

便民“扫一扫”扫出广告链接——

“数治”暗藏二维码风险

当前,我国多地积极搭建数字治理平台,为基层治理提供技术支持。半月谈记者发现,以便民服务二维码为代表的智治手段,在服务响应、指挥调度、矛盾化解、风险研判等环节发挥了积极作用,但也容易遭遇恶意利用或攻击,其中风险须加防范。



新华社发 商海春 作

A

便民二维码存数据安全隐忧

家住西部某地的王女士发现小区垃圾未及时清理,她扫了扫张贴在小区的便民服务二维码,上传照片,反映问题,不到半小时便接到后台回应。社区工作人员联系确认后,立即通知小区物业处理。“线上反映诉求方便快捷,问题能得到及时解决。”王女士说。

在西北某市一街道综合治理中心,半月谈记者看到工作人员正在通过公众诉求办理平台处理、反馈线上诉求。工作人员表示,数字化治理平台整合多项服务事项,二维码一扫即查、一点即看,提高了群众办事效率;街道社区通过收集信息数据、及时处理监测预警信息、办理交办诉求事件等,提升了日常工作的质效。

时下,数字政府建设不断推进,多地创新推出各类便民服务二维码,以“数治”赋能“善治”,提升治理效能。然而,半月谈记者调研发现,由于便民服务二维码容易获得使用者信任,交互多,使用频率高,更易遭遇恶意利用或攻击,暗含安全风险。

——二维码暴露在外,易遭恶意篡改、替换。半月谈记者注意到,一些街道社区将便民服务二维码张贴在小区门外、楼院墙外,有些地方是监控盲区,极易被人调包替换,真伪难辨。2020年,西安地铁站就曾发生过防疫二维码被恶意替换为理财产品推广链接的情形。

——运维企业违规操作或过度收集用户信息。今年3月,相关部门在查处一起涉数据安全违法案件时发现,浙江一科技公司在为当地政府部门开发运维信息管理系统的过程中,未经同意擅自将建设单位采集的敏感业务数据上传至租用的公有云服务器上,且未采取安全防护措施,造成严重数据泄露。

——政务服务数字系统收集的数据商业和社会价值高,易成黑客攻击对象。“智治管理模式依据大量的数据获取和分析,谁建的数据库,数据就掌握在谁手里,潜在风险很难规避。”大数据分析系统国家工程研究中心纪检监察大数据部主任方金云说,通过便民服务二维码等政务数据平台收集的数据信息数量庞大、来源多样,敏感信息一旦被恶意获取和利用,将造成严重后果。

B

三大漏洞危及数据信息安全

受访专家和干部表示,便民服务二维码目前存在三类漏洞,或危及数据安全。

一是制码近乎“零门槛”。二维码生成器能将任意网址转换为二维码供用户扫码访问,不法分子将病毒、木马程序等下载地址编入二维码,用户扫码后,手机里的通讯录、银行卡号等信息极易泄露。中国科学技术大学网络空间安全学院教授左晓栋认为,篡改、伪造二维码,使其指向恶意地址或下载恶意程序,已成为手机病毒传播、用户钱财盗取和不良信

息传播等案件发生的新渠道,而在此过程中,并无对二维码进行审核、监控、追溯和认证的手段。

二是数据安全监管滞后,海量数据成“烫手山芋”。方金云表示,目前数据监管仍未形成统一体系,数据收集通常先于数据管理和保护,一定程度上也会造成安全风险的防范缺位。半月谈记者调研发现,一些地方数据安全监管工作存在多头管理、权属不清的情况。有大数据管理部门工作人员表示,目前国家层面成立了大

数据局,但省(区、市)机构改革方案仍未明确,部分职能边界不清。

三是数据采集和提供方均缺乏数据安全和防护意识。多名受访专家表示,一些数据收集部门缺少对数据收集合规合法性的论证以及对数据安全保障的有效措施。“很多线上填报数据和信息涉及个人隐私和数据的过度采集,这与国家法律法规和相关精神相悖。”方金云说,公众对个人数据安全性的重要性的认识不足的问题。

C

便民二维码亟待从严监管

数字技术赋能社会治理,数据安全是“红线”,必须守住。受访干部、专家建议,推动数据安全措施与各类数字治理平台搭建同规划、同建设、同使用,确保国家数据安全、公共信息安全和个人隐私安全。

首先要筑牢数字安全监管堤坝。数据安全事关国家安全,数据安全监管权任何时候不能丢失、不能旁落。方金云建议,要从中央层面部署统一的数据监管体系,加强数据安全监管和数据交易规范化,一把尺子量到底。

其次要强化细化数字安全法律保障,依法收集、管理数据资源。左晓栋等人建议,进一步明确现行数据安全相关法律法规的实施细则,完善分级分类授权、使用主体合法性背景审查、数据共享和合规风控等安全管理制度,加大对涉事企业违规违法的处罚力度,严格防范企业技术优势滥用,推动权责匹配。同时,针对各类二维码当前应用场景广泛的现实,创立二维码安全认证和防伪溯源技术体系,实现二维码生成、运行

全过程管理,防堵数据安全漏洞。

最后要培养数字治理专业队伍,培育公众数字安全意识。多名受访专家和干部表示,加强领导干部智治能力和数字化思维能力建设是推进数字政府转型的重要抓手。应培养一批善于获取、分析、运用数据的干部人才队伍,推动建立一支政治强、业务精、技术通的专业数字人才力量。同时,加强宣传警示,强化公众数据安全意识 and 数字法治素养。(据《半月谈》)