

# “人脸识别第一案”背后的安全隐患

备受关注的“人脸识别第一案”近日在杭州市富阳区人民法院一审公开宣判。法院判决杭州野生动物世界赔偿郭兵合同利益损失及交通费,删除其办理指纹年卡时提交的包括照片在内的面部特征信息;驳回了郭兵提出的其他诉讼请求。

该案一审落槌,如同一颗石子落入湖水。这一案件所激起的关于个人生物识别信息安全话题,值得社会各方思考。



## “人脸识别”背后的安全之忧

“人脸识别第一案”表面上是一场看似有些较真的诉讼,但背后反映出的是随着近些年技术进步,人脸识别等应用快速铺开后的安全之忧。

近期,某视频平台上一段名为“戴头盔看房”的短视频火了。爆料人表示,出现这种滑稽现象,是因为房地产“老带新”、商业中介、自然看房人等不同类型客户可以拿到不同程度的买房优惠,所以看房人极力掩盖面容,以“对抗”售楼处用人脸识别判断客户

类型。

一位网络安全专家表示,目前,摄像头捕捉人脸静态画面的技术已经相当成熟。“如果你在看房过程中留下了个人信息,那么你的生物特征信息、身份证号、出生年月等就形成了一个‘信息包’。在这个过程中,没有人会征求你的意见。”

业内人士表示,因为技术的成熟、成本的降低,许多应用开发过程中,已经可以购买现成的程序模块嵌套进系统,相当于做好

了一个成熟的输入、输出接口的代码组件,可以直接实现人脸识别功能。有些这样的模块已经完全免费,因而人脸识别的应用场景得以大面积铺开。

网络安全企业奇安信集团网络安全专家陈洪波说,人脸识别的大面积推广应用,无论是出于方便管理、便利客户还是其他商业目的,但技术的推广必须让用户有知情权和选择权,并遵循最小必要的原则。

## “人脸识别”技术呼唤加强监管

“人脸识别第一案”宣判后,郭兵接受记者采访时表示,由于法院并未支持他关于“确认多项告示、通知内容无效”等诉讼请求,他已考虑针对这部分诉求提出上诉。而相较于个案本身,部分受访法律、网络安全专家表示,通过民事诉讼维护个人权益具有重要意义,但更希望这一个案能引起相关方面的重视,进而完善法律法规,强化对人脸识别的规范和监管。

北京大学法学院教授薛军表示,这一案件很有启发性。除了个人提起民事诉讼以外,未来还可能出现集团诉讼、代表人诉讼,或者消费者组织公益诉讼等,对侵犯个人信息的行为进行遏制。

实际上,在法律层面,针对生物特征信息采集储存,我国已对个人信息安全规范等做了具体规定。例如个人生物特征信息属于敏感信息,要求个人生物识别信息要与个人身份信息分开存储;原则上不应存储原始个人生物识别信息,可采取的措施包括但不限于:仅存储摘要信息。

本案原告代理律师张延来表示,现行法律法规体系下,指纹、人脸等个人生物特征信息,在搜集使用的边界层面已经比较明确。“比如网络安全法、消费者权益保护法、电子商务法中,对采集信息合法性、正当性、必要性三原则的规定都是高度一致的,民法典也专辟一章规定公民信息保护。”

陈洪波表示,除了法律,目前在技术层面,监管是相对成熟的,也就是说通过监测、爬虫等手段可以自动发现隐私收集的情况。除了个案捍卫自身权益,有关部门监管还需真正“亮剑”,进一步净化行业,推动人脸识别规范安全有序发展。(吴帅帅)

## 信息泄露“细思恐极”

此前接受采访时,“人脸识别第一案”的当事人郭兵曾表示,自己并不是一个技术上的“保守者”,是面对越来越多的应用场景,人脸识别技术大规模铺开,他习惯多问几个为什么,这些问题几乎都让他想到数据安全问题。

在技术层面,陈洪波说:“现在对数据的存储,无论是本地服务器还是托管到公有云,实际上都面临被攻破的风险。更何况许多企业推广人脸识别并没有有效的安防措施,在技术日新月异的背景下,随意采集人脸信息很难保证数据安全。”

一旦数据因为黑客侵入、员工倒卖、企业私自使用等原因泄露,人脸等“不可更改的”生物识别信息就会流入网络黑灰产市场,可能造成很大的社会危害。

陈洪波介绍,一方面人脸识别存储原本只是一张静态图像,但现在一些新技术可以通过静态图片来模拟动态行为,可以攻破一些识别系统;另一方面,如果人脸、个人身份



信息一一对应挂钩,这样的“信息包”价值密度将更高,可能对个人的损害也更大。

记者此前调查也发现,为了通过实名认证,达到注册虚假账号或者侵犯他人账号等非法目的,人脸信息已经成为黑灰产的重要

交易信息,并催生了“过脸产业”:人脸信息泄露后,不法分子可以通过“照片活化”,将照片制作成动图,按照相应登录软件规定程序,图片可以完成点头、眨眼等认证动作,顺利通过部分软件的人脸认证。

社会需要法治  
法治改变生活

内蒙古法制报

2021年 彩色印刷

全年定价: 240元/份 垂询热线: 0471-4687563

欢迎订阅

国内统一连续出版物号 CN 15-0025 邮发代号 15-6 各地邮局均可订阅