大数据时代个人信息安全风险探析
——以健康码的应用为例

周　姮,张明彭
(安徽大学 法学院,合肥　230039)

摘　要:随着政府将大数据技术不断应用到社会治理的各个方面,个人信息安全受到威胁的风险也随之提升。社会治理不能以牺牲个人隐私为代价,在政府将大数据技术引入社会治理中时,必须兼顾个人权利的保护。以新冠疫情期间健康码的应用为例,政府收集个人信息在于保护公民身体健康权,是公权力对私权利的短暂限制,具有正当性基础。但是,健康码的应用也存在风险:个人信息收集主体过多、信息过度索取、重复索取可能导致信息泄漏;信息数据由企业存储、疫情后信息处理问题不明确可能导致信息滥用。在政府利用大数据进行社会治理常态化的趋势下,更应重视其对个人信息安全带来的风险和挑战。

关键词:大数据;个人信息安全;健康码;公权力
中图分类号:D63　　**文献标识码**:A　　**文章编号**:2096－2371(2021)06－0034－04

On the Risk of Personal Information in the Era of Big Data with "Health Code" Application as an Example

ZHOU Heng, ZHANG Ming-peng
(Law School, Anhui University, Hefei 230039, China)

Abstract: As the government continues to apply big data technology to social governance, the risk of personal information abusing and personal rights threatening also increases. Social governance development cannot be at the expense of personal privacy. When the government introduces big data technology into administrative management, it must give consideration to the protection of individual rights. The application of health code during the epidemic period of the COVID 2019 is taken as an example. The government collecting personal information to safeguard citizens' right of health is a temporary restriction of public power on private rights and interests, with legitimacy as its basis. However, the application of health code also has risks, for too many subjects to collect personal information and excessive and repeated collection may lead to the risk of information leakage; information data stored by enterprises and unclear information processing after the epidemic may lead to the risk of information abuse. Under the trend that the government uses big data to normalize public governance, it is especially important to notice the challenge and risk concerning the security of personal information.

Key words: big data; personal information security; health code; public power

---

收稿日期:2021－06－06　　**修回日期**:2021－09－20
基金项目:黄山市司法局委托课题"2020年黄山市专项法律服务协议"(K260148306)资助。
作者简介:周　姮(1994—),女,土家族,湖北恩施人,安徽大学法学院2019级宪法学与行政法学硕士研究生,研究方向:宪法学、行政法学;张明彭(1993—),男,安徽合肥人,安徽大学法学院2018级宪法学与行政法学硕士研究生,研究方向:宪法学、行政法学。

健康码,又称防疫通行码,它是以大数据为基础,由使用者申请,经过后台审核后而形成的个人二维码。作为新冠疫情爆发而产生的一种全新的事物,健康码的出现既是一种偶然,也是一种必然。大数据技术的运用在我国行政治理中并不罕见,利用公民日常生产、生活所产生的个人信息,经过后台分析进而做出相应的行政措施,如城市交通流量的控制、违法建筑的识别等。伴随科学技术水平的提高,政府对个人信息的使用程度也不断加深。“在现代化进程中……危险和潜在威胁的释放达到了一个我们前所未知的程度”,公民的隐私在大数据的使用中无处遁行,公民逐渐被标签化、失去个性,个人空间被进一步压缩。[1] 若任使用大数据技术而不对此予以规范,我们将丧失现代社会所珍视的个人信息权利,“极权社会”将威胁到每一个自由的公民。习近平总书记在党的十九大报告中也强调,在将大数据技术融入到社会治理中的同时,也要提升治理的专业化和法治化水平。基于此,文章以健康码为例,探析健康码应用的法律基础以及可能对个人信息安全带来的风险挑战,有助于更有效的规范政府利用大数据进行社会治理。

1　健康码的法律性质及其正当性论证

健康码作为大数据技术应用于社会治理的典型代表,在数字化抗疫中发挥了举足轻重的作用。尽管健康码是在特殊时期突破常规的非常举措,但其缺乏完整的制度设计和监管体系。因此,我们有必要从运作机制来分析健康码的法律性质,从制度规范角度来论证健康码应用的正当性,这是讨论健康码背后个人信息安全风险的前提。

1.1　健康码的法律性质

在疫情期间,健康码属于何种性质的文件? 是否如同个人身份证? 没有它又会产生何种后果? 我们可以从健康码的收集、运行以及审核方式上进行探讨。有学者认为健康码所收集的个人信息类型主要分为两大类: 单一授权信息和复合授权信息。[2] 单一授权信息的收集主要靠个人在系统中自主填报,包括个人身份信息以及个人健康信息。而复合授权信息需要公民授权系统,由系统在后台通过数据对比、分析生成,如个人行程信息。经过信息收集、数据分析,判断得出不同地区公民的感染概率,并通过不同的颜色(绿码、黄码、红码) 进行直观的展示。由于单一授权信息是由个人进行填报,存在瞒报或者谎报的可能。复合授权信息由系统后台进行自动判断,也可能出现判断错误。如在一些临近高风险地区的地方,因为后台系统对手机定位信息收集产生偏差,而把正常地区公民的健康码判定为红色。因此,从运行机制上来看,健康码并不能完全正确地反映个人健康风险状况。对于非绿色健康码的应对措施,一般也是限制出行和进行隔离,有的地区会要求进一步做核酸检测以确诊。此外,对于无健康码的老人或者儿童,一般会进行身份登记和体温测量。

可见,健康码事实上是一种以大数据为基础,对各地区公民的感染风险进行智能判断而生成、并动态更新的电子健康证明。尽管在使用初期,由于一些地方政府的懒政,将健康码的颜色标识从“基准”变成了“绝对标准”,但其本质上还是为了便于防疫而推行的辅助识别措施。有学者认为,健康码在行为类型上与行政评级相似,但其本身并没有直接引起行政法律关系的产生、变更或者消灭。[3] 因此,健康码不能代替核酸检测,其也不是法律规定的公民必须提供的身份证件。

1.2　收集个人信息的法理支点及法律依据

健康码的运行是以政府收集个人基本信息为基础。因此,我们有必要明确政府获取个人信息的法理支点及法律依据。风险社会背景下,人们对公共安全的担忧提升到一个前所未有的高度,对政府在保护公共利益方面的要求也越来越高。虽然公共利益绝不能凌驾与私人利益之上,但在两者发生冲突的情况下,必须进行利益衡量以保证社会的有序运行。[4] 在新冠疫情这场全人类的灾难面前,通过技术手段收集、使用个人信息以达到防控疫情的目的,是公共利益与个人权利权衡后的结果。面对国内数亿人的防疫工作,如果采取人工登记等传统手段,必将是杯水车薪,而利用大数据技术是最为高效的措施。相比于健康码带来的个人信息安全风险,优先保护公共安全更有利于实现效益最大化。当公民依靠自身力量已无法摆脱公共突发卫生事件带来的威胁时,借由政府收集和使用个人信息亦只是公民部分权利的临时性让渡。[5] 因此,健康码的应用是基于疫情防控与保护个人信息安全并重的法理逻辑,以保护个人的生命健康为根本目的。

虽然《民法典》明确规定个人的身份信息、健康信息以及行踪信息属于个人信息,受法律保护。但是,《民法典》第 1 035 条也规定了在法律、法规另有规定的情况下,可以不征得自然人同意收集个人信息。《突发事件应对法》《传染病防治法》和《突发公共卫生事件应急条例》都给了行政机关非常强的信息收集权,在没有个人授权下可以收集人口学信息,

如年龄、性别、位置等。“无需个人同意”并不意味着被收集人没有知情权,行政机关应明示信息收集的目的、范围以及方式,如江苏省的“苏康码”在信息收集时,会有详细的隐私协议告知被收集人。可见为了防控疫情的需要,健康码合理收集个人信息是合乎法理、法律的正当性举措,我们需要注意的应是政府如何收集个人信息以合乎比例原则。

2 健康码的应用对个人信息安全造成的风险

目前,对于收集个人信息所应遵循的规则很模糊,《民法典》中只原则性地规定了收集个人信息应合法、正当、必要,不得过度处理。在疫情防控中,很多有关保障信息安全的条款也只是原则性条款,缺少实际操作性。譬如,“为疫情防控、疾病防治收集的个人信息,不得用于其他用途”中,哪些属于“其他用途”并没有做详细规定。收集、保存、使用个人信息的规则不明确,可能导致个人信息遭到泄漏甚至滥用,给个人信息安全带来了极大的隐患。

2.1 信息泄漏风险

2.1.1 信息收集主体过多

如上所述,我国法律赋予了政府、卫生行政部门、疾病预防控制机构、医疗卫生机构等主体广泛的信息收集权。其中人民政府可以根据“突发公共卫生事件应急预案”将信息收集权再次授权给相关部门、机构或者组织,包括但不限于公安、基层群众自治组织。以节后合肥返乡人员登记为例,有三个主体对个人信息进行收集:公安部门对主要交通站点(火车站、飞机场、汽车站)的人员进行登记,村委会、居委会对辖区内返乡人员进行登记,高校对返校学生进行登记。但是,在实际操作中,很多法律授权和有权委托范围以外的主体。都可能收集个人健康码信息,如物业、商场、企业。此外,为健康码提供技术支持的互联网企业、电信公司也掌握着大量的个人信息。在水平参差不齐、数量众多的信息收集主体面前,个人信息泄漏的风险急剧上升。虽然我国对有权收集个人信息的主体做出了严格限定,但是在实际操作中存在的众多无权收集主体使得个人信息泄漏风险进一步累积。

2.1.2 信息过度索取

2020年11月13日,网信办发布“关于35款App存在个人信息收集使用问题的通告”,其中安康码的皖事通、湖北健康码的鄂汇办都存在过度收集用户信息等问题,如在收集用户身份证号、支付宝账号、过往病史时并没有明确告知用途及目的。北京、上海等部分城市健康码申请需要提交人脸特征等个人敏感信息,而其他省市的健康码(如湖北、江苏)却不以提交面部信息为必要申请条件。这也说明在没有采集人脸信息的情况下,并不影响健康码的正常运行。通过以上实例,我们不得不发出疑问,这些涉及到个人隐私的敏感信息与疫情防控有多大的关系?更令人担忧的是,信息的过度索取预示着未来可能对个人信息的利用超出必要的限度。近期,包括杭州等国内众多城市设想提出“渐变色健康码”,通过疫情期间集成的公民相关数据,探索建立个人健康指数排行榜。人们在疫情期间已经逐渐习惯于在公共场所填报个人信息,即使存在过度索取也很可能不以为然。当政府将包含人们隐私的个人信息随意取用时,那么公权力与私权利的界限将不再清晰。

2.1.3 信息重复索取

在健康码运行初期,各地纷纷推出本地健康码,不同省份健康码不同,甚至是同一省内各市的健康码也不统一。以长三角地区三省一市为例,上海有“随申码”,江苏有“苏康码”,安徽有“安康码”,浙江有“浙江健康码”。其中,江苏省除有“苏康码”外,还包括各市的“宁归来”“苏城码”“淮上通”“锡康码”等等。各地因为采取不同的技术标准,各自为营,数据难以打通。虽然国务院早已上线全国统一健康码,但从实践来看,各地还是以本省、市健康码为标准,要求返程人员必须申请注册本地健康码。[6] 本应是方便复产复工的健康码,因全国没有统一的标准,反而给跨省、甚至是跨市返程人员造成极大负担。互不相通的健康码使人们重复申请各地健康码,导致个人信息泄漏的风险增大。更为严重的是,各地对个人信息的保护措施存在差异,大多数省市在健康码申请注册程序中并未设置任何隐私保护条款,这就很可能使本受严格保护的个人信息在其他省市因重复索取而遭到泄漏。[7]

2.2 数据滥用风险

2.2.1 数据由企业储存并不安全

杭州健康码之所以能够在短时间内迅速推出并推广至全国,这与阿里巴巴公司背后的技术支撑密切相关。阿里巴巴旗下的淘宝、天猫、支付宝等产品在中国乃至世界范围拥有众多用户,面对海量数据的处理,其已拥有了完整、成熟、可靠的技术储备。在杭州市政府的牵头、协调下,阿里技术团队仅用4天就正式上线了杭州健康码,当天申领量达到134万。随后健康码在各地被推行,支付宝软件已涵盖上百城市的健康码。紧接着中国另一互联

网巨头腾讯公司也宣布在深圳推出全国首个“防疫健康码”,此后百度、美团等企业也纷纷加入健康码之争。如果说在紧急时期需要处理如此庞大的数据信息,政府借助企业的技术无可厚非,这也是企业利用自身优势积极承担社会责任的表现。但是随着众多科技企业纷纷加入这场投入巨大又“无利可图”的健康码之争时,仅靠“社会责任感”一说恐怕难以让人信服。

2.2.2　疫情后个人信息处理不明

虽然在健康码系统的管理和运行中,政府是数据控制者,企业只是数据处理者,必须按照政府的要求收集、储存数据。但是企业是存储着包含个人隐私等海量数据的服务器的实际拥有者,如果疫情过后企业私自将数据留存,那么企业便成了数据控制者。自疫情发生以来,人们出入小区、商场、车站等公共场所时,登记或展示个人信息已成为“新常态”。但是疫情过后,健康码等被各方储存的个人信息将何去何从,这成为人们心中的疑虑。尽管中央网络和信息化办公室早已发布《关于做好个人信息保护利用大数据支撑联防联控工作的通知》,要求对收集的信息采取动态删除。但此规定较为简单,没有明确规定具体的数据销毁程序以及后续检查制度。作为技术持有者的企业,如果在删除数据时有意留有后台,那么技术相对弱势的监管者将很难发现。虽然已有不少行业的信息收集主体作出声明,如多家航空公司在采集旅客信息时承诺,数据仅用于疫情防控,疫情结束后将全部销毁。但在《生物安全法》《个人信息保护法》《数据安全法》等相关法律中,就个人信息保障而言,立法修改进程明显滞后。若仅仅仰仗于存储海量个人信息数据的企业“自律”,那么人们对疫情后信息遭到滥用的担忧恐将成为现实。

3　个人信息使用常态化缺乏法律依据

在健康码成为疫情期间一项重要的防控手段后,不少地方政府开始考虑将健康码运用到日常社会治理中,推进健康码常态化。在创造出健康码的杭州,已有使用“渐变色健康码”的构想: 通过集成电子病历、健康体检、生活方式管理的相关数据,在关联健康指标和健康码颜色的基础上,探索建立个人健康指数排行榜,实现“一码知健”。此外,上海、苏州、广州等地都在考量如何将健康码实现升级转化,如作为市民的电子身份证或随身服务码。[8] 虽然,各地政府在接受媒体采访时表示健康码常态化只是一个设想,暂无具体实施时间。但是,这不妨碍将这看作是政府的一种试探,类似健康码的模式应用于日常的社会治理很可能成为现实。健康码的使用可以说是疫情防控的一项权宜之计,是公共健康与个人隐私之间短暂的取舍,在突发公共卫生事件中公共利益的价值位阶高于个人的信息自决权。[9] 但无论是《民法典》,还是《传染病防治法》《突发公共卫生事件应急条例》都规定了只有在突发公共卫生事件下,政府才能够不经同意大规模收集个人信息,且不能用于其他用途。因此,如果疫情后政府继续使用健康码所采集的数据,那么就可能涉嫌滥用个人信息; 如果使用的数据不是由健康码升级而来,那么则可能涉及违法收集个人信息。

在此次新冠疫情防控中,我们深刻体会到大数据技术在社会治理中的巨大优势,但同时也应认识到其对个人信息安全带来的威胁。行政管理者不能一味追求“数字治理第一城”而逾越公权力行使的边界,将个人信息安全抛之脑后。在大数据时代,需要建立完善的制度以规范政府收集和使用个人信息,而对健康码应用下个人信息安全风险的探讨或许只是刚刚开始。

参考文献:

[1] 乌尔里希·贝克. 风险社会[M]. 译林出版社,2004: 15-16.

[2] 陈禹衡,陈洪兵. 反思与完善: 算法行政背景下健康码的适用风险探析[J]. 电子政务,2020(8): 93-101.

[3] 查云飞. 健康码: 个人疫情风险的自动化评级与利用[J]. 浙江学刊,2020(3): 28-35.

[4] 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(2): 5-16.

[5] 鲍坤. 健康码数据常态化应用的比例原则限制[J]. 电子政务,2021(1): 32-41.

[6] 新华网. 期待全国统一健康码发挥更大作用[EB/OL]. (2020-02-18)[2021-03-10]. http://www.xinhuanet.com/comments/2020-02/18/c_1125589441.htm.

[7] 澎湃新闻. 14 省市健康码仅 3 地有知情同意和隐私保护条款[EB/OL]. (2020-04-30)[2021-03-10]. https://www.thepaper.cn/newsDetail_forward_7210904.

[8] 珠江时报. 如何让健康码越“长大”越“健康”? [EB/OL]. (2020-06-08)[2021-03-10]. http://szb.nanhaitoday.com/epaper/zjsb/html/2020-06/08/content_10078.htm.

[9] 李晓楠. “数据抗疫”中个人信息利用的法律因应[J]. 财经法学,2020(4): 108-120.

[责任编辑: 李玉年]