



“一天下来，脸要被扫十几次”

专家呼吁警惕人脸识别技术滥用切实保护个人信息安全

□ 本报记者 张守坤

打开手机，上海市民陈宽发现，每天需要进行人脸识别的App太多。“从手机银行App到购物软件，从化妆类App到游戏防沉迷……一天下来，脸要被扫十几次。”

对此，陈宽感到颇为担忧：“虽然有些App使用人脸识别是出于使用需求和安全考虑，但也并没给我们拒绝使用的权利，这是否属于人脸识别技术被滥用？随着人脸识别技术的应用越来越广泛，会不会导致个人信息泄露？”

陈宽的担心并非毫无道理。《法治日报》记者了解到，人脸信息是具有不可更改性和唯一性的生物识别信息，容易被犯罪分子窃取利用或者制作合成，破解人脸识别验证程序，侵害隐私、名誉和财产，由此引发的案件也不在少数。

那么，为何许多手机App会采用人脸识别技术？在使用过程中，应该如何防止该技术被滥用？近日，记者对此进行了采访。

人脸识别广泛应用 个人信息存在风险

想知道这个月账单明细，要先刷脸验证身份；进站乘坐地铁，不用扫码或购票，刷脸即可进站乘车；想办理相关业务，先刷脸注册账号……记者在调查中发现，从金融类、电商类到出行类、美图娱乐类，很多类型的App中都能找到人脸识别的痕迹。

2022年2月，有媒体对人脸识别技术相关问题进行调查，从使用频率来看，超过九成的参与调查者在生活中、工作中会使用人脸识别技术。其中，44.95%的参与调查者经常使用，48.88%的参与调查者偶尔使用。

调查还提到，自个人信息保护法实施后，有近四成参与者认为人脸识别技术滥用情况有好转。

但记者发现，目前在支持人脸识别功能的App中，仍有部分App没有明确的人脸识别使用协议，在人脸识别功能中没有征得用户同意。

在用户个人隐私政策里，虽然包含采集人脸识别等信息，但也有App并未在形式上加以突出，让用户清晰意识到人脸信息等生物识别信息被采集，而是将“人脸信息”与姓名等一般个人信息相混淆。

记者选取了10款热门消费类App进行个人信息保护合规检测，发现不少金融消费类App均为人脸识别功能提供单独授权页面并设置专有规则，但也有部分App则将人脸识别的单独同意与相机功能设为同一授权。

□ 本报记者 张雪泓

近日，北京互联网法院审结了一起App强制收集用户画像信息侵权案。

法院经审理认为，涉案软件在首次登录界面收集用户画像信息，未设置“跳过”“拒绝”等路径，属于强制收集，构成侵权，判决被告涉案软件运营者承担相应侵权责任。

被告上诉后，二审法院维持原判，目前判决已生效。

原告用户罗某在使用软件时，发现被告运营的软件在未告知隐私政策的情况下，要求用户必须填写“姓名”“职业”“学习目的”“英语水平”等内容才能完成登录。罗某认为，被告的这一行为属于强制收集用户画像信息。

同时，罗某还主张被告存在未经同意向其发送营销短信、向关联软件共享信息等行为，侵犯其个人信息权益，遂诉至法院，要求

此外，还有部分App采用“不点击同意人脸识别就不提供服务”的方式，强行收集用户个人信息。

南都人工智能伦理课题组发布的《人脸识别应用场合合规报告(2021)》(以下简称《报告》)显示，其对20款移动端人脸识别应用的合规情况进行了测评分析，其中六成具有人脸识别功能的App没有单独的人脸识别规则，很多App人脸识别规则没有告知存储时限或位置，仅有6款App提及人脸信息存储情况。

《报告》还显示，20款App中，16款对个人信息做了信息加密和传输加密处理，另有4款娱乐特效App存在问题，比如某App的“AI换装”功能是通过用户上传照片，然后选择视频模板后可生成一段换脸视频，但由于没有加密措施，用户的换脸视频的链接可被公开访问。这意味着，换脸视频可能被任何人获取，存在个人信息泄露风险。

“人脸识别技术的出现和应用，在很大程度上提升了用户认证的效率和准确性，因而逐步取代了传统密码、验证码等认证方式，在金融支付、交通出行、门禁考勤等领域得到了广泛应用。”内蒙古大学法学院讲师李东方告诉记者，目前对于App中使用人脸识别技术，法律法规并没有专门的禁止性规定，但是不能违反现行法律规范的相关规定。

李东方说，此类敏感个人信息的储存、传输、分析、转让、删除等环节，也应当满足更为严格的要求，如国家标准化管理委员会2022年出台的《信息安全技术 人脸识别数据安全要求》等，切实保护个人信息安全。

据上海瀛东律师事务所合伙人、瑞中法律协会顾问胡鹏介绍，人脸识别属于敏感个人信息，个人信息保护法明确规定，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，个人信息处理者方可处理敏感个人信息。民法典和网络安全法中也均规定了收集和处理个人信息的“最小必要原则”。

人脸信息一旦泄露 个人权益易受侵害

“在生活中，人脸识别技术确实具备独特的优势，但作为敏感个人信息的人脸信息一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害，值得警惕。”李东方说。

去年12月7日，最高人民法院发布了5件依法惩治侵犯公民个人信息犯罪典型案例，其中一起就是李某利用“颜值检测”软件侵犯公民个人信息。

法院判令被告涉案软件运营者向原告提供个人信息副本，停止侵权、删除个人信息、赔礼道歉并赔偿损失。

被告涉案软件运营者辩称，被告需根据不同用户需求，为用户推荐合适的服务内容，收集相关标签是提供服务所必需，并未违反个人信息收集的必要性原则，且该信息是原告主动填写，原告通过自己主动做出的行为同意了被告的信息收集行为。

法院查明，原告在登录涉案软件时，进入账号登录界面输入用户名和密码，点击登录，即出现若干问答界面，需要对用户“职业”“学习目的”“英语水平”等内容进行填写，填写完成后，还需填写个人基本信息界面，输入中英文姓名等必填内容才能完成注册并进入首页。上述过程中并无“跳过”选项，亦无关于同意收集个人信息的提示，原告另行取证，在新用户注册登录时，在上述过程中出现若干问答界面，会出现个人信息收集授权同意界面，

据了解，李某是某网络科技有限公司软件开发人员，他将自己制作的“颜值检测”软件发布在某论坛，供网友免费下载安装，以此方式窃取安装者手机相册照片1751张，其中含有人脸信息、姓名、身份证号码、联系方式、家庭住址等公民个人信息100余条。

那么，如何才能防止人脸识别技术滥用？2021年7月，最高法相关负责人就审理使用人脸识别技术处理个人信息相关民事案件的司法解释回答记者提问时曾指出，自愿原则是民法典的基本原则，个人的同意必须是基于自愿而作出。特别是对人脸信息的处理，不能带有任何强迫因素。

相关司法解释规定，信息处理者采取未单独征求用户同意，强制刷脸等方式处理用户人脸信息的行为，在相关民事诉讼案件中都会被认定为侵害自然人人格权益的行为。

“上述规定在很大程度上保护了用户在人脸识别技术应用过程中的权益，但现实是，在许多人脸识别技术滥用的场景中，用户往往只能被迫接受，大多并不会提起诉讼，维护自身合法权益。”李东方认为，如何进一步细化相关规定，还需要法律研究者和立法者进行更多的思考。

中国政法大学传播法研究中心副主任朱巍说，人脸识别不单是涉及人的长相，还关联着个人财产信息、金融信息以及家庭成员相关信息，用户隐私协议中，不能仅用一句话简单说明要保护个人信息，还应载明在什么情况下采集个人信息、如何采集、如何使用、如何删除等内容。

对此，胡鹏建议采取一系列相关的措施，比如就人脸识别和人脸图像处理等事项进行单独弹窗以获得单独同意，App在征得个人同意时明示处理个人信息的目的、方式和范围，个人信息主体享有撤回授权的权利，以及不得频繁地弹窗以获得个人同意等。

在接受记者采访的专家看来，人脸识别或人脸图像等相关信息不仅涉及个人隐私，还涉及生物学特征，不法分子如果获得人脸图像，可能冒用他人身份从事不法活动。

强化监督执法力度 完善行业自律机制

如何才能更安全使用人脸识别技术，让其给生活带来更便利？

今年广东省两会期间，民革广东省委向大会提交的集体提案《关于加强广东省人脸识别监管的建议》提出，要完善行业自律监督机制。

其中指出，人脸识别技术产业是高新产

业，随着互联网大数据时代的发展而发展，但相关行业内的企业良莠不齐，建议监管机构对要进入人脸识别行业的企业进行资金、技术方面的核查，减少低质量企业的进入，更好地保护公众的信息安全。同时，建立行业协会，设立人脸识别技术行业标准，通过行业内部监督，减少对人脸信息的侵权行为。

1月16日，由中国信息通信研究院云计算与大数据研究所、可信人应用守护计划(以下简称“护脸计划”)、中国通信标准化协会TC602联合主办的“护脸计划2022年度成果发布会”在云端召开，在护脸计划新一轮评测结果中，有多家企业及产品通过“人脸识别安全专项评测”“金融App人脸识别安全能力评测”“人脸识别系统保护人脸信息专项评测”等。

护脸计划由中国信息通信研究院云计算与大数据研究所于2021年4月发起，联合企业、金融机构、法律机构和学术团体，共同推动人脸识别生态安全和合规共治。截至2022年底，护脸计划成员单位达到148家。

“护脸计划”专家委员会主任、公安部信息安全等级保护评估中心原副主任毕马宁在致辞中指出，人脸识别目前是隐私保护和人工智能技术应用发生矛盾的焦点，产业发展面临三方面风险，分别是技术不过关、应用不合理和管理不到位。

“人脸识别近些年才被广泛使用和发展，而我国的相关立法也在不断完善的过程中。”胡鹏说，目前，我国相关立法还较为分散，各个法律法规的衔接需要进一步明确。一些上位法的规定较为笼统，如个人信息保护法规定，将由国家网信部门统筹协调有关部门推进人脸识别技术的个人信息保护工作，并制定专门的与人脸识别技术相关的个人信息保护规则，标准，而较为具体的操作指引则规定在非强制性的国家标准中，这些非强制性国家标准的有效性究竟如何认定，也有待司法实践进一步明确。

在个人信息保护公益诉讼取证，长春市检察院随后还开展了个人信息保护专项监督活动，对全市的汽车销售店、在售楼盘等进行排查。其间，绿园区人民检察院发现一家售楼中心存在非法获取个人信息的行为，积极与相关行政主管部门沟通，并制定检察建议督促其尽快整改，目前该售楼中心已经整改完毕，取得了较好效果。

“这就需要辨别客户是中介带来的，还是客户自行前来的情况，因此售楼中心安装了人脸抓拍系统，买房的客户到底算谁的，通过系统查询一目了然。”张先生坦言，绝大多数客户对此并不知情，只有内部人员或从事这个行业的人才知道其中奥秘。

对于偷偷抓拍人脸信息行为，张先生认为，这在一定程度上确实存在个人信息泄露的风险。

“售楼中心的行为违反了收集个人信息的必要性原则，侵犯了消费者的知情权、肖像权、隐私权，存在个人信息泄露风险。”吉林律师吴秀燕说，售楼中心或其他机构在未获得消费者同意的情况下，通过摄像头实现人脸抓拍收集、存储消费者人脸信息，并通过抓取的信息实现客户分类，虽然是为了业务运营，但严重损害了消费者权益和社会公共利益。

吴秀燕建议，市场监管、公安、检察、网信等部门应协作配合，齐抓共管形成工作合力，制定行之有效的规章制度，督促整治非法采集公民个人信息行为，协同引导行业自律，促进行业健康发展。

履行公益监督职责 消除信息安全隐患

民法典规定，处理个人信息应当征得自然人或者其监护人同意。消费者权益保护法规定，经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

对此，检察机关也一直在努力。

前不久，吉林省人民检察院印发了《关于加强经济犯罪检察与公益诉讼检察衔接协作的工作意见》，要求全省经济犯罪检察部门与公益诉讼检察部门加强衔接协作，充分发挥各自职能优势，聚焦重点行业、重点监督领域开展监督办案，包括处理大规模个人信息特别是敏感信息，容易产生个人信息泄露、电信网络诈骗违法犯罪风险的重点行业等。该《意见》全面加强个人信息等领域社会公共利益保护，进一步完善了公益诉讼制度，推动相关领域溯源治理，实现治罪与治理相结合。

针对公民个人信息泄露隐患，长春检察机关履行公益监督职责，召开了快递行业“个人信息保护”公开听证会，针对调查中发现各类违法行为，检察机关发出检察建议，提起公益诉讼等方式，督促商家采取有效措施积极整改，消除安全隐患。

长春市检察院相关负责人表示，长春检察机关将通过发布典型案例、以案释法等形式，进一步加大法治宣传力度，凝聚社会共识，做到宣传的多样化、常态化、全覆盖，强化人民群众对个人信息保护的防范意识。

法院判决，被告涉案软件运营者向原告罗某提供个人信息副本，删除个人信息并停止个人信息处理行为，赔礼道歉并赔偿维权支出2900元。

漫画/李晓军

□ 本报记者 刘中全

“我们绝不会再安装摄像头了，以前我们不知道这种行为违法，现在通过检察官们的释法说理，认识到了自己的错误……”

近日，吉林省长春市南关区人民法院立案庭法官到各售楼中心开展公益诉讼“回头看”时，某售楼中心工作人员表示对非法采集人脸信息行为有了全新的认识，以后绝不会再安装拍摄人脸信息的摄像头。

在过去的一年里，针对售楼中心安装人脸抓拍系统的现象，长春检察机关积极履行公益监督职责，消除了公民个人信息泄露的安全隐患。此前存在人脸信息被非法采集的几家售楼中心，目前均已主动拆除。

长春市人民检察院相关负责人接受《法治日报》记者采访时表示，长春检察机关充分发挥公益诉讼职能，持续加强与各职能部门的沟通协作，形成打击侵犯公民个人信息犯罪合力。

售楼中心暗藏猫腻 违法收集人脸信息

2021年10月，长春市人民检察院依托公益诉讼大数据平台，发现了南关区某售楼中心非法采集人脸信息的案件线索。

长春市民王女士跟随中介去南关区某售楼中心看房时，被领到指定区域“刷脸”。中介告诉她，这样才能获得具体价格及购房折扣。回家后，王女士怀疑此举可能存在人脸信息泄露的风险，于是向12309检察服务热线举报。

“我们对案件线索开展初步调查，并邀请南关区公安分局信息技术部门的民警辅助调查取证。”南关区检察院办案检察官告诉记者，他们一行人走访了4家售楼中心，发现有3家售楼中心均安装具有人脸识别功能的摄像头，调查人员通过拍照、现场询问等方式固定了证据，民警提取了后台操作系统的人脸数据存储信息。

在办案检察官提供的图片材料上，记者看到在某销售管理系统上，摄像头的画面正对着售楼中心大门，系统对经过人员的人脸实现自动抓拍并存储，形成清晰的人脸图像，在每个图像下面都有精确到秒的详细时间，该系统还自动生成一组复制人脸的ID，管理员可以对图像标签进行编辑设置……

“我们询问售楼中心负责人得知，安装人脸抓拍摄像头主要是为了判定到访者是否人到访还是由中介带访，以便同中介结算带客佣金。”办案检察官说。

南关区检察院经审查认为，涉案的几家售楼中心均在人口、沙盘等消费者经常停留的地方，安装带有人脸识别功能的摄像头，在未征得消费者明示同意的情况下，非法收集、使用、存储消费者的个人信息行为已经严重侵犯社会公共利益。

“去年年初，我们依法向相关行政主管部门发出检察建议，建议其立即履行监管职责，对涉案售楼中心违法收集消费者人脸信息的行为依法查处，并开展个人信息保护领域专项整治行动。”办案检察官说。

2022年6月，长春市相关行政主管部门以书面回复的形式采纳了检察建议，依法向涉案售楼中心下达《责令整改通知书》，要求其限期改正违法行为，同时针对辖区内15家售楼中心开展行业专项整治工作，对存在非法获取人脸信息的违法行为坚决予以查处。经过专项整治活动，下达责令整改通知书1份，累计消除公民个人信息泄露隐患5000余人次。

为充分发挥公益诉讼检察职能，长春市检察院随后还开展了个人信息保护专项监督活动，对全市的汽车销售店、在售楼盘等进行排查。其间，绿园区人民检察院发现一家售楼中心存在非法获取个人信息的行为，积极与相关行政主管部门沟通，并制定检察建议督促其尽快整改，目前该售楼中心已经整改完毕，取得了较好效果。

滥用人脸采集技术 侵犯社会公共利益

各大售楼中心不惜花钱购买人脸抓拍系统，是真的用于识别“中介带客”还是另有他用？记者采访了在长春市从事十余年房屋中介工作的张先生。

“在售楼中心安装人脸抓拍系统是最近两年开始的，此前没有这么先进的技术。”张先生说，售楼中心的人脸抓拍系统主要用于识别“中介带客”的情况。

据张先生介绍，各大楼盘建好后，开发商会想尽办法扩大销售渠道，最终目的是将建好的楼房卖出去，于是他们会选择销售公司进行现场销售，同时还会委托房屋中介公司，利用中介人员带客户到销售中心进行销售。

“这就需要辨别客户是中介带来的，还是客户自行前来的情况，因此售楼中心安装了人脸抓拍系统，买房的客户到底算谁的，通过系统查询一目了然。”张先生坦言，绝大多数客户对此并不知情，只有内部人员或从事这个行业的人才知道其中奥秘。

对于偷偷抓拍人脸信息行为，张先生认为，这在一定程度上确实存在个人信息泄露的风险。

“售楼中心的行为违反了收集个人信息的必要性原则，侵犯了消费者的知情权、肖像权、隐私权，存在个人信息泄露风险。”吉林律师吴秀燕说，售楼中心或其他机构在未获得消费者同意的情况下，通过摄像头实现人脸抓拍收集、存储消费者人脸信息，并通过抓取的信息实现客户分类，虽然是为了业务运营，但严重损害了消费者权益和社会公共利益。

吴秀燕建议，市场监管、公安、检察、网信等部门应协作配合，齐抓共管形成工作合力，制定行之有效的规章制度，督促整治非法采集公民个人信息行为，协同引导行业自律，促进行业健康发展。

履行公益监督职责 消除信息安全隐患

民法典规定，处理个人信息应当征得自然人或者其监护人同意。消费者权益保护法规定，经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

对此，检察机关也一直在努力。

前不久，吉林省人民检察院印发了《关于加强经济犯罪检察与公益诉讼检察衔接协作的工作意见》，要求全省经济犯罪检察部门与公益诉讼检察部门加强衔接协作，充分发挥各自职能优势，聚焦重点行业、重点监督领域开展监督办案，包括处理大规模个人信息特别是敏感信息，容易产生个人信息泄露、电信网络诈骗违法犯罪风险的重点行业等。该《意见》全面加强个人信息等领域社会公共利益保护，进一步完善了公益诉讼制度，推动相关领域溯源治理，实现治罪与治理相结合。

针对公民个人信息泄露隐患，长春检察机关履行公益监督职责，召开了快递行业“个人信息保护”公开听证会，针对调查中发现各类违法行为，检察机关发出检察建议，提起公益诉讼等方式，督促商家采取有效措施积极整改，消除安全隐患。