

为什么要销毁“健康码”收集的个人信息

□张新宝

2022 年底，国务院联防联控机制发布《关于进一步优化落实新冠肺炎疫情防控措施的通知》降级新冠病毒的防疫级别，不再要求查验健康码和行程码。各地陆续停止了健康码收集处理个人信息的活动，几家电信营运商也相继宣布销毁存储的个人行踪信息。一年多以来，部分省市政府部门根据变化了的防疫形势对健康码所收集的个人信息进行销毁或者对健康码的功能进行调整、下线当地的健康码，也有一些地方尚按兵不动存储大量涉疫的个人信息。值得一提的是江苏省无锡市的做法：公开举行销毁涉疫个人信息仪式，彻底销毁此等个人信息并确保无法还原。我们也注意到，有些地方的健康码仍然显示“绿码”，有些地方甚至将防控新冠肺炎收集处理的个人信息用于新版的健康码。这是需要严肃认真对待的问题。

第一，防控政策调整后继续存储相关个人信息没有合法性基础。

处理个人信息包括收集、存储、使用、加工、传输、提供、公开、删除个人信息，应当遵循《个人信息保护法》规定的合法、正当、必要和诚信原则，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

最小的方式进行处理，收集个人信息应当限于实现处理目的的最小范围而不得过度收集个人信息，应当遵循公开、透明原则且采取必要措施保障所处理的个人信息的安全。地方政府部门基于防疫目的处理个人信息，应当遵循这些法律原则，特别是不得将此等个人信息用于新冠防控之外的其他目的。随着新冠防控政策的变化，有关部门不得再以防疫目的处理相关个人信息，对已经收集存储的相关个人信息进行存储和使用等方式的处理也不再具有合法性基础。

第二，国家机关依法行政的原则要求销毁相关个人信息。

《个人信息保护法》对国家机关处理个人信息作出了特别规定。主要包括：国家机关为履行法定职责处理个人信息，应当依照法律、行政法规规定的权限、程序进行，不得超出履行法定职责所必需的范围和限度；国家机关为履行法定职责处理个人信息应当依照《个人信息保护法》规定履行告知义务，有法律规定的特殊情形除外；国家机关处理的个人信息应当在中华人民共和国境内存储；确需向境外提供的，应当进行安全评估。安全评估可以要求有关部门提供支持协助。地方政府部门收集处理防疫相关的个人信息，是依据《传染病防治法》和国务院的有关规定依法进

行的，为依法强制处理个人信息，无须得到相关个人的同意，但是应当依法履行告知义务，特别是对存储的相关个人信息保障安全并且原则上不得向境外提供。由于新冠防疫情势紧急，一些地方在收集处理新冠个人信息时的程序并不完全合规，主体责任比较模糊，特别是存储方面存在诸多隐患，也有被用作非防疫目的，甚至用作地方保护限制外地公民行使合法权益（如主张债权、提起诉讼）的情况。有鉴于此，对于因防疫收集处理的相关个人信息，予以彻底销毁或删除，更符合行政部门依法行政的要求，特别是有利于避免泄露、非法使用个人信息的风险，更有利于对个人信息的保护。

第三，销毁相关个人信息更符合广大人民群众的利益。

《个人信息保护法》第 28 条规定：“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。”地方政府部门处理的涉及防控新冠的相关个人信息大多是敏感个人信息，在防控新冠的阶段和防控政策

调整后，都应当更加严格保护个人的此类敏感信息。目前，最佳的保护方式或途径就是彻底销毁。敏感个人信息一旦泄露严重威胁自然人的尊严乃至生命、财产安全，是人民群众的重大关切之所在。因此，从人民群众的权利保护角度来看，彻底销毁此等个人信息更符合广大人民群众的利益，更符合执政为民的要求。

最后，不宜将相关个人信息转作他用。

一些地方政府部门试图将防控新冠收集处理的个人信息转作其他用途，以达到“物尽其用”的效果。这样的想法和做法表面上看起来具有一定的合理性，实则具有巨大的潜在风险。首先，此等使用缺乏法律依据，也不符合依法行政的要求；其次，存储的不安全性和匿名化的不彻底性，留下了个人信息泄露、毁损、非法使用甚至非法出境的隐患。有鉴于此，还是应当以销毁相关个人信息为唯一考量，而不能尝试将之转做他用。为了社会管理等目的需要收集处理个人信息的，应当依据相关法律法规及其正当程序另行为之。

（作者系中国人民大学法学院教授、博导，中国法学会法学期刊研究会会长、中国法学会网络信息法学研究会副会长）

“健康码”能否安全合法地转型？

□赵宏

近日，有消息称：“湖南省居民健康卡”新版上线一个月以来运行良好，实现了统一预约挂号、一码就诊、健康档案共享等新功能，成为服务群众健康的总入口。这与此前江苏省无锡市举行涉疫个人数据销毁仪式，确保数据彻底销毁、无法还原的做法形成鲜明对比。“健康码”究竟能否安全合法地实现转型？是彻底销毁还是实现功能转型更佳？也再度成为公众热议的话题。

过去几年，健康码几乎成为人们每天都会使用的新型身份标识，它发挥着风险防控的重要功能，却也在很多时候成为束缚个人行动自由的工具。由于在应急状态下诞生，健康码表现出的对个人信息无差别全员收集、实时收集和事无巨细等特征，都隐藏着个人隐私被泄露和滥用的巨大风险。正因如此，当国家防疫政策发生重大调整后，彻底下线健康码，并将附着其上的个人数据永久性删除，成为公众的普遍呼声。

但在健康码的存废去留问题上，一直也有另一种声音，主张其尚有保存的必要。理由之一是，其中存储的疫苗接种信息或许在危重病人诊疗过程中会为医生提供诊疗依据。但伴随数轮感染过去，此类信息的有效性已彻底消失。而彼时很多地方政府希望保留健康码的理

由还在于应对未来可能的疫情,但这个理由同样无法证立。未来如果再暴发其他大规模传染病，地方政府完全可以通过更精细、更合法合规的方式进行数据收集和突发公共卫生事件的应对。还有地方政府欲将其转型处理，在去标识化和匿名化处理后，将健康码的数据信息继续保留，并转用做诸如健康医疗、交通出行、文化旅游等其他目的。早在湖南省政府转型处理前，2022 年底北京市就曾启动“京通”小程序上线试运行，尝试融合“北京通”与“健康宝”。市民可自愿或自主授权，选择是否将健康宝的个人身份验证信息拓展到“京通”页面。

地方政府将健康码转型挪作他用，当然是在健康码的疫情防控功能失效后的另一设想。但要落于实践却至少需要满足如下法治要求：

其一，删除和销毁与疫情防控相关的敏感个人信息。生成健康码的底层个人数据和衍生用户画像都与个人人格尊严高度相关，也属敏感个人信息，在完成既定功能后，无论是废弃还是转做他用，首要的都是将附着在健康码之上、与疫情防控相关的敏感个人信息彻底删除和集中销毁，这其中尤其包含个人的行动轨迹、健康信息、生物识别信息等。此类信息若继续留存就可能被泄露或滥用，不仅会危及个人人身财产安

全，也极易导致个人名誉受损或遭歧视性对待。《个人信息保护法》规定，删除个人信息不仅是信息处理者的义务，也同样是个人重要的信息权利。这种权利的目的就是为了确保在信息处理目的已经完成或是已无必要时，避免个人信息被不当存储而可能导致的信息被泄露、被非法买卖甚至被用以其他目的的高度危险。

而此前很多专家反对将健康码转做他用的重要原因也在于：健康码在信息收集上表现出“可长期保存且易跨平台复制转移认证”的特点，而现有的脱敏化处理并不能彻底消除个人隐私被暴露和个人信息被滥用的风险。与此同时，尽管公众对此呼声很高，将健康码数据存而不废却一直是各个地方政府的普遍做法。这不仅体现了个人信息对于政府治理和管控的巨大诱惑，也能窥见各地政府对码化治理方式的路径依赖。据此，若将健康码转做他用，首先应确保在技术上能够删除和销毁个人此前存贮于健康码的敏感信息，或者至少通过脱敏处理排除个人隐私被暴露的可能。否则，无锡市政府举行涉疫个人数据销毁仪式，确保数据彻底销毁、无法还原的做法才更为稳妥。

其二，实现功能转型必须征得个人的重新同意。地方政府如果要想实现健康码的转型，即使将所涉及的敏感个人信

息进行脱敏化或去标识化处理，并由此转做他用，也必须重新征得个人同意，否则即属违法。就相关新闻来看，湖南省将健康码信息转做他用是否经过公众的重新同意并未明确。而此前曾尝试对健康码“转型升级”的一些地方政府，很多时候也忽略了这一法治要求，未意识到其中包含的法治风险。

目前，一些地方的市民查验健康码页面会发现，包括个人健康状况、感染风险以及接种疫苗情况等信息依旧存在，甚至实时查询功能也依旧可用，只是因很久不登录而未获更新。仍在运行的健康码中究竟关停了哪些功能，哪些数据信息目前依旧可用，对于普通用户都是一个谜团，也因此引发普遍担忧。在数据化时代，这几乎就像悬在每个人头上的达摩克利斯之剑。没有人愿意活在他人无时不在的窥视之下，也没有人愿意成为数据监控甚至数据操纵的对象。为避免这种危险的发生，政府即使要实现健康码的转型也必须符合严格的法律要求，否则彻底下线销毁才是最令人心安的做法。

（作者系中国政法大学法学院教授、博导）



扫描左侧二维码关注