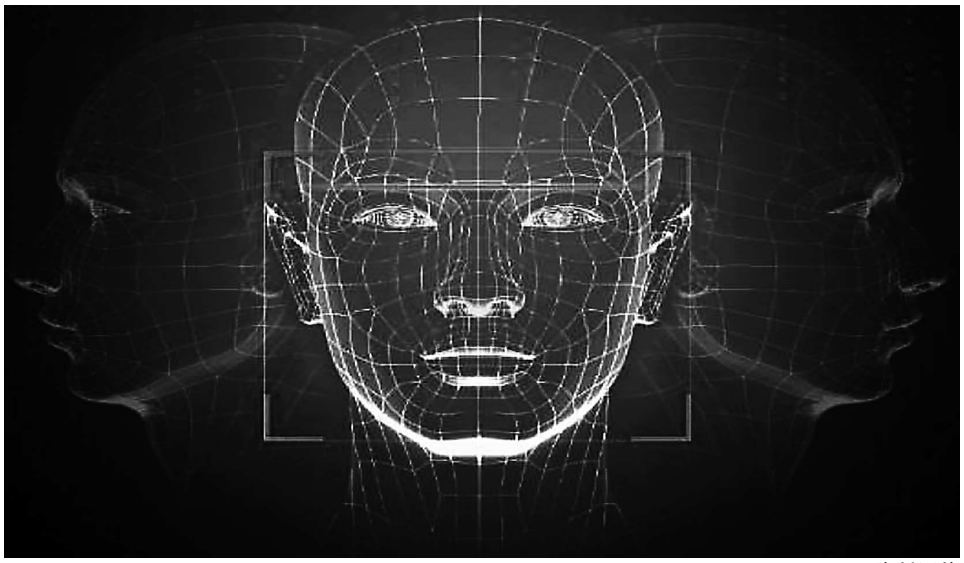
新老问题叠加，个人信息保护面临新挑战

如何保护我们的“脸”？

“在快递实名制全面普及的今天，快递隐私面单的推行并不理想，这为网络诈骗、群发骚扰短信等提供了便利。特别是疫情期间，居家抗疫的一大批老人也学会了网购，他们的信息一旦泄露，很容易被不法分子盯上。”日前，中国邮政集团有限公司上海市邮区中心局接发员柴闪闪对记者说，一些APP过度索权、违规收集使用个人信息等问题也很突出。

快递单“裸奔”、APP过度索权等老问题没解决，人脸识别等新技术带来的新问题又来了。今年4月，江苏省宿迁市公安局宿豫分局网安大队按照《公安机关互联网安全监督检查规定》的要求，对一家健身中心进行了现场监督检查。调查发现，这家健身中心有5家门店，共收集存储了2万多名会员的人脸照片等个人信息。

今年的全国人大常委会工作报告提到，围绕国家安全和社会治理，制定生物安全法、个人信息保护法等。在一些业内人士看来，新老问题叠加，使得个人信息保护面临新挑战。因此，个人信息保护法的出台有望解决个人信息保护面临的突出问题，守好个人信息安全防线。



资料图片

个人信息曝光增加 如何保护个人隐私

新冠疫情发生后，大数据、人工智能、人脸识别等技术广泛应用在防疫中。突然增加的信息曝光，让很多人担忧自己的个人信息是否能得到有效保护。

个人信息应分类分级保护

近日，一份在京发布的《人脸识别与公共卫生调研报告》，对疫情期间公众对人脸识别的接受度进行了研究。报告显示，疫情中大规模使用的人脸识别及其增强形式，让很多受访者担忧其自身信息安全。受访的1100多人中，60.3%的受访者不知道哪些实体拥有自己的面部数据，93.8%的受访者认为自己有权知道，仅有33.5%认为自己的面部数据是安全的。

这一现象也受到全国政协委员、北京国际城市发展研究院院长连玉明关注。他注意到，这次新冠肺炎疫情防控在不断扩大公众知情权的同时，也出现了由于信息权保护缺失导致某些信息泄露的问题。

缺乏根据应用场景对个人信息的分类分级保护，导致个人信息无序传播。掌握个人信息的主体多元，对这些机构主体在信息收集、使用、处理和保护方面，还缺乏规范和监管。另外，缺乏收集、使用和处理个人信息的合法性基础，无法保证个人信息有效使用于合法性事由，导致类似“人肉搜索”等隐私泄露问题。从另一方面看，个人信息泄露也直接影响公众对公共机构的信任，对疫情防控带来负面影响。

因此，在突发公共卫生事件应急处置中，姓名、出生日期、身份证件号码、生物识别信息、住址、电话、电子邮箱、定位数据、在线活动等行踪信息，也应“升格”为特殊类型信息，从个人信息权高度加以法律保护。基因数据、生物数据和健康数据等本身作为特殊类型信息，更应特别保护。

疫情期间个人信息保护问题凸显

柴闪闪在调研中发现，疫情期间，快递没法进入小区，很多快递小哥便在小区门口“摆地摊”，由于很多快递没有采用隐私面单，来取快递的市民可以轻易看到其他市民的信息。

除了快递之外，柴闪闪也发现，一些APP过度索权、违规收集使用个人信息等问题也在疫情期间凸显。今年4月，因存在涉嫌侵犯用户隐私的不合规行为，叮当快药、春雨医生等20多款生鲜外卖、医疗和在线教育类移动应用被国家计算机病毒应急处理中心点名通报，并进行下架整改。

江苏省律师协会副会长车捷指出，针对政府部门及基层群众性自治组织、其他相关主体（互联网公司、医院、超市、药店、公交、出租、物业、学校等）为疫情防控需要，收集、使用、保存、传输、销毁个人信息的规则仍未出台，存在着个人信息的不当泄露和使用的风险，需要引起注意。

“刷脸”带来新的个人信息保护难题

疫情防控期间，一些小区引入“人脸识别门禁系统”，其在保证人员的安全和信息精准性的同时，也极大节省了社区和物业的人员成本，保证了出入人员的通行效率。不过，此举也带来“人脸”信息泄露的风险。

今年3月，不少媒体报道称，有不法商家在网络上兜售十几万张戴口罩的人脸照片，这些照片0.2元1张，10万张以上还有优惠。其中，就有一些人上班打卡或进出门禁时拍的面部照片。

针对最近流行的“刷脸”，上海市信息安全行业协会会长谈剑锋持审慎态度。“为什么人脸识别不安全？并不是技术本身不安全，技术只是辅助的，更关键的是监管是否到位，安全防护是否完善。”在谈剑锋看来，许多互联网企业重发展轻安全、重建设轻防护。按照国家网络安全法的相关规定，数据谁采集谁负责，但现在能做到的平台不多。

“生物特性数据具有唯一性和不可再生性，脸部特征和指纹是无法更改的，不可能通过传统更改密码的简单方式来实现，这是生物特征数据与传统的认证数据最为关键的区别。”谈剑锋说。

给个人信息套上一件“防护服”

“因个人信息泄露，用户可能遭受推销电话、垃圾短信、垃圾邮件甚至诈骗电话的骚扰，不仅会对被侵权者个人生活带来不便，也可能造成物质、精神上的实质损害，因此应为个人信息套上一件‘防护服’。”柴闪闪说，从邮政快递行业来讲，政府部门应在加强快递企业内部信息运营监管的同时，加大力度推进快递企业使用隐私面单技术。

“目前，我国尚未制定关于个人信息保护的专项法律，个人信息保护由具体的法律、行政法规、地方性法规、各类规范性文件和部门规章等共同组成，内容分散、未成体系。因此，加快推进个人信息保护法的立法进程对于当前统筹做好疫情防控和经济社会发展，加强个人信息保护，具有重要意义。”中华全国律师协会副会长迟日大对记者说。

针对疫情防控期间收集的个人信息存在泄露风险问题，车捷建议，当收集信息的目的已经实现时（如疫情防控工作不再需要时），应分析已经收集和使用的个人信息的留存期限限制，同时满足疫情后期监测预警和存量数据保护的需求。对个人信息进行必要的删除、清理或至少进行脱敏处理，避免非疫情防控的滥用。

对于“刷脸”带来的个人信息泄露风险，谈剑锋则指出，不管是个人用户还是企业，对生物特征数据的采集一定要遵循严格的安全策略和要求。例如，尽量减少生物特征数据的使用场景，及时删除不必要的生物特征数据，避免集中数据存储方式。自身安全性不高或不能为用户提供安全保护的单位更不能收集生物特征数据。

疫情缓解后部分应急措施应解除

全国人大代表、上海财经大学公共经济与管理学院院长刘小兵认为，为了应急防疫采取的一些措施，在疫情缓解之后，应该尽量取消，不能将暂时措施变成永久措施。

这一观点与调研报告不谋而合。上述调研报告显示，超八成受访者认为，公共卫生危机结束后，应销毁在非公共空间内搜集的人脸信息，超七成受访者希望减少不必要的人脸识别应用场景。

尤其是在恢复正常生活后，受访者普遍认为，应削减出于应对危机需要采集的人脸信息和部署的人脸识别应用。

“从政府管理角度，拥有更多居民信息或许有利，但从个人角度出发，自由一定会受到部分限制，这些临时应急措施不能称为常态。”刘小兵说。

针对后疫情时期个人信息管理，连玉明则建议，尽快启动建立专门的个人信息保护监管机构，“随着《网络安全法》的颁布实施和《个人信息保护法》《数据安全法》陆续颁布，建立个人信息保护监管机构势在必行。”

公共机构收集使用信息需依法规范

连玉明建议，行政机关、公共机构的信息收集、使用和处理需要在《个人信息保护法》中加以规范。

我国《传染病防治法》《突发公共卫生事件应急条例》对重大传染病疫情突发公共卫生事件应急处置中，授权进行个人信息收集和使用均做出明确规定。但现实中掌握个人信息的主体众多，包括地方教育部门、公安部门、铁路航空交通部门、基层政府工作人员、电信运营商以及互联网公司等。这些主体在什么条件下可以收集信息、收集哪些信息、如何收集信息，以及这些信息在收集后的安全使用，都应划定边界并依法规范。

连玉明说，对基于数据关联分析的个人信息应加大监管力度，对未经授权披露在传染病暴发期间收集的个人信息可能会使个人面临风险，包括污名化、歧视、暴力等，应依法提供足够的保护。

“现在有的小区强制安装人脸识别门禁，有的商店只接受移动支付，这些做法其实都将个人信息暴露在各种平台上，是有风险的。”刘小兵说。他认为，个人生活便利和隐私保护之间存在权衡关系，很多人为了获取便利将个人信息暴露在技术提供者的视野里，如果技术提供者没有受到良好的规范，就有隐私泄露的危险。

“比如小区强制安装人脸识别门禁，个人可以请政府出面阻止，也可以起诉，外国就有这样的事件发生。”刘小兵说，归根结底，在技术发展越来越快的形势下，个人永远要为自己的意识安装“防盗网”。

连玉明建议，面对在重大突发公共卫生事件应急处置中对侵害众多公民个人信息权的行为，以及相关行政机关违法行使职权或不作为致使众多公民个人信息权被侵害的，应当纳入检察机关公益诉讼范畴加以法律保护。

（综合自《工人日报》《新京报》等）