保护个人信息安全,委员联名建议规范人脸识别技术应用——

小区装人脸识别应用须经业主投票同意

近年来,随着人工智能技术发展,人脸识别技术已经从理论研究走向大规模的应用落地,在居民消费领域,刷脸购物、刷脸进出等应用场景屡见不鲜。然而,伴随着人脸识别技术的广泛使用,海量人脸识别生物信息数据在各个场景被采集,在相关法律法规相对滞后的情况下,一旦人脸数据被非法使用,极可能引发科技伦理、公共安全和法律等众多方面的风险,危及公众人身与财产安全。

全国政协委员、广州市政协副主席于欣伟,全国政协委员、佳都科技集团董事长刘伟都关注到这个问题,拟向今年的全国两会联名提交《关于规范人脸识别技术应用,防范伦理与法律风险,促进人工智能健康发展》的提案。

■全国政协委员、广州市政协副主席于欣伟

■全国政协委员、佳都科技集团董事长刘伟

问题 | 生物信息具有唯一性 一旦泄露即终身泄露

全国政协委员、广州市政协副主席于欣伟表示,人脸识别技术已在各地商场、写字楼、房地产等机构及学校、医院、车站、出租车等场所广泛、大量使用,存在公共安全隐患。

例如,市民买房往往就被售楼部摄像头偷拍人脸数据;商场的人脸及消费特征信息贯穿注册、到店、跟踪、管理的会员管理全流程;部分处所还强制使用人脸识别。市民诉杭州野生动物园的"人脸识别第一案"、消费者戴头盔看房等事件引发公众对此技术滥用的忧虑。

全国政协委员、佳都科技集团董事长刘伟在提案中提到,人脸识别系统容易受到各类蓄意的仿冒攻击。他分析到,人脸识别系统可以对摄像头采集的人脸图像进行辨认,却无法识别采集的人脸图像是来自真人还是一张照片,人脸照片、视频及伪造3D头套等均有可能被机器识别。因此,人脸识别系统容易受到各类蓄意的仿冒攻击,常见手段包括盗用合法用户人脸照片、盗用合法用户人脸视频及盗用三维人脸面具等。

提案指出,一旦人脸数据被非法使用,极可能引发科技伦理、公共安全和法律等众多方面的风险,危及公众人身与财产安全。并且,人脸识别生物信息具有唯一性、永久性与不可替换性,终身无法修改,一旦泄露即终身泄露,即便维权成功也难以恢复原状。

现状 | 相关法规与管理约束不足

联名提案指出,目前人脸识别技术应用的相关法规和管理不足,行业治理框架尚未形成。无限制使用人脸识别技术不符合《民法典》《信息安全技术 个人信息安全规范》《个人信息保护法》(草案)等法规和标准要求。面对人工智能迅猛发展,亟需建立行业治理框架,促进产业健康发展,相关立法与部门管理刻不容缓。

同时,由于法规与管理约束不足,相关开发和应用单位在信息保护、身份认证等技术上明显缺少安保主动性与责任感,一旦出现重大侵害公众隐私或公共安全事故将会导致严重社会与经济后果。

建议 | 建立人脸识别技术应用必要性审查

如何规范人脸识别技术应用?要明晰谁来管,管什么,怎么管。两位全国政协委员认为,首先要为技术应用设立行政管理职能。建议由各级公安部门统一承担人脸识别应用的审批与监管职能,设立相应审批标准及程序。除道路、交通工具、银行等法律规定的安防应用以外,涉及对特定及非特定对象的处所,如写字楼、商场、企业等单位及公园、学校等在应用人脸识别技术前都应申报审批,公安部门依法审核其合法、正当和必要性,并监控数据安全。

"其次,以自愿、最小化原则规范人脸识别应用场景。"于欣伟表示,切实维护个人信息主体权益,需要建立必要性审查。例如,对于小区管理等特定人群人脸识别应用,须以自愿为原则由个人信息主体进行必要性审查,物业应将其视作新增公共设施建设项目,交由业主按户数及面积2/3以上投票通过后方可申报审批,禁止非授权擅自使用人脸识别。对于如商场等非特定人群的经审批的人脸识别应用,须以显著标识告知相应人员。

再者,做好立法顶层设计,组织人工智能专项立法。界定设备及数据主管职责、技术标准、数据使用、管理权限、资质要求等。规范数据权属、使用、交易、共享机制,明确数据所有、使用与收益权限。明确机构权限,制定采集、储存、传播、使用、销毁等法定程序及数据分类管理规则。此外,引导人工智能行业自律,完善相关标准和伦理规范。

全国人大代表蔡卫平:建议在常态化疫情防控中加强公民信息保护

为了配合新冠肺炎疫情防控,公民的个人信息包括身份证、行程轨迹、健康码除了要接受各个部门的调查、收集和统计,还要接受各种公共场合的大量检查。一些病例和密切接触者的个人信息被泄露,经社交媒体迅速传播后,引发了网络暴力。

对此,全国人大代表、广州市第八人民医院国家临床重点专科(感染性疾病科)首席专家蔡卫平今年提出了有关在常态化疫情防控中,加强公民信息保护的建议。除了建议合法采集、公开个人信息,他建议全国统一流调采集数据和信息公开模式。针对个人信息在防控突发公共卫生事件过程中被泄露的情况,他还建议在《突发公共卫生事件应急法》中增加相应的处罚条款,建立起一套严格的保密制度。

防控工作做精细不等于个人信息公开详细

"如果群众因为担心隐私泄露而不愿意配合流调,将会影响疫情防控工作大局。所以这些信息检查和收集如果不加以规范,个人隐私保护无从谈起。"此前出现的新冠肺炎密切接触者和病例个人信息在社交网络传播并引发网络暴力的个案,是蔡卫平此次提出加强公民信息保护建议的案由。

蔡卫平指出,这些个案透露出相关部门对个人信息保护存在明显漏洞。如何在政府信息公开过程中保护公民的隐私权,如何在调查、收集个人信息的过程中处理好个人隐私保护的关系,就成为一个亟待破解的难题。"事实上,个人信息公开的详细程度与疫情控制得好不好并没有直接关系,防控工作做精细才是关键"。

在撰写建议的过程中,蔡卫平查阅了《民法典》《传染病防治法》《网络安全法》《突发公共事件应急条例》等有关法律法规,征求了多位法律专家的意见。

建议全国统一采集数据模板和信息公开模式

在常态化疫情防控中加强公民信息保护的建议里,蔡卫平指出,首先要合法采集、公开个人信息。对于传染病的调查,《传染病防治法》第十二条仅授权疾病预防控制机构和医疗机构。其他机构或组织需要配合上述机构采集相关信息必须获得委托权,否则无权采集。针对患者或无症状感染者的个人信息公开不得违反《网络安全法》第七十六条第五款的规定。根据《民法典》规定,行踪信息属于受法律保护的个人信息。通信大数据行程卡查验个人行踪信息后只需显示不同颜色码以供识别,不应显示14天内到达或途经的地区。商业性机构不应当自行采集个人信息,而是通过查验当地政府的健康码即可,不应当要求进入者填写纸质个人信息。

由于各地公开数据涉及个人可识别信息方面差别较大,蔡卫平建议全国统一流调采集数据和信息公开模式。具体可由国家疾病预防控制中心设计一个全国统一的流调数据采集表,以最简便的方式采集,减少工作人员工作量和被采集人的不便。

在严格保密纪律方面,他建议对参与疫情信息采集的单位和个人必须开展相关法律和规章的学习教育,签署保密协议,严格执行保密制度。如发生泄密事件应对相关个人进行严厉处罚。有关单位和个人合法权益被侵犯可以依法申请行政复议或者提起行政诉讼、民事诉讼。

近日国家卫健委透露,正在考虑把《突发公共卫生事件应急条例》上升为法律。蔡卫平建议在其中加入个人信息保护的内容。例如在法律责任中增加因防控突发公共卫生事件而收集到的自然人隐私和个人信息被泄露的处罚条款。

■采写:新快报记者 陈慕媛 黄闻禹 李佳文 ■图片:新快报记者 夏世焱