

别让“刷脸”丢了脸

人脸识别技术需要更强有力的监管

近两年随着技术的发展,人脸识别应用逐渐深入到人们生活的方方面面,既有刑事侦查、交通安检等公共应用,也包含金融支付、出入门禁、智能家居等商业活动,甚至出现了学生课堂签到、卫生间取纸也得刷脸的情况。

人脸识别，有“21 世纪十大人类生活革命性技术”之称，是继指纹、虹膜、语音等之后的最新生物特征识别应用。在众多的“人体密码”中，人脸识别具有与人身不可分离、难以篡改、交互性强、易提取性、符合人类识别习惯等特点，以人脸来识别个体，在可操作性、效率和识别准确度上均具有无与伦比的优势。

诚然，技术的使用为人们带来了一定便利，但应用的泛化、滥化，也引起了社会的争议与恐慌。

目前,世界范围内已掀起人脸识别技术的强监管风暴。技术的便捷性必须以安全性为前提。就目前人脸识别应用的滥用、恶化情况来看,其所带来的人身财产损失、隐私权侵犯、民主性消解等安全性风险,已经远远超过了其所带来的便捷性收益。

无节制“刷脸”，丢的不只是脸

在数据风险频发的信息社会，人脸识别技术被称作是人类的“最后一道安全防线”，因为它具有功能强大、获取隐蔽、泄露之后难以救济等诸多特性。

人脸不单单是脸，完全可以与个人身份、人身、财产等各维度信息直接构建联系，从而建立起针对个人的全方位信息库。一旦被不法分子窃取利用，对个人来说，其后果将是灾难性的。如将人脸信息和其他身份信息相关联，可能会被不法分子用以盗取网络社交平台账号或窃取金融账户内财产；将人脸信息和行踪信息相匹配，可能会被用于精准诈骗、敲诈勒索等违法犯罪活动。

可怕的是，这个泄露过程可能在人们浑然不知的情况下发生。基于人脸识别的无接触性、远程识别性，这一技术可以通过远程、无感抓拍甚至偷拍的形式收集人脸信息。也许在某个时刻，遍布街头的众多摄像头就已经精确收集了你的

我的臉如何才能由我做主？

技术的建构性与其破坏性相生相伴。随着人脸识别应用的泛化与滥化,相关的风险也在迅速深化与恶化,我们必须顺应全球技术强监管的发展潮流,尽早行动、补足漏洞。

一是推动对于人脸识别的专门立法。目前中国出台的《个人信息保护法（草案）》已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。不过，基于人脸识别技术的特殊性及应用影响广泛性，借鉴国际经验，仍然有必要制定一部专门规制人脸识别技术及人脸识别信息的法规，对人脸识别技术的研发应用范围、技术使用者的主体责任、权利侵害的法律责任及制裁体系等进行明确规定。

二是加快应用监管整顿。明确统一人脸识别技术的监管机构,承担人脸识别应用的审批与监管职能。设置必要门槛、明确审核流程,改变任何企业、任何场景都可以染指公民生物识别信息的现状,除道路、机场、银行等法律规定的必要安防应用,包括社区、学校、

人脸信息，而你对此浑然不知。

一旦人脸数据泄露,当事人很难得到有效救济。因为相较于数字密码,人脸这样的生物特征具有终身唯一、无法改变的特性。若是密码丢失尚可改变密码,但“换脸”几乎没有实现的可能性。

这意味着，人脸识别的滥用，将造就透明化的公众，无论是个人商业价值，还是个人秘密隐私，都将暴露在技术的强大视线之下，被精确计算、全面洞察、全面榨取。

一方面是日益严重的滥用后果；另一方面却是易被攻破的“技术盾牌”。根据新华社对网络安全专家裴智勇的采访，现在的技术完全可以做到仅利用一张二维照片，就可以充分提取人脸特征信息进行针对性训练，很容易就能获得人脸图像，甚至眨眼和来回转动都没问题。此前，还有人专门对某快递柜的人脸识别别人做了实验，而只要用一张打印照片就能代替真人刷脸，骗过智能柜取出货件。

商业场所等在内的人脸识别技术在应用之前都应申报审批，对其合法、正当和必要性进行审核；并立即对现有人脸识别应用开展整顿行动，尽快纠偏滥用行为。

三是切实保障公众知情权、拒绝权等在内的各项权利。压实技术使用者的主体责任，要求其在收集人脸识别信息等时需要获取公民明示同意，而这一同意的前提是当事人完全知情，在后继对于人脸识别信息的处理、转移、分享过程中，也应当再次向公众进行告知及获取同意。此外，赋予公民可拒绝人脸被收集的权利，在不提供相关信息的情况下，依然能享受企业所提供服务的的基本功能。当公民的人脸识别信息被不合理采集时，可要求个人信息处理者进行删除，并为其权利侵害提供畅通的维权、救济渠道。

总而言之，人脸识别就像当代智能技术应用的一面镜子。在人类与技术深度融合的当下，必须探索人与技术的相处之道。既要看到技术对于美好生活的推动作用，也要清醒意识到技术及其应用的限度。从人的立场去寻找技术治理与应用的最优方案，让技术服务于人，服务于最广大的群体。



资料照片

向滥用人脸识别技术亮剑

大到智慧城市建设，小到手机客户端的登录解锁，近年来，人脸识别逐步渗透到生活的方方面面，在为社会生活带来便利的同时，个人信息保护问题日益凸显。

7月28日,《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》)发布,向滥用人脸识别技术处理人脸信息行为问题亮剑。

对经营场所滥用人脸识别技术说不

据 APP 专项治理工作组 2020 年发布的《人脸识别应用公众调研报告》显示,在 2 万多名受访者中,94.07%的受访者用过人脸识别技术,64.39%的受访者认为人脸识别技术有被滥用的趋势,30.86%的受访者已经因为人脸信息泄露、滥用等遭受损失或者隐私被侵犯。

最高人民法院党组成员、副院长杨万明指出，现实中，一些经营者滥用人脸识别技术侵害自然人合法权益的事件多发。比如，有些知名门店使用“无感式”人脸识别技术，在未经同意的情况下擅自采集消费者人脸信息。有的卖家在社交平台 and 网站公开售卖人脸识别视频、买卖人脸信息等。因人脸信息等身份信息泄露导致“被贷款”和隐私权、名誉权被侵害等问题也多有发生。

针对经营场所滥用人脸识别技术进行人脸辨识、人脸分析等行为,《规定》第2条明确,在宾馆、商场、银行、车站、机场、体育场馆、娱乐场所等经营场所、公共场所违反法律、行政法规的规定使用人脸识别技术进行人脸验证、辨识或者分析,属于侵害自然人人格权益的行为。

针对部分商家采用一次概括授权、与其他授权捆绑、“不同意就不提供服务”等不合理手段处理自然人人脸信息的,《规定》第2条和第4条明确,处理自然人的人脸信息,必须征得自然人或者其监护人的单独同意;对于违反单独同意,或者强迫、变相强迫自然人同意处理其人脸信息的,构成侵害自然人人格权益的行为。

为平衡个人利益和公共利益,《规定》第5条明确了使用人脸识别的免责情形,包括为应对突发公共卫生事件,或者紧急情况下为保护自然人的生命健康和财产安全所必需而处理人脸信息的;为维护公共安全,依据国家有关规定在公共场所使用人脸识别技术的;为公共利益实施新闻报道等行為在合理的范围内处理人脸信息的等。

特别保护未成年人人脸信息

伴随着人脸识别应用场景越来越广泛，未成年人的人脸信息被采集的场景也越来越多。“由于未成年人个人信息保护意识相对淡薄，加之对新生事物较为好奇，其人脸信息被采集的概率相对较大。”最高人民法院研究室副主任郭锋说。

郭锋介绍,《规定》从司法审判层面加强对未成年人人脸信息的保护。按照告知同意原则,第2条第3项规定,信息处理者处理未成年人人脸信息的,必须征得其监护人的单独同意。

责任认定角度方面,《规定》明确将“受害人是否未成年人”作为责任认定特殊考量因素,对于违法处理未成年人人脸信息的,在责任承担时依法予以从重从严,确保未成年人人脸信息依法得到特别保护。

“刷脸”不能随便代替“刷卡”

伴随着人脸识别技术应用场景的不断丰富，一些小区引入人脸识别系统，用“刷脸”代替“刷卡”。

有人认为,将人脸识别作为住户身份验证方式,可以更精准识别出入小区人员,让小区管理更安

全、更高效。也有人担忧，人脸信息一旦泄露，可能给个人隐私造成损害。

“人脸信息属于敏感个人信息，小区物业对人脸信息的采集、使用必须依法征得业主或者物业使用人的同意。”郭锋指出，实践中，部分小区物业强制要求居民录入人脸信息，并将人脸识别作为出入小区的唯一验证方式，这种行为违反“告知同意”原则。根据《规定》第10条第1款，小区物业在使用人脸识别门禁系统录入人脸信息时，应当征得业主或者物业使用人的同意，对于不同意的，小区物业应当提供替代性验证方式，不得侵害业主或物业使用人的人格权益和其他合法权益。

APP强迫索权人脸信息无效

一段时间以来，部分 APP 通过一揽子授权、与其他授权捆绑等方式，强制索取非必要个人信息，成为许多消费者维权的难点。

为从司法角度规范此类行为，最高人民法院研究室民事处处长陈龙业介绍，《规定》根据民法典第1035条，在吸收个人信息保护立法精神、借鉴域外做法的基础上，明确了以下处理人脸信息的规则：一是单独同意规则。信息处理者在征得个人同意时，必须就人脸信息处理活动单独取得个人的同意，不能通过一揽子告知同意等方式征得个人同意。二是强迫同意无效规则。对于信息处理者采取“与其他授权捆绑”“不点击同意就不提供服务”等方式强迫或者变相强迫自然人同意处理其人脸信息的，信息处理者据此认为其已征得相应同意的，人民法院不予支持。