紧急状态下个人信息保护的理论分析与制度探索
——以健康码的应用为契机

高润青[1], 路瑞香[2]
(1. 中国政法大学 法学院,北京 100089;2. 德国慕尼黑大学 法学院,慕尼黑 999035)

[摘 要]为应对2020年肺炎紧急状态的蔓延,全国各个城市采取了一系列采集与登记公民个人信息的防控措施,以维护城市安全、社会稳定和公民健康。而这些防控措施背后存在着信息滥用的隐忧,如何平衡紧急状态与个人信息保护,社会上存在讨论和争议。有鉴于此,该文拟以健康码的应用为契点,结合我国《民法典》中新增个人信息保护的相关规定,分析提炼紧急状态下个人信息保护的特征和重点问题,提出完善我国紧急状态下个人信息保护制度的初步设想。

[关键词]紧急状态;个人信息保护;健康码;民法典
doi:10.3969/j.issn.1673-9477.2021.03.013
[中图分类号]D923 [文献标识码]A [文章编号]1673-9477(2021)03-077-06

2020年1月23日以来,各地纷纷采取特殊时期封锁和监控措施,用以防止紧急状态扩散,保障公共安全。在这场紧急状态危机管控中,我国涉及个人信息采集和登记的措施层出不穷,记录个人信息的健康码逐步在全国范围内得到推广和应用。出于紧急状态的需要,公民通常会同意这些个人信息收集行为。但是近期不断出现的个人信息滥用、泄露事件让公众对个人信息的安全问题产生了担忧,对政府在个人信息保护方面的信任度也有所下降。

此次紧急状态再次唤起了人们对个人信息保护的关注,有关部门和专家学者呼吁在做好紧急状态工作的同时也要保护好公民的个人信息。2020年出台的《中华人民共和国民法典》(以下简称《民法典》)新增了个人信息保护的内容,对个人信息保护做了较为详尽的规定。但是,在紧急状态中如何保护公民的个人信息、限制个人信息权的正当性何在、界限何在等问题还有待解决。有鉴于此,笔者将充分借鉴此次紧急状态中我国有关个人信息保护的经验教训,以广泛应用的健康码为契点,进一步思考如何完善我国紧急状态下的个人信息保护体系,期待本文可以为个人信息保护与公共利益的平衡问题做出贡献。

一、个人信息与个人信息保护

在大数据时代,个人信息被收集、储存、转让和使用已经成为每个自然人被嵌入其中的社会生活常态,无法改变[1]。

因此,个人信息安全问题逐渐成为我国社会关注的热点。2020年5月28日表决通过的《民法典》在人格权编的第六章独立设置个人信息保护条款,可谓是我国个人信息保护发展道路上的里程碑,充分彰显了我国对个人信息保护问题的高度重视。根据《民法典》第1034条的规定,个人信息被定义为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。

相较于2018年公布的第一版《民法典》草案,2020年正式表决通过的《民法典》中有关个人信息的定义新增了“健康信息”。笔者认为,关于个人信息定义的这一变动,正是立法者出于对紧急状态背景下个人信息保护问题的关注。健康码等涉及公民个人信息的防控措施在便利收集与利用公民个人信息的同时,也会带来一系列个人信息保护的问题。从长远来看,个人信息保护的发展伴随着互联网技术和数字时代的发展。我国颁布的《民法典》与时俱进,对个人信息的定义已经考量到日前信息技术的发展与社会的实际情况。个人信息的范围和种类是随着社会发展而不断增长的。个人信息不仅指单独即可识别自然人的具体数据,还包含可以通过与其他信息结合识别自然人的诸如健康状况之类的抽象信息。另外,根据《民法典》第一千零三十四条的规

[投稿日期]2021-09-04
[作者简介]高润青(1997-),女,河北邢台人,硕士在读,研究方向:宪法、行政法;
通讯作者:路瑞香(1994-),女,河北邢台人,博士在读,研究方向:中德环境犯罪比较研究。

定,“自然人的个人信息受法律保护”。因此,这里所指的个人信息保护的主体为自然人,本文所讨论的也是紧急状态下自然人的个人信息保护问题。

从健康码应用的具体场景和操作流程来看,虽然《民法典》中明确规定的用户个人信息的合法权利使用主体并非是一个自然人,但是真正掌握和管理使用用户个人信息的权利主体不仅仅是自然人,还包括网络社会中的平台企业、政府机关、医院、学校等权利主体。这些应用主体往往出于自身商业价值、公共安全等诸多方面的重要考虑,相对于其他自然人本身而言更容易表现成为公民个人信息泄露与非法滥用的主体,对公民的个人信息安全造成危害。公民对保护个人人身信息安全的严重担忧以及对网络平台和及企业等运营主体的严重不信任感呈现明显的上升态势。新规范的有效推行往往是主观性和客观性的结合。数字经济时代下个人信息安全泄露违法行为的不断增加和其他非法途径侵犯公民个人信息受到保护权益漏洞的广泛利用,加快了社会相关国家法律法规的完善,促成了《网络安全法》与《民法总则》中接连写入有关个人信息受到保护的法律条文。从本质上来讲,个人信息的自由保护体现了自然人对其自身日常生活的自主决定权。《民法典》中写入保护个人信息的规定体现了我国对个人信息利用的价值的关注,反映了以人为本和意思自治的民法精神。

二、紧急状态下个人信息保护的特点

(一)紧急状态下个人信息保护与个体尊严紧密相关

紧急状态期间,为了便于对公民的健康状况进行监测,全国各地陆续推行了健康码。用户在相关小程序、Web 端应用或 App 上填写个人信息,平台会结合用户个人的健康记录、行踪轨迹等数据,最终生成反映用户个人健康状况的带有颜色的二维码。健康码通过颜色来区分不同的风险级别,持有“绿码”的公民可以正常通行,而“黄码”和“红码”则意味着需要继续等待以满足相应的隔离要求。此种根据健康码颜色的不同而对个体进行区别对待的做法确实在紧急状态中减少了重复登记,避免了交叉感染,提高了政府的管理效率。

然而,在此种高效手段的背后隐藏着个体尊严的保障问题。从健康码的实际使用过程来看,健康码的背后不仅仅是个人交通出行记录、通信记录、就诊记录、个人登记信息等各类数据,而且还包括了大数据分析给出的个人的健康状态的判断,也就是健康码的颜色,其直接关系到了用户切身利益。紧急状态下收集和使用的个人信息通常会涉及公民个人的健康状况,而在公共卫生危机面前每个公民最想守护的便是自身的生命安全。当身边有需要等待隔离或被隔离的人员出现时,每个人都避之而不及,甚至会采取一些极端方法。我们试想一下,如果“黄码”和“红码”中的公民个人信息被泄露或者滥用,那么在当前的互联网时代下,很有可能引发网民们对持有“黄码”或“红码”的公民进行搜索或甚至攻击。一旦出现这种情况,等待隔离或者已被隔离的公民将被歧视对待,其个体尊严必然会受到严重侵害。

(二)紧急状态下个人信息权受到限制

《民法典》在人格权编的第六章独立设置有关公民个人信息的条款,不仅体现了我国在数字时代下对个人信息保护的重视,也是对自然人拥有个人信息权的一种肯定。个人信息权的本质是“个人具备权利,以自行决定何时并在何种限度内披露其个人生活事实”[2]。换言之,个人对其拥有的各种信息享有自由支配的权利,但这种信息支配权并不是绝对的。

在紧急状态的重大背景下,健康码主要依附于自然人本身,与公民的个人身份信息绑定,反映我国公民个体的健康相关信息与日常活动情况。这一具有用户个人信息的二维码在我国的紧急状态中不只用于用户个人的日常生活与工作,还会被各地的政务主管部门广泛用于加强行政区划内工作人员的健康管理尤其是对已经确诊或疑似感染肺炎者的健康监测与动态追踪上。在各地政务主管部门通过健康码进行紧急状态监测、防控的工作过程中,国家的行政权在一定程度上进行了扩张,主要表现为可以对我国公民的个人信息权利也进行限制。而在正常情况下,国家的政务主管部门是无权对公民的个人信息及其权益安全进行任何干涉或加以侵犯的。但在紧急状态迅速蔓延乃至波及全国的背景下,在我国公民生命健康与国家安全利益遭遇严重威胁的现实情况下,国家权力的不断扩张势必会以公民个人信息保护权益的减损作为代价。但是,这种对用户个人信息所有权的限制应是有一定范围和限度的。

(三)紧急状态下个人信息权的限制应遵循法定程序

正如笔者在上文提到的,在突发公共卫生事件面前,公民个人确实不得不让渡部分个人信息权,以便紧急状态工作的迅速开展。但是在现代法治社会中,此种在突发公共卫生事件下的临时需求也不能

违反法定程序。有关部门须依照相关法律规定取得授权后在法律规定的情况下对公民的个人信息进行收集与使用,并且不得随意泄露或滥用公民个人信息。只有在程序上对紧急状态中扩大的行政权进行限制,才能实现对公民个人信息权益的保护。

三、紧急状态下个人信息保护的相关法理分析

(一)健康码收集与使用个人信息的正当性

1. 用户的知情同意

2012 年《全国人民代表大会常务委员会关于加强网络信息保护的决定》首次在国家法律文件中正式确定了关于个人信息可以收集的“知情同意原则”,规定网络服务提供者在收集使用公民的个人电子信息时,应当明示其收集、使用个人信息的目的、方式和范围,并经被收集者本人同意,不得违反国家法律、法规的有关规定。《网络安全法》第四十一条将该使用原则进一步规范拓展涉及到用户个人信息的后续使用环节。2020 年的《民法典》第一千零三十五条也明确规定了用户个人信息的合理收集与使用处理应事先征得有关自然人或其法定监护人的明确同意。在目前的此种立法模式下,用户及其个人的合法知情权和同意条件构成了目前我国一般认为收集和处理用户个人信息的合法性和正当性基础。在收集和使用公民个人信息的实践中,健康码的网络服务提供者在收集和处理用户的个人信息前,应将用户个人信息的处理状况告知其本人,向健康码的用户发布个人隐私保护声明,用户在仔细阅读上述声明并做出表示同意的声明意思后即为表示同意,此种意思表示声明是对用户个人信息进行收集及处理和利用的合法授权。

2. 维护公共卫生安全的需要

大数据时代下,知情同意的有效性大幅削弱,且不符合经济考量,忽视了公共利益,难以实现个人利益保护与促进信息利用的平衡[3]。在紧急状态的背景下,知情同意模式的局限性更是日渐凸显。如果国家卫生部门、医院、学校等信息掌控者,对紧急状态工作所需要的个人信息,必须要向每一个健康码的用户进行履行告知义务并且获得其同意,那么基于个人信息的紧急状态措施将无法得到迅速开展,公共卫生安全将无法第一时间得到有效维护。我们必须充分意识到,紧急状态下个人信息的收集与使用是有别于正常状态下个人信息的收集与使用的。紧急状态下对个人信息的保护更加侧重于其对社会整体的价值而非对单独个体的价值。而且根据目前《中华人民共和国传染病防治法》(以下简称《传染病防治法》)等法律的规定,在紧急状态的特殊情况下,为了维护国家安全和公共利益的需要,国家卫生部门和医院可以在未事先征得个人信息主体同意的情况下合理收集和使用我国公民的个人信息。

(二)紧急状态下个人信息权限制的界限

与紧急状态下个人信息保护紧密相连的问题即是个人信息权的限制问题。尽管紧急状态下国家权力可以出于维护国家安全和公共利益的需要对公民的个人信息权进行限制,但是从规范科学的角度来看,此种限制应该是有界限的。此种限制的界限主要表现为紧急状态下公民的某些个人信息权可以受到限制,而某些个人信息权是不应受到限制的;部分受到限制的个人信息权受限制的程度应该是合理的,其受到的限制应当合乎紧急状态下维护公共利益的正当目的,与保护公共利益的紧迫程度成比例。

1. 紧急状态下个人信息权的限制应限定在一定范围内

尽管在与紧急状态抗争的过程中公民不得已需要放弃部分个人信息权,但是这也不能作为践踏人权的依据。与传统意义上的人格权不同,个人信息权既有消极的权能,亦有积极的权能[4]。个人信息权的知情权、决定权、处分权,是个人信息权所具有的最显著的积极权能[5]。个人信息权的消极权能表征信息主体排除侵害的可能性,仅在个人信息的完整性、准确性、私密性遭破坏时才体现出来。它包括更正权、限制权、反对权以及删除权(被遗忘权)[6]。笔者认为,出于紧急状态下维护公共卫生安全的需要,国家权力对公民个人信息权的限制应仅涵盖决定权、处分权等积极权能;而对主要涉及防御个人信息权受侵害的更证权、限制权、删除权等消极权能则无限制的必要。以健康码的应用为例,本次紧急状态中曾经出现过公民个人注册时填写错误其个人信息或临时离开经常居住地,而造成健康码突然从绿色变成红色的情况。在这种情况下,若公民无法行使其个人信息权的消极权能,那么其基本的人身自由将受到严重侵害,甚至会造成其在紧急状态之下的基本人权无从获得保障。因此,紧急状态下国家对公民个人信息权的限制应是有界限的,不能对其中的消极权能进行限制,而具体限制哪些积极权能则需要根据必要性和适当性原则进行确定。

2. 紧急状态下个人信息权的限制应是有限度的

在紧急状态的特殊时期,各级国家机关权力扩张意味着公民个体权利的减损。国家权力一旦扩张过度,就必然会导致对公民个人信息权的严重侵害。

国家公权力对公民权利的减损应借鉴公法上的比例原则对其进行适当限制,以保证其在紧急状态下对公民的个人信息权所采取的各种限制措施手段与紧急状态措施之目的是成比例的。公法上的比例原则具体包括三个子原则,分别是必要性原则、适当性原则和相称性原则。运用这三个子原则将公权力对公民个人信息权的限制限定在一定程度内既是出于降低个人信息泄露风险的需要,也有利于政务部门减轻负担、做到精准防控。在公民向政府让渡权利的情况下,除了公权力可能出现滥用、侵犯私权的问题,我们还应注意到政务部门的管理资源是有限的。从节约政务资源的角度来考量,政务部门对公民个人信息权也不应采取极端的限制手段或随意削减公民的个人信息权,而应努力将限制手段控制在必要的、适当的限度内。

(三)紧急状态下公民私权与公共利益的平衡

行文至此,笔者发现在紧急状态下无论对个人信息的保护还是对公民个人信息权的限制都无法绕开一个关键问题即政务部门如何在突发公共卫生事件下平衡公民私权与社会公共利益。政务部门想要平衡好个人信息保护与公共利益间的关系是非常不容易的,笔者注意到日本的民法学者提出利益衡量论以调整平等主体间的利益冲突。利益衡量论认为,法院进行法的解释,不可能不进行利益衡量,强调民法解释取决于利益衡量的思考方法,即关于某问题如果有A、B两种解释的情形,解释者究竟选择哪一种解释,只能依据利益衡量论决定,并在做出选择时对既存法规及所谓法律构成不应考虑[7]。民法学者提出的利益衡量论是私法上平衡利益冲突的理论,然而在紧急状态下的利益冲突则是私人利益与公共利益的冲突,不仅涉及私法调整,也涉及到公权力的扩张及其控制。在紧急状态的重大背景下为平衡好个人信息保护与公共利益的关系,我们当然可以充分借鉴利益衡量论中有关于利益衡量的思考方法,但是在利益衡量时不可抛弃既存的公法层面的法律、法规。私法领域秉持法无禁止皆可为的原则,而公法领域则奉行法无授权不可为的准则。我们在运用利益衡量的方法权衡私人利益与公共利益时要充分考虑两项基本原则,兼顾私权自治的维护与公权滥用的防止、控制。对于紧急状态下公民私权与公共利益的平衡,可以从以下三个方面展开具体分析。

1. 立法层面

根据我国《民法典》第一千零三十六条的规定,行为人为维护公共利益而处理他人信息的,不承担民事责任。根据我国《传染病防治法》的规定,“在紧急状态的特殊情况下,为了维护国家安全和公共利益的需要,国家卫生部门和医院可以在未征得个人信息主体同意的情况下合理收集公民的个人信息”。以上立法层面的规定都体现了公民私权与公共利益间张力关系的考量,我国未来在完善其他法律法规或制定单独的个人信息保护法时也应做出此种利益衡量,以维护整个社会的公正秩序。

2. 司法层面

利益衡量与司法审查活动相伴而生,是法官在对具体案件进行审查时所不能回避的问题。“‘利益衡量’一词并非对新创建的一种方法的概括,而是对普遍的已经运用着的司法方法的概括。[8]”法官在对紧急状态下涉及公民个人信息保护的案件进行裁量时,应运用利益衡量的方法对相关法律条文做出合理解释,协调公民个人利益与公共利益间的冲突,确定合理的界限,为受到侵害的公民个人权利提供必要的救济。

3. 执法层面

执法机关在执行有关紧急状态的法律法规时,可以采用操作性较强的比例原则在公民私权与公共利益间寻找平衡点,使得公民个人信息的保护与公共卫生安全的维护间形成合适的比例,做到既不因较小的的公民个人信息权益而损害公共利益,也不能因为较小的公共利益而放弃对较大的个人信息权的保护。

四、完善我国紧急状态下个人信息保护的制度进路

(一)对我国紧急状态下个人信息保护制度的反思

从健康码应用的视角来看我国目前对紧急状态下个人信息的保护方面存在的问题如下。

1. 现行法律规范对紧急状态下个人信息的保护力度较弱

随着互联网时代的发展,我国不断通过完善现有的法律规范体系为网络中个人信息的保护提供法律依据,主要包括下表中罗列的八个法律规范。

根据下表的汇总,我们可以发现我国现行法律规范对个人信息的保护主要是从维护互联网安全的角度出发,对网络服务的提供者提出具体要求来保护公民的个人信息权。我国在紧急状态下公民个人信息的保护力度是较弱的,不仅事前缺乏风险预防机制,事中对个人信息侵害行为的制裁也是更多地依靠行政措施,事后对违法行为的惩戒也仅限于《中

序号	名称	法条	年份	颁布机关
1	《民法典》	第一千零三十四条、第一千零三十五条、第一千零三十六条、第一千零三十七条、第一千零三十八条、第一千零三十九条	2020	全国人民代表大会
2	《儿童个人信息网络保护规定》	—	2019	国家互联网信息办公室
3	《民法总则》	第一百一十一条	2017	全国人民代表大会
4	《刑法》	第二百五十三条之一	2017	全国人民代表大会
5	《最高人民法院、最高人民检察院关于亲发公民个人信息刑事案件使用法律若干问题的解释》	—	2017	最高人民法院、最高人民检察院
6	《网络安全法》	第二十二条、第三十七条、第四十一条、第四十二条、第四十三条、第四十四条、第四十五条、第六十四条、第七十六条	2016	全国人大常委会
7	《电信和互联网用户个人信息保护规定》	—	2013	工业和信息化部
8	《消费者权益保护法》	第十四条、第二十九条、第五十条、第五十六条	2013	全国人大常委会

华人民共和国刑法》规定的泄露公民个人信息严重的情形下而未涉及信息滥用行为。另外,与紧急状态密切相关的《传染病防治法》和《突发公共卫生事件应急条例》的重点也没有放在公民个人信息的保护方面,而是更多地规定了紧急状态下公民为相关政务部门提供个人信息的义务。由此可以看出,我国现行法律规范是无法为紧急状态下个人信息面临的风险提供全方位覆盖,更无法对紧急状态下的公民个人信息权进行充分保护。

2. 紧急状态下对个人信息的保护一把抓,缺乏对敏感信息的重点保护

从规范性角度进行考量,公民的个人信息按敏感程度的不同可以被划分为敏感信息和一般信息。敏感信息是指构成个人隐私的信息,一般信息是指通常状态下不构成隐私的信息[7]。根据最高人民法院《关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》第五条的规定,“敏感信息主要包含轨迹信息、通信内容、征信信息、财产信息、住宿信息、通信记录、健康生理信息和交易信息”。我国为控制紧急状态的蔓延利用健康码等手段收集和处理了大量公民个人信息,其中也包含很多敏感信息。然而,令人痛心的是,近期一些省份在紧急状态期间出现了敏感信息泄露的事件,这对公民的个人隐私造成了严重破坏。

3. “合法、正当、必要”原则缺乏具体的判断标准

鉴于“知情同意”原则在平衡个人信息保护与公共利益、数据利用方面的局限性,我国在实践中不能过度依赖“知情同意”原则。而《民法典》中规定的“合法、正当、必要”原则也缺乏具有可操作性的标准。由于具体判断标准的缺乏,紧急状态期间很多个人信息的收集和处理者在收集、保存和共享个人信息的过程中缺乏保密措施,造成了公民个人信息的滥用和泄露。

4. 我国对紧急状态过后个人信息的保护问题未做出规定,存在严重缺失

紧急状态期间,网络服务提供者和被授权的相关部门通过健康码等小程序或 App 收集与处理了大量公民的个人信息。随着紧急状态的退散,这些被收集的个人信息是否还能被网络服务提供者和相关部门使用,如果能被继续使用,那么使用的范围该如何限定;如果不能被使用,那么这些公民的个人信息该由谁进行处理,该选择怎样的具体处理方式。这些问题都亟待回应和解决,但是我国目前对紧急状态过后如何保护紧急状态中收集的公民个人信息是没有相关法律规范和政策规定的。

(二)完善我国紧急状态下个人信息保护制度的初步设想

1. 完善相关法律规范,形成私法与公法协力的保护机制

紧急状态下对公民个人信息的保护不仅是私法领域的问题,也是公法领域中值得关注的对象。健全紧急状态下对个人信息事前、事中和事后的保护机制是私法与公法共同承担的任务。推动私法与公法在个人信息保护方面的协调与衔接是大数据时代发展的需要,也是平衡公民私权与公共利益的需要。私法与公法应对紧急状态中滥用公民个人信息、泄露公民

个人信息等侵害公民个人信息权的行为分别做出民事、行政、刑事方面的制裁规定,以对个人信息的侵害者形成震慑力,为公民个人信息提供全方位的保护。

2. 对个人信息实行分类保护,强化对敏感信息的保护

我国应借鉴欧盟《通用数据保护条例》的规定,根据公民个人信息的应用场景对其进行分类分级保护,将个人信息划分为一般信息与敏感信息,施以不同的保护力度。在紧急状态的背景下,姓名、出生日期、身份证件号码、生物识别信息、住址、电话、电子邮箱、定位数据、在线活动等行踪信息,也应认定为构成隐私的敏感信息,从个人信息权的高度加以法律保护。基因数据、生物数据和健康数据等本身作为敏感信息,更应得到重点关注和特别保护。

3. 明确"合法、正当、必要"原则的具体标准,细化个人信息收集与处理规范

紧急状态下对公民个人信息的收集与处理涉及多个主体,只有明确"合法、正当、必要"原则的具体标准,细化个人信息收集与处理规范,才能防范公民个人信息的滥用与泄露。首先,促进信息共享的同时应对各方主体收集与使用信息的范畴做出具体规定;其次,可以根据比例原则对公民个人信息处理的限度问题做出明确规定;最后,应对多方主体收集与处理个人信息的渠道进行统筹规划,明确各方主体收集与使用信息的渠道。

4. 制定紧急状态过后保护个人信息的法律法规,对紧急状态过后个人信息的处理问题进行实体规范与程序规范

随着紧急状态蔓延的态势得到控制,我国应及时制定紧急状态过后保护个人信息的法律法规。笔者认为,在相关法律法规中应规定政务部门在紧急状态下依法收集的公民个人信息,紧急状态过后要严格保存或销毁,防止公民隐私泄露和滥用;网络服务提供者不得以违法或不正当手段收集、加工、保存和利用个人信息;因业务工作而收集、保存的个人信息,要严防泄露或非法交易。另外,网络服务提供者在紧急状态过后收集和保存的个人信息以及处理个人信息的方式应及时报监管部门备案;政务部门与网络服务提供者对紧急状态过后用户个人信息的处理情况,也应告知个人信息主体,在程序上保障公民的知情权。

参考文献

[1]程啸. 民法典编纂视野下的个人信息保护[J]. 中国法学,2019(4):26-43.
[2]赵宏. 紧急状态下个人的权利限缩与边界[J]. 比较法研究 2020(2):11-24.
[3]王文祥. 知情同意作为个人信息处理正当性基础的局限与出路[J]. 东南大学学报,2018(20):142-146.
[4]李延舜. 个人信息权保护的法经济学分析及其限制[J]. 法学论坛,2015(3):43-53.
[5]张里安,韩旭至. 大数据时代下个人信息权的私法属性[J]. 法学论坛,2016(3):119-129.
[6]叶名怡. 论个人信息权的基本范畴[J]. 清华法学,2018(5):143-158.
[7]梁慧星. 民法解释学[M]. 北京:中国政法大学出版社,1995.
[8]胡玉鸿. 关于"利益衡量"的几个法理问题[J]. 现代法学,2001(4):32-38.
[9]姚辉. 人格权法论[M]. 北京:中国人民大学出版社,2011.
[10]王泽鉴. 人格权法:法释义学、比较法、案例研究[M]. 北京:北京大学出版社,2013.

[责任编辑 王云江]

Theoretical Analysis and Institutional Exploration of Personal Information Protection in Emergency ——From the Perspective of the Application of Health QR Code

GAO Runqing[1], LU Ruixiang[2]
(1. School of Law, China University of Political Science and Law, Beijing 100089, China;
2. School of Law, University of Munich, Munich 999035, Germany)

Abstract: In response to the epidemic in 2020, cities across the country have taken a series of prevention and control measures to collect and register citizens' personal information, so as to maintain urban security, social stability and citizens' health. However, there are hidden worries of information abusing behind these prevention and control measures. How to balance the state of emergency with the protection of personal information has been discussed and disputed in the society. From the perspective of the application of health QR code, this paper combines with the relevant provisions of personal information protection newly added in The Civil Code, to analyze and refine the characteristics and key issues of personal information protection under the state of emergency, and put forward the preliminary idea of improving the personal information protection system under the state of emergency in China.

Key Words: emergency state; personal information protection; health QR code; the Civil Code