

公共视频监控信息安全保护的法治化研究

◆王玉全*

(烟台大学法学院, 山东 烟台 264005)

【摘要】当前我国公共视频监控信息安全保护的立法立规主要体现在关联性立法立规和 21 部省市地方政府规章之中。推进公共视频监控信息安全保护法治化建设,有利于维护社会公共安全、保护个人信息安全、规范公共视频监控管理。公共视频监控信息安全保护的问题主要表现为无专门立规,缺乏处罚依据、权限划分不清晰、建设程序及审批不规范、设施和信息不安全等。为此,需要明确技术标准、安装程序、责任主体、信息收集、使用和保存的规则、不同主体的法律责任,厘清不同部门的权限划分等。

【关键词】公共视频监控;信息安全保护;公共安全;个人信息保护

随着社会经济的发展,公共视频监控运用越来越多,大街小巷随处可见公共视频监控的分布。公共视频监控的全域覆盖建设、全天候应用能够加强社会治安、提升生活质量、防范社会风险,但实践中过度收集和窃取公共视频监控信息、不当运用人脸识别技术挖掘个人信息、视频监控个人敏感信息泄露等现象层出不穷,亟待规制。因此,加强公共视频监控信息安全保护的法治化研究,是解决上述问题的重要途径。

一、我国公共视频监控信息安全保护的立法立规内容

公安部 2016 年曾发布《公共安全视频图像信息系统管理条例(征求意见稿)》,但至今尚未通过。通过在北大法宝中输入“公共视频安全”,发现现行有效的有 21 部地方政府规章。从立规内容来看,不同省市的立规内容有所相同,又各有侧重。多数省市都在总则部分,规定了立规目的、公共安全视频图像信息概念、调整范围和主管机构等内容。在规划与建设方面,规定了应当建设公共安全视频系统的场所或者区域、建设规划、建设原则和要求,并要求系统建设必须明示标识,设计、施工、维护单位应当具备法律法规规定的相应资质。在应用与管理方面,规定了系统自身运行管理、信息管理、公安机关监督检查职责和管理人员的管理。在法律责任方面,规定了相关工作人员的法律责任。在附则方面,规定了规章与上位法、其他法规规章的衔接、实施日期等内容。

二、推进公共视频监控信息安全保护法治化的现实意义

(一)有利于维护社会公共安全

公共视频监控可以应用于维护社会公共安全的诸多领域,能够有效提升社会治安的防控水平。对于抢劫、盗窃等犯罪案件,森林火灾、公共卫生防疫、社区治安等领域,公共视频可以实现有效监控,破解社会治理难题。例如,小区公共视频监控一定程度上可以了解空巢老人的生活状

况,建构智慧社区模型,更好改进社区服务,建设平安社区。随着智能摄像头的发展和图像处理技术的优化,公安机关可以依据公共视频监控全方位把握公共区域的安全情况,充分了解公共场所的各种情况,及时预防和发现违法犯罪行为。同时,基于公共视频监控技术,公安机关可以绘制出犯罪分子的行为轨迹。另外,借助公共视频监控的人脸识别技术,公安机关可以第一时间锁定犯罪嫌疑人的踪迹,迅速出击有效打击犯罪行为。除了实时记录和即时传输功能,公共视频监控系统还具备强大的存储能力,能够储存大量个人信息,便于突发公共卫生事件的防控。

(二)有利于保护个人信息安全

随着公共视频监控数量的增加和覆盖范围的扩大,人们日常生活中的一言一行都将可能被公共视频监控所记录、审视,保护个人信息也变得十分重要。安装在公共场所的视频监控能够实时记录个人活动,完整呈现每个人的活动范围、路径,进而会形成每个人的私人画像。如果视频监控者运用人脸识别技术收集到足够多的私人画像,那么就能窥见公民的生活全貌,可能会产生过度分析和使用个人信息的情形。同时,公共视频监控信息具有信息量大、公共性和隐私性的特点,在社会治安、交通出行、城市管理等方面皆有适用。加强公共视频监控信息安全保护能够破除公共场所难以界定、采集和使用个人信息限度不明,以及滥用个人信息等问题,完善个人信息知情同意制度,为个人信息提供全方位保护。

(三)有利于规范公共视频监控信息管理

公共视频监控在建设过程中部分存在着施工管理不规范、建设不科学、责任不明等问题。现有的公共视频监控信息缺乏统一的行业标准,可能会造成公共视频监控建设的质量不一。随着智能化、数字化和网络化的发展,质量不一的视频监控将会产生信息管理的疏漏。另外,公共视频

监控信息联网共享、网络传输、后台处理等诸多阶段与大数据、云计算等相结合,也会存在信息泄露的风险。例如,2023年,江苏森林防火队员在值班期间,违规拍摄监控画面并转发,造成不良社会影响。虽然直接原因是工作人员的违法操作,但也反映出管理不当,从而为侵犯个人隐私提供了可乘之机。加强公共视频监控信息安全保护的研究,将能够破解“信息孤岛”、加强技术标准与立法保护衔接、完善平台建设等,不断完善共建共享共治的公共视频监控信息管理制度。

三、推进公共视频监控信息安全保护法治化的问题

(一)无专门立规,缺乏处罚依据

在公共视频监控立法中,我国尚未有统一的专门立法,而是散见于地方政府规章之中。地方政府规章的不同,导致实践中可操作空间过大,增加公民权利受侵害的可能性。除了个人信息安全保护之外,对于维护公共安全而言,执法机构大多利用《中华人民共和国反恐怖主义法》《中华人民共和国治安管理处罚法》《中华人民共和国个人信息保护法》等法律法规。分散、笼统的立法立规显然不能满足视频大数据智能应用、法律与技术嵌合治理的现实需要。若地方政府规章中存在职权不清、控权不足、立法层级有限、立法特色不明显等问题,将不能理顺地方立法与上位法之间的关系,不能满足差异化的民众需求,使个人信息陷入被侵害的境地。

(二)权限划分不清晰

用于社会管理的公共视频监控主体范围非常广泛。例如,在《无锡市公共安全视频图像信息系统管理办法》中,公共视频监控的主体包括公安机关、财政、住房城乡建设、城市管理、大数据管理、国家安全、广电、电力、电信以及具有公共服务管理职能的企事业单位、社会组织等。在《广州市公共安全视频系统管理规定》中,公共视频监控的主体是公安机关、信息化主管部门、规划、建设、林业园林、国土、房屋、市场监督管理、交通、城管、应急管理、水务等行政管理部门。公共视频监控需要行政机关、企事业单位、社会组织的协调配合,最大程度实现社会物资及人员的整合。例如,政法委“雪亮工程”与公安部“天网工程”的重复建设,可能会带来人员冗杂与物资消耗。各自为政的视频监控安装以及系统利用,不仅导致资源浪费,也会造成个人信息利用的冲突与矛盾。

(三)建设程序及审批不规范

各大城市为推进公共视频监控建设,通常没有将设置公共视频监控的安装场所予以明确列举,对于完全公共场所和半公开场所也没有明确界分。部分隐蔽的针孔型监控摄像头没有做到公开透明、明确固定方位和监控范围,侵犯了当事人的知情同意权。部分公共视频监控甚至能监控私人办

公室、卧室等私密场所,直接侵犯了公民的个人信息保护权。公共视频监控安装参与程序的缺失、个人信息收集利用公开程序的匮乏,将会造成当事人隐私泄露的精神性和物质性损害。审批过程的不一致、责任划分的不明确,也会造成公共视频监控权力的滥用。如果公共视频监控建设没有详细的程序性规定及审批规范,则会导致大量的摄像头非法安装在私人的场所,从而暴露个人隐私,对个人权利造成侵害。

(四)设施和信息不安全

对于公共视频监控设备而言,有些设施由于缺乏必要防护,因而出现了盗窃、人为破坏等现象。例如,大量设备由于风吹日晒,缺少相关专业人员维护,或者因维护成本过高出现了损害。有些人员在设备交接维修的过程中,出现了信息泄露的情形。有些单位的操作人员不熟悉相关的数据流程,出现了删除或修改的相关问题。部分工作人员不适当使用视频图像画面、非法同步录像、违法调取个人信息、没有妥善存储保管图像信息等行为,将会给公众的合理隐私期待权和咨询自决权造成严重的危害。设施和信息的不安全将会对个人隐私造成破坏,损害他人合法权益。

四、推进公共视频监控信息安全保护立法的路径

(一)明确技术标准、安装程序与责任主体

公共视频监控信息安全保护应当与技术应用规范程序、安全保障等标准衔接,结合深度学习、生成式人工智能与大数据等相关内容,遵守公共安全视频图像信息采集、接入、共享和使用等相关技术要求。监控安装阶段应区分私人领域与公共空间,安装范围原则上限于公共空间。基于对大众的尊重,在安装公共视频监控系统前应当启动评估程序,充分听取大众的意见。按照“建设者管理、管理者负责”的理念,明确各主体责任范围,建立备案登记制度,在发生侵害行为时快速找到责任人员,促进运维使用的稳定有序。技术服务单位要加强行业自律,建立个人信息安全保护自愿性认证制度,制定统一行业标准,逐步形成行业惯例,自觉接受社会监督。

(二)明确收集、使用和保存的规则

首先,规范技术运用条件。除非经过合法授权,否则不能随意对特定人进行信息采集。对于个人信息的采集,必须有书面的申请报告,同时附有相关的时间、地点和人物限制。智能视频人脸识别需设置显著提示标识,取得个人同意,只能用于维护公共安全目的。其次,规范监控数据传输、使用、共享等制度。数据的使用、共享等必须出于维护公共利益的需要,坚持必要、审慎、比例等原则,只利用与处理目的有关的信息,推动公共利益和个人信息保护的动态平衡。只有公安机关、大数据局等有权机关才能访问个人信息内容。不同部门信息共享要采取个人信息匿名化



处理措施,防止敏感隐私信息的泄露。对于非法获取的视听资料、电子数据等公共视频监控信息,依法予以排除。对于人脸识别技术应用而言,应强调审慎、预防、公平、比例性、归责等原则,原则上须获得个人同意。最后,规范视频图像信息保存与删除。建立信息适时删除制度,根据信息的敏感程度和所涉对象明确删除期限。严格遵守保密规定,明确存储时间,超过规定期限数据自动删除。如需继续保存数据,需提交说明材料,详细论述理由和法律法规依据。

(三)厘清不同部门的权限划分

一是建立统一的领导协调机构。行政机关成立专门机构,建立公共安全视频图像信息系统联席会议制度,协调解决建设和管理中的重大问题,并将大数据相关经费纳入市级财政预算之中。二是明晰不同部门的职责权限。由公安机关负责总体指导、监督和管理。大数据局负责公共视频监控信息的汇集、使用、传输、共享等工作。其他各部门按照各自的职责分工,建立完善的信息分级分类部门处理机制,协同做好相关工作。三是做好公共视频监控信息安全保护的沟通工作。将公安局、政务服务中心等单位的公共监控视频信息汇集到大数据局之中,然后再由大数据局进行整合和转发。在公共监控的数据收集整理方面建立统一的平台系统,从而促进公共监控视频信息的共享。

(四)明确不同主体的法律责任

问责是规制公共视频监控的最后一道法律防线。一方面,设备用户认证、视频监控信息加密,这样即使被窃取,没有密钥也不能观看。公安部门同可接触到公众信息的企业部门,尤其是长期为公安部门提供服务的单位和个人,签订安全保密协议书,从而建立公共视频监控信息安全的预防机制。如有违反,如偷窥、偷拍、窃听、散布他人隐私,盗窃、损毁公共安全视频系统的设施、设备,擅自复制、提

供、传播视频信息,应当依据相关法律法规追究其责任。另一方面,严格执行相关规范,做到有责必追究。对个人隐私部位、获得的数据、人员的轨迹数据、人脸图片等内部管理,要严格保密协议和办案流程,遵守相关规范。遵循“谁使用谁负责原则”,施行严格登记制。相关人员须严格遵守公安信息共享查询应用七不准和《公安机关人民警察使用公安信息网违规行为行政处分暂行规定》等,做到查完就留痕迹,所有系统安全日志都有数字认证。构建监察机关监督、行政机关监督、舆论监督和公众监督的全方位监督体系。行政机关及其工作人员不履行或者不正确履行职责,依法追究行政责任,给予纪律处分、政务处分等;构成犯罪的,依法追究刑事责任。

参考文献:

- [1]刘艳红.公共空间运用大规模监控的法理逻辑及限度——基于个人信息有序共享之视角[J].法学论坛,2020,35(02):5-16.
- [2]石佳友.公共视频设备应用中的个人信息保护[J].江苏社会科学,2022(03):90-101,242-243.
- [3]李延舜.公共视频监控中的公民隐私权保护研究[J].法律科学(西北政法大学学报),2019,37(03):54-63.
- [4]张新平.智能视频监控之法律与技术的嵌合治理[J].法制与社会发展,2020,26(05):206-224.

基金项目:

山东省社会科学规划数字山东研究专项项目,项目名称:山东省公共视频监控信息安全保护的法治化研究,项目编号:21CSDJ69。

通讯作者:

王玉全(1991—),男,汉族,山东枣庄人,博士,讲师,研究方向:宪法学与行政法学。