的细节、连接的云服务供应商及双方协议条款,这些他都应该报备,以保证万一出问题时,可以溯源,如果没有报备就有问题。”Eric说,“这是一个产业链,不要指望一家单位能帮你管好数据,这是不现实的。”

他还透露,很多时候,有人已经不知不觉通过技术手段获取了人脸、声音,甚至指纹等信息。“购买相关产品时,不要图便宜,因为便宜货有可能被商家植入了连接渠道,在你刷脸时信息就传到商家的云服务器上去了。”

在采访中,两人不约而同地提到了一句话“道高一尺魔高一丈,或者反过来”,这就是技术便捷与安全相悖的宿命。

五 “最小必要化”

技术应用走得越来越快,社会亟需与其发展程度相配套的基础设施,这包括国家基本大法、专门领域的立法,以及行业标准。

郭兵是浙江大学法学博士,毕业后一直从事隐私保护方面的研究,对人脸识别等生物识别信息安全的关注始于两三年前。2019年4月,他去杭州野生动物世界办理年卡时,被告知除提交身份证信息、手机号码、拍照外,还要提供指纹,并且指纹识别是唯一入园的途径。随后又两次接到短信称入园方式升级为人脸识别,指纹识别已取消,让他前去注册。

郭兵质疑,年卡实名可以理解,但这一应用场景下,指纹和人脸是否必要?他认为,互联网时代,个人信息的收集使用不可避免,但不能过度,更不能强制。在交涉中,他也担心园方无法保障他个人信息安全。2019年10月28日,他向杭州市富阳区人民法院提起诉讼,被称为国内“人脸识别第一案”。

在维权的过程中,他对相关立法作了深入研究。《网络安全法》《民法典》都有一章对个人信息保护进行专门规定,但郭兵认为《民法典》虽然提到了生物识别信息,但没有对它作出更加针对性的规定。《网络安全法》的问题也在于此。

2020年10月21日,《个人信息保护法》(草案)公布并公开征求社会公众意见。草案对处理包括人脸等个人生物特征在内的敏感个人信息作出了专门规定,要求只有在具有特定目的和充分必要性的前提下,方可处理敏感个人信息,并在事前进行风险评估。

郭兵递交了自己的意见,认为应通过“行政许可”等方式提高人脸识别技术应用的门槛,降低潜在的风险。“这可能是目前遏制人脸识别技术滥用的最有力措施,其他方式的效果可能都具有一定的局限性。”

针对草案中提到的在公共场所以公共安全为目的可采集个人图像,郭兵也提出了相应的意见,指出对公共场所和公共安全要进一步具体化,不能只用一个不确定的法律概念,否则会导致商家和市场主体打着这样的旗号去使用人脸识别技术。

在他维权的过程中,国家一些行业标准也陆续出台。2020年3月6日国家市场监督管理总局、国家标准化管理委员会发布《信息安全技术个人信息安全规范》(2020年10月1日实施)。它规定在收集个人生物识别信息前,应单独告知收集及使用目的、方式、范围和存储时间,并征得同意。对于生物识别信息的存储,要与个人身份信息分开存储,仅存储个人生物识别信息的摘要信息等。

2020年末,工信部也要求App在收集用户图片、人脸等个人信息时要遵循“最小必要化”原则。

六 立法破困境

在起诉之前,郭兵就发现普通人因个人信息权益受损诉讼的案例非常少,当个人信息大面积泄漏时,公安查处的刑事案件反倒更为常见,这与其他类别民事案件恰好相反。“原因无外乎两方面,违法成本低,维权成本太高。”郭兵说,因为违法成本低,才导致那么多人过度收集个人信息,甚至进行不法交易;而普通人举证证明对个人信息权益造成的损失非常困难,如果缺乏足够的法律知识,打官司也很可能是败诉。

“这样的背景下客观上导致个人信息滥用愈演愈烈。”郭兵说。目前最紧迫的问题是立法不足,以致监管和维权都会出现困境。很大程度上,人脸识别滥用也是法律空白、监管不足导致的。

他强调了公益诉讼的重要性。在打这个官司前,他首先想到的是通过公益诉讼来维护包括他在内的年卡用户的合法权益,但由于现有立法在个人信息保护上规定是不足的。“对公权力、司法部门而言,法律要有明确规定,不然很难启动公益诉讼。”不得已他选择了自己提起诉讼。

公益诉讼的好处是在发现个人信息受到侵害时,能够及时介入来预防和制止,不至于发生严重后果后才由公安介入。

他指出《个人信息保护法》(草案)中增加了公益诉讼,“是个亮点”,但他也指出有进一步完善的空间。

其间他还参加了《杭州物业管理条例》的听证会,呼吁增加小区人脸识别应用的内容,最终得到接纳,增加在公布出来的草案里。“当时我主张得更多元一些,我认为不仅仅是物业不能强制,而是物业和社区等部门都不能。”郭兵说。他所在的小区去年8月通知要装人脸识别门禁,郭兵第一时间和物业提出安全风险和法律风险。但10月小区突然启用人脸识别系统,郭兵交涉时得到的答复是街道要求,街道也向郭兵表示确实是他们花钱安装的设备。

郭兵发现,他没有同意也没做过任何注册,但只要机器人脸识别到他,门就打开了。办理门禁时曾经在物业处拍过照,可能是被用在了人脸识别上,“这是明显违法收集和使用人脸信息。”郭兵说,“我不排除通过法律程序要个说法的可能性。”

2020年11月20日,杭州市富阳区人民法院作出一审判决,判杭州野生动物世界有限公司赔偿郭兵合同利益损失及交通费共计1038元,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,驳回原告郭兵的其他诉讼请求。郭兵不服并上诉,认为店堂告示和短信通知中部分内容对消费者不公平、不合理的规定,属无效,收集个人生物识别信息的过程中存在欺诈行为,应该删除收集到的他的全部个人信息。2020年12月29日,杭州市中级人民法院公开审理,择日作出宣判。

“维权要花很多成本,我事先就知道赔偿是非常少的,但揭示这个案件中存在的个人信息保护问题本身就是意义所在。”郭兵说。