Open Journal of Legal Science 法学, 2022, 10(5), 784-793
Published Online September 2022 in Hans. http://www.hanspub.org/journal/ojls
https://doi.org/10.12677/ojls.2022.105100

Hans汉斯

后疫情时代“健康码”个人信息保护新探

王舒宁

山东建筑大学法学院，山东 济南

收稿日期：2022年6月30日；录用日期：2022年7月13日；发布日期：2022年9月5日

摘　要

健康码通过整合时间、空间和人员三个维度的信息，即时改变二维码的颜色从而有效地完成疫情的实时监测、重点筛查和有效预防。当前我国疫情得到有效控制，各领域重回正常运转，后疫情时代来临，防疫进入常态化。社会背景的转变意味着健康码从应急防控转入常态化应用场景，其运作及延展应用离不开对个人数据的使用，与个人权利息息相关，面临着一系列的风险与挑战，导致个人信息保护步履维艰。对此，通过总结健康码领域个人信息保护现存的发展困境，引入法律原则，就原则体系加以精修填补，界定权限范围，制定合理标准以保障个人信息安全，奠定健康码常态化应用之合法性。

关键词

后疫情时代，健康码常态化，个人信息保护

New Research on Personal Information Protection of “Health Code” in the Post-EPIDEMIC Era

Shuning Wang

Law School, Shandong Jianzhu University, Jinan Shandong

Received: Jun. 30th, 2022; accepted: Jul. 13th, 2022; published: Sep. 5th, 2022

Abstract

By integrating the information of time, space and people, the health code can change the color of the QR code instantly to effectively complete the real-time monitoring, key screening and effective prevention of the epidemic. At present, the epidemic in China has been effectively brought under

文章引用: 王舒宁. 后疫情时代“健康码”个人信息保护新探[J]. 法学, 2022, 10(5): 784-793.
DOI: 10.12677/ojls.2022.105100

control, and all sectors have returned to normal operation. The post-epidemic era is approaching, and epidemic prevention has become normal. The change of social background means that the health code has changed from emergency prevention and control to regular application scenarios. Its operation and extended application cannot be separated from the use of personal data, which is closely related to individual rights and faces a series of risks and challenges, making it difficult to protect personal information. Therefore, summarize the existing development difficulties of personal information protection in the field of health code, introducing legal principles, elaborating and filling the implementation of each principle, defining the scope of authority, establishing reasonable standards to protect personal information security, and establishing the legitimacy of the regular application of health code.

Keywords

Post-Epidemic Era, Health Code Normalization, Personal Information Protection

1. 问题的提出

1.1. 背景与起因

2020 年初，各地方政府为抗击疫情，将个人健康信息码系统作为疫情管控、社区管理、个人出行三位一体的重要数字化抗疫工具。[1]其数据基础来源于公民在疫情时期的信息填报，通过整合统计到的信息，利用数据云算法技术处理后形成红、黄、绿三色二维码，防疫人员在日常的生活中可以通过二维码的颜色来判定持有人是否存在携带和传播新冠肺炎病毒的风险。

根据我国公安部第一研究所参与编制的《个人信息健康码》3 项国家标准[1]，健康码数据包括公民个人基本信息、健康信息、行程信息以及同居人信息等，根据《民法典》[2]第 1034 条[3]、《个人信息保护法》第 4 条[4]以及《网络安全法》第 76 条[5]之规定，以“识别性”作为个人信息的判定标准，健康码数据具有强识别性。根据《个人信息保护法》第 28 条[6]之规定，健康码中的健康生理信息、生物识别信息，日常出行轨迹以及过往病史都属于“敏感信息”。为适应疫情防控的灵活需求，健康码以“互联网+”可信身份认证的平台为基础，将收集的身份信息与一体化政务服务平台整合的国家卫生健康部门汇聚的确诊或疑似患者数据[2]，同时依据交通部门收集的资源，整合确定确诊或疑似患者的同乘者数据以及全国各

[1] 我国公安部第一研究所参与编制的《个人信息健康码》国家标准已正式发布，由 GB/T38961-2020《参考模型》GB/T38962-2020《数据格式》和《应用接口》3 项组成。
[2] 为阅读方便起见，本文所引我国法律、法规均省去“中华人民共和国”，例如，《中华人民共和国民法典》本文简称为《民法典》，其他所引的我国法律法规均同此例。
[3] 《民法典》第 1034 条：个人信息是以电子或者其他方式记录的能够单独或者与其他信息结合识别特定自然人的各种信息，包括自然人的姓名、出生日期、身份证件号码、生物识别信息、住址、电话号码、电子邮箱、健康信息、行踪信息等。
[4] 《个人信息保护法》第 4 条：个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括匿名化处理后的信息。个人信息的处理包括个人信息的收集、存储、使用、加工、传输、提供、公开、删除等。
[5] 《网络安全法》第 76 条：个人信息，是指以电子或者其他方式记录的能够单独或者与其他信息结合识别自然人个人身份的各种信息，包括但不限于自然人的姓名、出生日期、身份证件号码、个人生物识别信息、住址、电话号码等。
[6] 《个人信息保护法》第 28 条：敏感个人信息是一旦泄露或者非法使用，容易导致自然人的人格尊严受到侵害或者人身、财产安全受到危害的个人信息，包括生物识别、宗教信仰、特定身份、医疗健康、金融账户、行踪轨迹等信息，以及不满十四周岁未成年人的个人信息。

地健康码数据进行关联和绑定[3]。完备的平台及信息机制构建为健康码的常态化应用奠定了良好基础。健康码作为防疫数字化工具，可以维护社会整体利益，其数据的收集及运用得到《突发事件法》、《传染病防治法》等规定的许可，许可的原因在于当面临社会整体重大突发事件时，公民应适当让步一部分权利交由公权力统一行使，因此疫情防控背景下的公共利益价值位阶高于公民的个人信息法益[4]，健康码的产生与应用至此有了正当性基础。

1.2. 演化与争议

1.2.1. 健康码常态化的演进历程

随着疫情防控战线的不断拉长，健康码的应用范围越来越广、承载的数据越来越多，适用范围由各省份内部应用逐渐扩大到全国，各省份间的健康码数据更加互联互通。种种现象表明，健康码应用已步入常态化进程，例如：杭州市卫建委召开了关于“杭州健康码常态化应用工作部署”[5]的会议；全国各省市将健康码应用到日常生活检查之中，公民进出商场、景点、办公单位等场所时都应当先出示健康码，我国社会公众的日常生活处处离不开健康码的参与。在此背景下，健康码好似无形的摄像头，时时刻刻监控着人们的一举一动。故为了适应当前发展局势，国家已于 2020 年正式发布《个人信息健康码》国家标准，由 GB/T38961-2020《参考模型》GB/T38962-2020《数据格式》和《应用接口》3 项组成。

1.2.2. 后疫情时代的演进历程

“疫情时代”跨越到“后疫情时代”，首先可以看出两者发生的时间具有先后顺序，具有承接的关系。其次“后”字的出现难免会让人认为这里指的是“疫情结束后的时代”，但事实并非如此，当今世界呈现出各国紧密相连的发展趋势，虽我国当前疫情现状相较于 2020 年初有了质的好转，大面积的新冠疫情已经结束，但就世界整体而言，日新增确诊病例仍破万，世界整体仍处于疫情时代。与此同时，我国各地疫情时起时伏，国外疫情防控现状导致的回流也会产生相应的影响，病毒毒株仍不断变异，从“德尔塔”到“奥密克戎”，病毒在短期内并不会从人们的生活中消失，随时都有小范围内爆发疫情的风险。

将我国当下所处的时代界定为“后疫情时代”主要是有以下三点原因：其一，从世界范围内进行综合考量，我国整体防疫工作取得了重大战略成果，坚持动态清零方针，疫情防控状态已从应急转向常态化，积累了众多经验；其二，我国经济整体发展水平呈现平稳向上之趋势，正在有序弥补疫情所带来的冲击，我国在疫情防控的基础上，正常进行对外经贸往来；其三，社会经济、文化、医疗等领域在经历疫情后产生了相应的变化，公民的生活习惯、学习工作方式以及消费观念都有所改变，逐步适应疫情带给社会方方面面的影响。综上，“后疫情时代”的内涵在于疫情得到有效控制，进而在全社会展开防控常态化的基础上，各领域重回正常运转，经济发展水平得以恢复的时代。

1.2.3. 演进之争议所在

受病毒的特性以及疫情的不确定性，后疫情时代我国需要随时做好应对疫情突发的准备。健康码作为防控常态化时期的特殊通行证，提高了公民的出行效率、加快了密切接触者的隔离速度，同时确诊的患者也可以得到及时救治，从而降低了疫情传染的风险。但常态化对健康码的功能提出了更高标准的要求，在此背景下，健康码的功能不断加以扩展，使其背负着更多样的数据信息，增加了公民的部分健康信息和行为信息，其中健康生理信息、生物识别信息，日常出行轨迹以及过往病史都属于《个人信息保护法》中的“敏感信息”。随着后疫情时代的来临，健康码数据的常态化运用导致公民的敏感信息将继续留存在政府机关和各大企业，同时个人生活中的许多底层信息也以健康之名被逐步纳入采集范畴[6]，

有关健康码数据泄漏及个人信息问题滥用问题引发愈来愈多的争议。

2.“健康码”领域之个人信息保护困境

2.1. 研发企业权限相较过大

健康码的运行多由国内各大互联网公司主导，譬如阿里巴巴、腾讯以及浪潮集团等，这是由于互联网公司拥有大量的用户数据，具有天然优势。在防疫背景下的政企合作中，政府先是让与了部分公共管理权，再是允许平台获取了公众的个人信息[7]。健康码生成目的在于维护公共安全的有序以及公民个体的人身安全，其保护主体是公众，具有整体性和普遍性两大特点[8]，是我国数字抗疫的一部分，应当由公权力占据主导地位，当前的发展现状有违健康码应用的初始目的。同时个人数据在当今具有重要的财富价值，互联网公司通过健康码掌握着大量详细的公民信息，且健康码常态化的发展使得这些企业仍将长时间控制这部分数据，若不加以严格管控，随时可能产生数据泄露的风险。

例如在 2020 年底，“健康宝照片泄露”事件[7]正是由于健康宝研发公司中关村科学城城市大脑股份有限公司缺乏内部个人信息保护合规要求，开发出“他人代查”这一选项，使得大量公众人物健康宝照片被泄露。这一事件的发生不仅表明负责采购和推广使用健康宝的部门或者企业存在明显的个人信息保护意识不足的问题，而且表明在北京健康码被投入使用前并没有进行个人信息保护是否合规的检测。

2.2. 个人信息“匿名化”的处理力度相较不足

根据《网络安全法》第 42 条第 1 款[8]的规定可知“匿名化”的个人信息是指“经过处理无法识别特定个人且不能复原的信息”，由此认为对个人数据进行“匿名化”处理之后便无法识别信息主体的真实身份[9]。健康码涉及的各类信息若不经过“匿名化”处理将会导致很多不必要的困扰[10]。例如，“成都新冠肺炎确诊女孩信息外露事件”[9]的发生正是由于健康码数据的“匿名化”处理程度较轻，导致确诊患者的个人数据泄漏，遭受被人肉搜索及网络暴力的后果。由此可见，在实际运用过程中，“健康码”领域关于个人信息“匿名化”的处理力度相较不足。

2.3. 独立的监管机构缺位

我国并无统一且独立的个人信息保护主体，仅由中央网信办、工信部、卫健委等部门共同承担个人信息领域的监管工作。以上各部门分管不同领域，呈现出明显的部门区隔特征，相互掣肘的现象时有发生，导致行政执法权责不清，不同机关冲突又难以协调[11]。“健康码”在生成之时，因情况紧急并没有就个人信息监管主体进行明确的设定。随着“后疫情时代”的来临，健康码的常态化运用使得该领域的个人信息监管出现了“空白地带”，无法有效保障“健康码”在个人信息保护与疫情防控等公共利益之间的平衡。

[7]在“明星健康宝照片被泄露”(此处“健康宝”指的是北京健康码)事件爆发前，在健康宝小程序中，除了“本人健康码自查询”、“本人信息扫码登记”等功能，还有“他人健康码代查询”功能。而此次“明星健康宝照片泄露”风波，正是起于“他人健康码代查询”功能。此前通过健康宝输入姓名、身份证号码，无需再次人脸识别，即可查询到他人的健康宝照片。而明星个人信息泄露严重，正是钻了健康宝“他人代查”规则的漏洞，大量明星健康宝照片被泄露甚至被叫卖。详见刘青青、石丹。健康宝照片泄露风波背后，中科大脑陷信任危机[J]。商学院，2021(2)：62-64。

[8]《网络安全法》第 42 条第 1 款：网络运营者不得泄露、篡改、毁损其收集的个人信息;未经被收集者同意，不得向他人提供个人信息。但是，经过处理无法识别特定个人且不能复原的除外。

[9]成都曾于 2020 年 12 月 8 日公布了新增确诊病例活动的轨迹，其中一位患者赵某是之前确诊病例的孙女，但“成都确诊病例孙女”的词条却登上热搜；原因在于赵某自身健康码记录下的活动轨迹牵涉酒吧等场地，一张具体到时间、地点的赵某活动轨迹图随后在网络热传，赵某的私人信息更遭到“人肉”，姓名、身份证号等信息一一公布。详情可见左翊庭、王田阳。疫情背景下公众知情权与公民隐私权的冲突及解决—以成都新冠肺炎确诊女孩信息外露事件为例[J]。西部学刊，2021(08)：49-51。

2.4. 现有法律原则进路的困惑与缺位

2.4.1. 存在知情同意原则被虚置的风险

我根据《民法典》第 1035 条[10]、《网络安全法》第 41 条第 1 款[11]、《个人信息保护法》第 14 条第 1 款[12]以及《信息安全技术个人信息安全规范》第 5 项的规定均强调了知情同意原则，即信息处理主体在收集个人信息时，需履行告知义务，征得个人信息主体明确、具体的同意。这一在原则在健康码《参考模型》3.5 款[13]和 7.5 款[14]中均有所规定。

知情同意原则诞生于医疗领域，其最初演进确立的目的在于让患者自己决定应当接受何种诊疗，而非一味地让医生下决定。随着信息时代的来临，知情同意原则在个人信息保护领域发生嬗变，成为个人信息保护的帝王性条款。各大 APP 在用户开始使用前提供平台隐私政策条款，虽用户拥有自主决定的权利，但用户一旦选择拒绝则无法正常享有 APP 厂商提供的服务，实际上，用户只面临着 2 类选择，即完全同意或放弃，但微信、支付宝等 App 早已成为公众生活的一部分，无法放弃使用的情况下只能被迫选择同意。同时大多数 APP 平台采用隐私政策一次性的同意方式，加大了知情同意原则被虚置的可能。例如俞某诉支付宝、天猫超市案[15]中，体现出 App 对用户知情同意原则的弱化。

健康码领域同样出现知情同意原则被虚置的现象，有两个方面加以论证。其一，大多数省市在健康码申领程序中并未设置任何知情同意、隐私保护条款[16]，例如山东健康码在用户填写个人信息时并没有作出相关提示。公众对于收集信息的范围、具体使用模式并不了解，例如黄冈的一位确诊患者在新冠治愈 2 个月后，自己的健康码依然是红色的，没办法及时复工，经咨询才得知由“红码”变为“绿码”并非系统自动识别，应当由“符合条件的市民需要主动提交转码申请”[17]。其二，随着健康码常态化的发展，这枚小小的二维码应用频率有增无减。虽健康码是个人通过实名认证在手机 APP 上自主选择申领得到的，但健康码在实际运用过程中无法完全被知情同意原则所约束。例如公民乘坐交通工具出行之时也被要求出示健康码，进入超市、景区时同样需要出示二维码，因此健康码具有现实层面上的强制使用性，健康码成为公民在疫情常态化背景下必不可少的正常生活工具。种种案例揭示了健康码常态化使用过程中存在知情同意原则被虚置的风险。

2.4.2. 产生最小必要原则被逾越的情形

根据《个人信息保护法》第 6 条[18]和《信息安全技术个人信息安全规范》第 4 条[19]的规定，最小必要原则为我国法律实践中被普遍接受的个人信息处理原则，其源于“比例原则”[20]，现以“最小”来界定

[10]《民法典》第 1035 条规定：“处理个人信息的，应当遵循合法、正当、必要原则，不得过度处理，并符合下列条件：(一)征得该自然人或者其监护人同意，但是法律、行政法规另有规定的除外。”

[11]《网络安全法》第 41 条第 1 款：“网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

[12]《个人信息保护法》第 14 条第 1 款：基于个人同意处理个人信息的，该同意应当由个人在充分知情的前提下自愿、明确作出。法律、行政法规规定处理个人信息应当取得个人单独同意或者书面同意的，从其规定。

[13]GB/T38961-2020《参考模型》3.5 规定：健康码的申请使用要经过公民的明示同意。

[14]《参考模型》7.5 规定：个人健康信息服务及其应用采集数据时，应获取用户的明示同意或授权同意。

[15]参见(2018)京 0108 民初 13661 号民事判决书，俞某在乐友清河线下店购买商品并使用支付宝支付时，则默认授权将自己在乐友清河店发生的交易详细信息显示在天猫客户端中，使个人交易信息泄露。当 App 用户选择同意协议，就意味着用户本身并无选择余地。

[16]参见《14 省市健康码仅 3 地有知情同意和隐私保护条款》，载澎湃新闻 2020 年 4 月 3 日，http://m.cnwest.com/tianxia/a/2020/04/30/18710830.html.

[17]参见《新冠肺炎治愈后两个月为何还是红码？》，载澎湃新闻 2020 年 4 月 24 日，https://www.163.com/dy/article/FB0EN1AO0514R9P4.html.

[18]《个人信息保护法》第 6 条：处理个人信息应当具有明确、合理的目的，并应当与处理目的直接相关，采取对个人权益影响最小的方式。收集个人信息，应当限于实现处理目的的最小范围，不得过度收集个人信息。

[19]《信息安全技术个人信息安全规范(GB/T 35273-2020)》第 4 条；最小必要原则要求“只处理满足个人信息主体授权同意的目的所需的最少个人信息类型和数量。目的达成后，应及时删除个人信息”。

[20]欧盟《通用数据保护条例》中的数据最小化原则被认为符合欧盟《基本权利宪章》第 52 条第 1 款关于限制基本权利应遵循比例原则的规定。参见[日]宮下紘『EU 一般データ保護規則』(勁草書房，2018 年) 47 頁。

“必要”所需的范围。最小必要原则主要包括：其一，相关性，根据《个人信息保护法》第 6 条第 1 款的规定，健康码收集信息的种类须与抗击疫情的目的所相关；其二，符合比例，即处理个人信息所带来的风险应当与所保护的法益大小成正比。故健康码在处理个人信息时应牢牢把握抗疫之大方向，同时尽可能保持克己谨慎[12]；其三，最小化，即个人信息处理应限制在离开某项个人信息的处理，就无法合理实现最终目的的范围内。在健康码信息处理过程中应在实现目的的范围内尽可能少地收集个人信息数量及类型、尽可能低地减少数据共享范围，尽快将处理完不再需要的信息数据删除。

健康码常态化过程中个人信息重复收集以及超越收集范围的现象频频发生，此处通过举例证明健康码常态化过程中最小必要原则形同虚设。例一：山东省健康码的申领并不需要市民进行人脸识别，但在北京则需要进行人脸识别。这一差异可知人脸识别并不是健康码正常运行的必备条件。由此可见健康码在生成过程中存在重复收集公民信息，扩大了收集范围的行为，违背了个人信息保护的最小必要原则；例二：在健康码常态化的过程中，大量企业基于健康码技术成本低、获利高而纷纷投身于此，除阿里巴巴、腾讯两大数据业巨头主导健康码平台运作外，百度及美团也开始提供相关服务，随着政府和企业合作的深入，个人信息被重复收集利用的现象愈演愈烈；例三：苏州新推出了“文明码”，主要通过收集市民的个人信息以及日常的行动轨迹和多个政府部门的数据以数据算法的方式给每个市民的文明程度下判断，显然这一举措超越了健康码诞生的最初目的和治理边界，造成了公民个人信息的过当利用，扩大了个人信息收集范围。

2.4.3. 出现公开透明原则被忽略的可能性

根据《个人信息保护法》第 7 条[21]、《网络安全法》第 41、42 条[22]及《消费者权益保护法》第 29 条[23]的规定以上条文规定了个人信息保护的公开透明原则，即个人信息收集后的控制者与处理者应以公开透明的方式对信息进行处理同时使信息主体知悉，信息主体对利用个人信息处理的目的、方式方法、内容都享有知情的权利。

在实践中，公民提交完个人信息申领完健康码之后并不了解个人的数据信息将会被如何处理，因而在健康码的生成过程中易导致信息“黑箱”[24]的产生。同时公民无法对健康码生成过程中使用的个人信息进行查询和更正，只能通过系统的申诉渠道对“健康码”的结果提出异议[13]。公民在日常生活中往往会有跨省行程，因此需要申领多个地区的健康码，例如山东省市民若因行程需要去北京则应当提前申领北京健康码才可顺利入京。虽然根据《参考模型》[25]的规定，我国已经实现各地各领域健康码的互通互认，但健康码背后的数据处理及流通方式仍然存在一定的差异，各地区对于健康码数据处理方式的不同更易导致信息管理黑箱的产生，公民在此过程中并不知悉个人数据将会被如何处理，出现公开透明原则被忽略的可能性。

3. 破解困境与完善建议

3.1. 明确健康码研发、管理及核验主体权限

1) 以公权力为主导，明确健康码关于公民个人信息的收集目的在于抗击疫情所必需，其用途必须是

[21]《个人信息保护法》第 7 条：处理个人信息应当遵循公开、透明原则，公开个人信息处理规则，明示处理的目的、方式和范围。

[22]《网络安全法》第 41~42 条：网络运营者收集、使用个人信息，应当遵循合法、正当、必要的原则,公开收集、使用规则,明示收集、使用信息的目的、方式和范围,并经被收集者同意。

[23]《消费者权益保护法》第 26 条：经营者收集、使用消费者个人信息，应当遵循合法、正当、必要的原则，明示收集、使用信息的目的、方式和范围，并经消费者同意。经营者收集、使用消费者个人信息，应当公开其收集、使用规则，不得违反法律、法规的规定和双方的约定收集、使用信息。

[24]“信息黑箱”通过信息不对等与黑箱的隐秘性，影响信息的正常输出结果，个人无法得知信息在经由发布者发布之后是否有失真、变质、被替换或被二次加工的行为。当我们作为信息接收者接收到信息后，根据我们得出的信息作出反馈，而这个反馈正是信息黑箱导致的结果。

[25]《GB/T38961-2020 参考模型》规定：“健康码由ＡＢＳ这 3 段组成”，其中“Ａ段代表个人信息主体的身份、Ｂ段代表码的类型、Ｓ段代表了健康码跨地区互认的技术规制原则。

接触者追踪等以疫情防控为目的的事项。限定健康码研发的主体必须是政府或者经其批准、授权的开发者，其余主体一律不得擅自收集个人信息进行研发；健康码的平台管理者和核验主体必须经过政府或经其批准、授权。

2) 督促健康码研发及管理企业在内部建立信息安全保护架构，提升企业内部的个人信息保护意识，制定完备的企业内部个人信息保护合规体系。主动全面地进行动自查自纠，一旦产生信息泄漏，及时采取补救措施，按照规定告知自然人并向有关主管部门报告。当泄漏发生后，追根溯源，寻找症结所在，加大信息泄漏惩罚成本，并不能仅仅以罚款收场，针对企业的信息泄漏问题，建立行业“黑名单”制度，向社会发布风险预警，降低企业信誉，使其在行业内寸步难行。

3.2. 提升个人信息“匿名化”力度

当前我国小规模疫情与散发疫情交织，政府公布最新确诊患者的流调信息时都会进行匿名化处理，避免将信息主体身份显化[14]。若匿名化处理程度较轻，则会导致确诊患者的个人数据泄漏，产生“被人肉”以及网络暴力的可能性。“成都新冠肺炎确诊女孩信息外露事件”的发生表明我国在健康码领域，应加大个人信息“匿名化”处理力度。

1) 就个人信息“匿名化”设定国家标准，《信息安全技术个人信息去标识化指南》已于 2017 年进行立项，“匿名化”成为个人信息保护领域的一项发展共识。首先，在制定技术标准时，应当列明具体的“匿名化”过程，即所需要的程序；其次，根据数据泄露的风险大小以及个人信息的重要程度，分别加以评估，建立弹性标准。对于向社会公告的信息，应采用力度最大的“匿名化”处理方式，即隐去当事人所有的直接标识符，如：姓名、具体职位等，适当保留性别、年龄及行踪等间接识别符；最后，制定标准时应当明确信息“匿名化”后的留存期限下限，进而有效提高个人信息匿名化处理的有效程度。

2) 引入第三方认证机制，由于“匿名化”手段不仅涉及个人信息保护，也涉及数据处理技术规制。政府在进行处理的过程中引入第三方认证机制，凭借其专业性更容易实现与被规制者之间实现信息共享，进而及时纠正匿名化过程中出现的违规行为。第三方认证机构具有完备的人才储备以及领先的技术优势，设立第三方认证机制，可及时对个人信息匿名化的处理力度加以检查及监督，避免纰漏的出现。

3.3. 完善个人信息监管职能及机构设置

随着后疫情时代的来临，健康码自身功能随着常态化进程而不断增加，个人信息保护的风险也随之增加。我国尚未设立统一且独立的个人信息保护机构，个人信息的收集运用仍由多个部门联合加以监管，分散的监管模式并不利于个人信息保护制度的健全发展。亟需借鉴欧盟等相关国家的先进经验，构建我国的个人信息监管保护主体。

在后疫情时代，为维护健康码常态化运用设置个人信息保护机构，其主要职责应有：1) 向健康码的收集、研发、管理及核验主体说明个人信息保护的重要性，使其产生敬畏心理；2) 编写具体指引，积极开展各项管理工作；3) 监管健康码在实际中的运行情况，对细微瑕疵问题加以完善和修复；4) 发现“健康码”在使用过程中有信息泄漏问题发生应及时加以制止，并进行处罚整治；5) 应当接收关于侵犯个人信息利益的举报行为，提供相应的救济手段，当证据确凿时，联系公安机关追究其刑事责任[4]。

3.4. 对各项法律原则的应用加以精修填补

3.4.1. 明确知情同意原则的让步与坚守

在“健康码”具体应用过程中，知情同意原则作为个人信息保护的基本原则，需权衡防疫公共需要和公民个人信息保护之间的关系，为了整体防疫需要，应作出适当让步。从字面理解，知情同意原则由两部分组成：“知情”和“同意”，指当事人在充分了解、知悉具体情况的基础上主动对某一事项加以

同意。故此处以“同意”规则的让步、“知情”规则的坚守加以论述，以期最大程度完善“健康码”之个人信息保护。

《杭州健康码开发运行规范管理办法》明确将授权同意作为健康码运行的基本原则之一。根据上文可知健康码领域出现了知情同意原则被虚置的现象，健康码的适用成为一种隐形的强制手段。防疫的重要性难以忽略，若不同意被收集个人信息，公众便无法正常持有并使用健康码，这一现象无疑增加了疫情防控难度，试想一下若未经出示健康码便随意乘坐各类类交通工具、进出各类公共场所，那必定会导致防疫盲区的形成。同时根据《信息安全技术个人信息安全规范》第 5 条[26]以及《民法典》第 1036 条[27]的规定，为确保防疫系统的有效运行，保护公共卫生安全，健康码中的知情同意原则可作出适当让步，其使用无须经个人信息主体的同意。

虽为了社会整体的疫情防控需要，授权同意规则在健康码的使用过程中有所放宽，但仍应坚持知情原则。首先，健康码的运营主体可运用简单易懂的语言设置隐私协议让公众获知信息处理范围、疫情防控需要之目的、具体的使用方式以及信息储存的期限，同时采用明显符号向公众提醒；其次，健康码的运营主体应定期向公众提供提出具体的信息变动情况，对相关的技术升级应当及时告知公众并加以详细说明，例如，健康码常态化的过程中，功能日益多样，打开健康码便可以查询自己的核酸检测情况，对于这类技术升级，政府和健康码运用主体应当及时告知公众并说明具体的运用方式，让公众对于健康码的更新内容加以知晓，避免对此产生困惑。

3.4.2. 充分保障公开透明原则

在“健康码”具体应用过程中，政府为充分保障公开透明原则应当向公民及时反馈其信息处理过程中的相应变化。主要包括：1) 确保公民知悉申领健康码的原因、申领健康码需要涉及到哪些个人信息以及健康码的变色原理；2) 告知公民健康码的颜色变化与日常出行紧密相关[11]，黄码以及红码用户会受到出行的限制；3) 为确保公众配合，打消其疑虑，应向其告知健康码是如何跟踪监测公民的出行信息以及如何获取其同行、同乘者的信息；4) 应当告知公民健康码运行时是如何管理储存各项信息的，从而减轻公民对于自身信息泄漏的担忧程度。

实践中已有地方政府为贯彻公开透明原则出台相关文件，如上海市“随申码”、广东省“粤省事”在注册时需用户点击同意政府运营管理机构制定的用户协议和隐私政策；针对这一原则深圳市政府还编制了《健康码操作指引》，向用户告知“健康码”汇聚分析的数据类型、申诉渠道等。

3.4.3. 有效遵循最小必要原则

在“健康码”具体应用过程中，个人信息的收集对象和收集范围都应当遵循最小必要原则。健康码收集的信息范围应围绕抗疫需要而展开，譬如公民的姓名、身份证号、联系电话、健康信息和出行轨迹信息、交通出行信息、家庭成员信息、工作单位信息等，超出此范围的信息并不是为了防疫需要而存在，因此禁止个人资产、家族病史、婚姻状况等非必要信息的大肆收集。

3.5. 提升技术标准

由上文可知，我国已于 2 年前正式发布《个人信息健康码》等 3 项国家标准，随着后疫情时代的来临，健康码在 2 年间的时间里被赋予了更多的功能，故该项国家标准应当及时加以更新，满足更深层次的使用需求。

[26]《信息安全技术个人信息安全规范》第 5 条：以下情形中，个人信息控制者收集、使用个人信息不必征得个人信息主体的授权同意：与公共安全、公共卫生、重大公共利益直接相关的。

[27]《民法典》第 1036 条：处理个人信息，有下列情形之一的，行为人不承担民事责任：(三)为维护公共利益或者该自然人合法权益，合理实施的其他行为。

1) 在 GB/T38961-2020《参考模型》3.4 项[GB/T38961-2020《参考模型》3.4：个人信息控制方：有能力决定个人信息处理目的、方式等的组织或个人。]中对于个人信息控制者的规定并不够完善具体，这一规定在健康码的常态化发展过程中显得较为单薄，越来越多的企业组织或个人都想借着健康码这一新兴事物在个人信息领域谋利益，加剧了个人信息泄漏的风险，故当前我国应当进一步完善关于个人信息控制者这一标准；在该标准的 8.1 项[GB/T38961-2020《参考模型》8.1：身份认证要求：健康码出示前应先进性用户实名使人认证，相关认证宜通过至少一种用户生物特征识别。关于身份认证的要求中规定公民在申请健康码时至少应提供一种生物识别特征，针对这一标准应对生物识别类型加以详细明确的规定，形成统一规范，例如：都需要且只需要通过人脸识别技术来进行实名实人认证；该标准也未针对健康码设立专门的监管机构，难免会导致健康码各阶段个人信息泄漏事件的发生，现行标准应针对这一现象增加相关规定，保障个人信息安全。

2) 国标 GB/T38962-2020 《数据格式》中信息种类规定不够全面，在健康码常态化的过程中，健康码体现公民接种疫苗的信息成为常态化的突出表现之一，公民在接种完新冠疫苗之后，健康码下方会出现“新冠疫苗接种查询”的提示，点进去便会清晰看到关于个人接种疫苗的接种机构、接种时间、接种针次、疫苗类型和疫苗厂家信息，但在标准中并未对疫苗的各类信息的数据元属性和数据格式加以规定，故 GB/T 38962-2020 中的数据种类也要及时加以更新。

4. 结语

随着“疫情时代”向“后疫情时代”的转变，社会整体发展开始有序回归，健康码不断被关联更多的个人信息数据、被赋予更多的功能，呈现出常态化应用之进程。健康码的长效应用不仅揭示了个人数据应用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。

健康码作为大数据背景下抗疫手段的创新性实验，其发展应用离不开对公民个人信息的收集、处理，常态化的发展进程使得健康码愈发与个人信息的适用息息相关，引发了一系列的个人信息安全风险。基于紧迫的防疫需求，政府在健康码研发之际让渡部分公权力，允许企业获取公众的个人信息，导致研发企业的权限相较过大，在个人信息处理过程中“匿名化”的力度缺乏明确的标准且独立监管机构的缺位导致个人信息保护遭受阻碍。结合《个人信息保护法》等规定不难看出“健康码”个人信息保护进路出现了法律原则缺位之现状，虚置知情同意原则、逾越最小必要原则、忽略公开透明原则的个人信息处理活动时有发生。

为破解健康码个人信息保护之困境，本文以明确权限、制定标准、完善机构设置、落实各项法律原则、提升技术等方面出发，提出具体举措加以完善个人信息保护的发展路径。个人信息保护力度锚定了健康码常态化进程的方向，或黑或白，或继续为抗疫展现强大力量或退出历史发展舞台，个人信息安全成为“健康码”两极发展之关键所在。

参考文献

[1] 王贵国. 国际公共卫生秩序与后新冠前瞻[J]. 中国政法大学学报, 2020(5): 5-27.

[2] 仇保利. 中国特色网络可信身份战略实践——互联网+可信身份认证平台[J]. 警察技术, 2020(3): 7-10.

[3] 国伟, 李恒训, 黄耀晖, 郝久月. 基于网证的“防疫健康信息码”应用研究[J]. 信息安全研究, 2020(9): 791-797.

[4] 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.

[5] 集众力 汇众智 市卫健委全力深化杭州健康码常态化应用[EB/OL]. http://wsjkw.hangzhou.gov.cn/art/2020/5/23/art_1229113672_47550183.html, 2020-09-02.

[6] 刘迎霜. 大数据时代个人信息保护再思考——以大数据产业发展之公共福利为视角[J]. 社会科学, 2019(3): 100-109.

[7] 方兴东, 严峰. “健康码”背后的数字社会治理挑战研究[J]. 人民论坛·学术前沿, 2020(16): 78-91.
[8] 梁上上. 利益衡量的界碑[J]. 政法论坛, 2006, 24(5): 66-80.
[9] 金耀. 个人信息去身份的法理基础与规范重塑[J]. 法学评论, 2017(3): 120-130.
[10] 王晨光. 疫情防控法律体系优化的逻辑及展开[J]. 中外法学, 2020, 32(3): 612-630.
[11] 许可. 健康码的法律之维[J]. 探索与争鸣, 2020(9): 130-136+160.
[12] 宁园. 健康码运用中的个人信息保护规制[J]. 法学评论, 2020, 38(6): 111-121.
[13] 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.
[14] 江海洋. 论疫情背景下个人信息保护——以比例原则为视角[J]. 中国政法大学学报, 2020(4): 183-194.