财经法学 No. 4，2020
pp. 108 - 120

“数据抗疫”中个人信息利用的法律因应

李晓楠*

内容提要：大数据在疫情态势研判、传播路径分析、精准防控及后续治理中都扮演着重要角色，有利于及时追溯疫情根源，有效切断疫情传播。但不当的数据处理行为可能导致个人信息的泄露，侵犯个人隐私，损害个人权益。为此，在重大疫情防控中，必须遵循法治路径，处理好公共利益维护与个人隐私保障之间的平衡关系。原则上，疫情防控可以作为豁免数据控制主体部分义务、克减信息主体部分权利的合法事由。但数据控制主体仍应承担起必要的个人信息安全保障责任，遵循“目的限制”和“必要性”等数据处理的基本原则。此外，基于公共利益和比例原则在概念上的抽象特质，应进一步完善公共利益下个人信息处理的具体法律安排，从数据利用规制和私权救济两个面向，共同促进个人信息在重大疫情防控中的规范化利用。

关键词：重大疫情防控　个人信息　规范利用

一、引　言

2019 年 12 底开始，新型冠状病毒逐步呈现出全国传播的严重态势。在证实病毒“人传人”的性质后，实现患者及疑似患者的有效隔离就成为了阻断传播的重要管理举措。在追踪确诊患者和疑似患者的过程中，从政府部门到基层自治组织再到企事业单位，均收集了大量的个人信息。一方面应当看到，个人信息的有效运用有助于实现疫情防控目的，各地充分运用“大数据+”等手段，为“抗疫”配上“最强大脑”。通过建立疫情防控专题数据库，加强疫情防控数据汇聚和共享应用，及时发挥大数据在服务决策、精准防控方面的作用。〔1〕另一方面也应看到，个人信息收集行为不规范甚至随意收集个人信息的行为导致了侵害个人隐私权等情形的发生，如云南文山

* 李晓楠，对外经济贸易大学法学院博士研究生。

〔1〕 参见《湖北宜昌：大数据为抗疫配上“最强大脑”》，载 https://baijiahao.baidu.com/s?id=1660404050154520788&wfr=spider&for=pc，最后访问时间：2020 年 3 月 10 日。

州5名医务人员利用工作便利，偷拍、散布患者信息，引发了隐私保护的担忧，反映了疫情防控下个人信息保护的短板。〔2〕

这一方面是因为我国个人信息保护规范还不健全，缺乏明确的数据利用行为指引；另一方面也在于公共利益优先、私利服务公益的思维惯性容易导致对个人数据权利的忽视。从我国的法律规定来看，《传染病防治法》第12条、第20条、第38条以及《突发公共卫生事件应急条例》第40条，均赋予了疾病预防控制机构、医疗机构及县级以上政府和乡镇基层自治组织收集个人信息的权利，但是上述法律法规缺少个人信息收集、管理、利用、存储、共享等数据生命周期全流程的具体操作规范。我国《网络安全法》虽然对个人信息保护作出了较为全面和广泛的要求，在个人信息更正与删除权、数据泄露通知、个人信息转让等方面有更为具体的规定，但《网络安全法》主要旨在保护国家的“网络主权”和落实网络安全要求，且规制的主体为网络运营者，〔3〕难以辐射疫情管控下多个主体的个人信息收集和利用行为。

但是，应当看到，在疫情防控的背景下，个人信息保护容易让位于公共安全维护，引发公共利益与个人权利的紧张冲突。为了处理好公共安全与个人隐私保护之间的平衡关系，在我国法律规范缺位的情况下，有必要进一步完善疫情防控下个人信息利用全流程的行为规范；明确个人数据的认定标准、范围和数据权能；构建专门的个人信息安全监督机构，从数据控制主体行为规制和数据主体权利救济两个方面，并行推进个人信息在疫情管控中的规范利用。

二、个人信息保护及重大疫情应对中收集利用个人信息的正当性证成

（一）个人信息及个人信息权利保护

数据是信息的形式，信息是数据的内容，没有个人信息的数据不是个人数据，个人信息的权利也即个人数据的权利。〔4〕依据我国《民法典》第1034条第2款规定，所谓个人信息，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。围绕个人数据权利的性质和内容，有学者认为，个人数据权利不同于人格权或财产权，而是一种“自决利益”，具体来说，表现为：数据控制主体未经数据主体同意不得收集、转让；数据主体有权知悉其个人数据使用的目的、方式、范围；数据主体有权查询个人数据并主张更正、删除等权利。〔5〕有学者认为，根据数据本身“指向性”的程度，可以将个人数据分为原始数据、信息和隐私，并对应数据权、信息权与隐私权，但总体上属于防御性权利，应以防止损害为中心，而不能主动援引。〔6〕还有学者认为，个人数据保护的人格权与财产权路径均存在难

〔2〕 参见《云南5名医务人员偷拍散布患者信息被罚》，载https://www.sohu.com/a/371387254_162645，最后访问时间：2020年3月10日。

〔3〕 See Asia Business Law Institute, Regulation of Cross-Border Transfers of Personal Data in Asia, available at https://www.abli.asia/UploadPDF/DP_Compendium_May_2018.pdf, last visited on Mar. 10, 2020.

〔4〕 参见程啸：《论大数据时代的个人数据权利》，载《中国社会科学》2018年第3期。

〔5〕 参见姚岳绒：《论信息自决权作为一项基本权利在我国的证成》，载《政治与法律》2012年第4期。

〔6〕 参见李勇坚：《个人数据权利体系的理论建构》，载《中国社会科学院研究生院学报》2019年第5期。

以克服的弊端，对于个人数据保护来说，应当借鉴欧盟《一般数据保护条例》（以下简称 GDPR）的规定，构建起消费者预期与风险规制相结合的路径。〔7〕

个人信息本身可能蕴含着数据主体的人格利益和财产利益，前者如个人隐私，后者如以个人数据为标的的商业交易。但是基于数据共享和流动对经济社会的重要意义，个人数据财产利益不应具有物权排他性的绝对效力。〔8〕而隐私权本身主要是一种被动性的人格权，通常在遭受侵害时，权利人才可援引，难以满足数据主体对个人数据积极管理的需要。〔9〕尽管针对个人数据权利有不同的表达，但为回应数据主体利益同时兼顾数字经济社会发展需要，我国也逐步形成了以“数据自主”为重要内容的个人信息保护和数据主体权利体系规则，包括“知情—同意”“数据可携带”“被遗忘权”等。〔10〕

从欧盟的 GDPR、美国《加州消费者隐私法案》（California Consumer Privacy Act，CCPA）和澳大利亚《竞争与消费者（消费者数据权）规则 2020》（Consumer Data Right，CDR）等个人信息保护实践看，个人数据权利不排除数据的共享利用，但数据控制主体、处理主体等需要履行数据主体保护义务，既包括提供安全可靠的技术防护手段以防止个人信息泄露，又包括数据利用全流程的安全管理义务，并需要满足数据主体的信息自主权。总之，尽管学界对个人数据权利的保护形式和具体行使方式还存在争议，但个人信息主体享有个人数据自主利益，数据控制主体具有配合数据主体自主利益实现的义务已经成为共识，并成为个人数据保护规范的重要内容。

（二）个人信息作为重大疫情防控中政府决策的基础

信息技术的高速发展，使政府利用海量数据进行公共决策成为可能。习近平总书记在北京市调研指导新型冠状病毒肺炎疫情防控工作时强调，要运用大数据等手段，加强疫情溯源和监测。〔11〕大量个人信息被收集，既包括公权力部门为履行法定职能或执行应急方案依职权收集个人信息，又包括非公主体依据法律法规或行政命令亦或出于自我防护需要而收集个人信息，并汇聚至政府大数据分析平台，辅助政府部门应急决策。例如，疫情暴发之初，浙江省当即启动重大突发公共卫生事件一级响应，并运用“大数据＋网格化”手段，精准滚动摸排所有相关人员，寻找“隐性传染源”。依托新型城市治理平台“城市大脑”搭建的“卫健警务—新型冠状病毒防控系统”，共享、比对卫健委、公安机关等各部门数据，有关部门可以了解每天从疫情重点区域到杭人员信息，实现了对过境车辆和人员“从哪里来、到哪里去、来干什么”的轨迹动态跟踪，便于早期介入、动态管理，并实现各区县市共享，提升防疫实效，避免防疫盲区。〔12〕总之，在疫情防控中，个人信息的大数据利用发挥了重要作用，成为疫情管控中不可或缺的一环。

---

〔7〕 参见丁晓东：《什么是数据权利？——从欧洲〈一般数据保护条例〉看数据隐私的保护》，载《华东政法大学学报》2018 年第 4 期。

〔8〕 参见梅夏英：《在分享和控制之间：数据保护的私法局限和公共秩序构建》，载《中外法学》2019 年第 4 期。

〔9〕 参见王利明：《论个人信息权的法律保护——以个人信息权和隐私权的界分为中心》，载《现代法学》2013 年第 4 期。

〔10〕 参见《网络安全法》第 40－44 条；《信息安全技术 个人信息安全规范》（GB/T 35273—2020）第 8 条。

〔11〕 参见济兼：《防控疫情要用好大数据》，载 http://opinion.people.com.cn/n1/2020/0217/c1003－31589986.html，最后访问时间：2020 年 3 月 10 日。

〔12〕 参见《浙江：让大数据成为“战疫”利剑》，载 https://baijiahao.baidu.com/s?id＝1658231498659116892&wfr＝spider&for＝pc，最后访问时间：2020 年 3 月 10 日。

（三）重大疫情防控作为克减个人信息权利的正当事由

基于数据权利自主性的特征，个人有权拒绝他人收集信息的行为。换句话来说，收集利用个人信息应当经过数据主体的同意，这也被称为数据管理中的“知情—同意”原则。〔13〕然而，拒绝权本身不是绝对的，在特定情况下，无须获得数据主体同意即可收集、使用其个人信息。之所以存在“同意”原则例外，是因为存在其他权利和合法事由在价值保护顺位上高于信息自决权。从个人信息保护实践看，国内外普遍将维护公共利益需要置于信息自决权之上，而不受“知情—同意”原则的约束。

如前所述，我国《传染病防治法》《突发事件应对法》《突发公共卫生事件应急条例》已经赋予了相关主体基于疫情防控收集个人数据的权能。我国《信息安全技术 个人信息安全规范》（GB/T 35273—2020）就规定了“同意”原则的几种例外事由，主要包括数据收集和使用与国家安全、国防安全直接相关的，与公共安全、公共卫生、重大公共利益直接相关的，出于维护个人信息主体或其他个人的生命、财产等重大合法权益的等。此外，根据我国《民法典》第1036条第3项之规定，为维护公共利益可以不经信息主体或其监护人同意直接处理自然人个人信息。从现有法律规定上看，公序良俗已经成为民法基本原则之一，公共利益维护本身就是限制私权的合法理由。〔14〕为此，即便个人享有信息权利，也不得违反法律，不得违背公序良俗原则。反过来说，为维护公共利益而合理收集、使用或者公开自然人个人信息时，无须承担侵害个人信息的民事责任。

欧盟GDPR序言第（46）条明确规定，传染病监测构成公共利益，处理个人数据时可不征得数据主体的同意，并在序言第（65）（73）条明确针对涉及公共卫生的公共利益，允许欧盟或成员国通过立法对数据主体权利、数据保护基本原则加以限制。第6条亦将为履行涉及公共利益的职责所必要的数据处理排除在“知情—同意”原则的约束外。此外，GDPR通过多个具体条文对公共利益下个人数据权利同时也是数据控制主体的义务进行了相应的克减。如GDPR第14条有条件豁免了出于公共利益目的而间接获得个人数据的主体的告知义务；第17条、第18条规定，当数据控制者为公共利益而履行义务或者为行使其职务权限进行数据处理时，数据主体不得行使删除权（被遗忘权）或限制处理权；第89条规定，当个人数据因公共利益存档的目的被处理时，欧盟法律或成员国法律可以针对个人数据权利和相关的安全保护措施设定克减条款等。

在新冠肺炎疫情期间，美国卫生部门通过发布公报的方式明确规定，出于公共卫生目的和“防止严重和迫在眉睫的威胁”，可以公开个人健康信息而豁免《健康保险可携带与责任法案隐私权规则》（HIPAA）患者健康信息的隐私期待。〔15〕在实践当中，美国卫生部门通过发出“迫在眉睫危险令”（an imminent danger order），可以直接调取个人信息。以密歇根州为例，如果密歇根州卫生服务部门（MDHHS）认定存在“迫在眉睫的危险”，则有权立刻发出“迫在眉睫危险令”，命令相关人员作出降低或消除危险所必要的动作，这其中自然包括要求个人汇报与疾病相

〔13〕 参见张新宝：《个人信息收集：告知同意原则适用的限制》，载《比较法研究》2019第6期。

〔14〕 参见程啸：《民法典编纂视野下的个人信息保护》，载《中国法学》2019年第4期。

〔15〕 See U. S. Department of Health and Human Services，Office for Civil Rights（2020），COVID-19 and HIPAA：Disclosures to Law Enforcement，Paramedics，Other First Responders and Public Health Authorities，available at https://www.hhs.gov/sites/default/files/covid-19-hipaa-and-first-responders-508.pdf，last visited on Mar. 10，2020.

关的情况。〔16〕

三、重大疫情下个人信息利用的法律限制

在利益衡量的基础上，个人信息自决权需部分让位于公共利益，但重大疫情下利用个人信息的行为也并非没有法律限制。基于个人信息收集的主体和具体场景，可将个人信息利用的法律限制分为对公权力主体和对非公主体的不同面向，同时亦应受到个人信息保护规范的一体限制。

（一）公权力主体收集利用个人数据的法律限制

《传染病防治法》《突发事件应对法》《突发公共卫生事件应急条例》均明确了公权力机关，包括县级以上人民政府及其有关部门，各级疾病预防控制机构，街道、乡镇以及居民委员会、村民委员会等疫情信息的收集职能，以供疫情的防控分析，传染病监测、预测和通报。个人应当配合公权力机关有关传染病的调查，如实提供有关信息，否则可能承担不利后果。如在本次疫情中，有地方明令所有通过公路、机场、铁路等方式进入本市的外来人员，在进入本市时应如实填写健康登记表。对于拒绝履行的人员，执法部门将依法协助卫生健康行政部门、医疗机构和疾病预防控制机构采取相应的强制措施。〔17〕从行为类型上看，公权力机关收集个人信息的行为，实质上为相对人创设了如实上报个人信息的义务，应当属于具体行政行为，受到行政法基本原则的限制。

尽管基于应急管理的需要，可以赋予公权力机关直接收集、处理个人信息的权力，个人信息自主权应当受到一定程度的限缩、克减，但对个人信息的处理仍需遵循法律的基本原则，并妥当平衡公权力和私权利之间的关系。〔18〕一方面，要通过法律明确授权，赋予公权力机关紧急行政权等应对紧急事件的必要职权；另一方面，要防止公权力滥用，避免对公民数据权利的过分限缩，克服极端倾向，防范应急状态下出现社会冲突，维护社会正常管理秩序。〔19〕

从行政法基本原则的具体内容看，合理行政原则中的比例原则可以作为规范行政机关收集、利用个人信息行为和维护个人信息权利的有益工具。在确认疫情应对中收集个人信息具有正当性的前提下，比例原则要求个人信息收集应当具有合目的性、适当性，并做到损失最小。具体而言，行政合目的性要求收集个人信息的目的必须是为了防控疫情需要；适当性原则要求收集个人信息时选择的具体措施和手段应为防控疫情所必须；损失最小原则要求收集个人信息应当采用对当事人权益损害最小的方式。总之，公权力机关在收集、利用个人信息的过程中，应当接受行政合理性原则的指导，妥当处理公权力行使与个人信息权利之间的协调关系。

（二）非公权力主体收集、利用个人信息的法律限制

从当前疫情防控的实践看，也存在非公权力主体收集个人信息的行为。如疫情期间，私营企业、小区物业、商场超市等要求进出人员登记个人信息；APP 如“航班管家”基于自有以及收

〔16〕 See Public Health Law Bench Book for Michigan Courts, available at https://www.michigan.gov/documents/ag/PHLBB_2016_Edition_532659_7.pdf, last visited on Mar. 10, 2020.

〔17〕 参见《郑州市新型冠状病毒感染的肺炎疫情防控领导小组办公室通告》（第 5 号），载 http://www.zhengzhou.gov.cn/html/www/news6/20200202/2343414.html，最后访问时间：2020 年 3 月 10 日。

〔18〕 参见江必新：《用法治思维和法治方式推进疫情防控工作》，载《求是》2020 年第 5 期。

〔19〕 参见王万华：《略论我国社会预警和应急管理法律体系的现状及其完善》，载《行政法学研究》2009 年第 2 期。

集的航班、铁路行程、确诊患者信息等数据，匹配新型肺炎确诊患者的行程信息。〔20〕非公权力主体收集、利用个人信息存在多元化的动机。比如，为了遵守公权力机关的行政要求。例如，各地方一般要求企业复工复产应提交《企业疫情防控工作承诺书》，承担疫情防控主体责任，并配合有关部门的流行病调查等工作。〔21〕比如，基于新冠肺炎的强传染性，有关主体为了实现自我防护目的，通过获取出入人员的个人信息，可以及时采取禁止入内等措施避免交叉感染。再如，为了扩大企业的影响力，如航班管家 APP 上线的“新型肺炎确诊患者同乘旅客查询工具”，在为用户提供便利的同时，也起到了吸引流量的效果。当然，非公权力主体收集、利用个人信息的各动机之间并不互相排斥，甚至可以互相包容，也就是说，既可能是为了遵从行政机关要求，同时又可能是为了自我防护并提供他人查询。

在依据行政机关的要求处理个人信息时，非公权力主体应当严格遵循行政机关确立的个人信息收集范围和利用方式，否则将失去个人信息收集、利用的合法性。在防控疫情实践中，非公权力主体用于收集个人信息的登记簿的条目一般由行政机关统一确定，主要包括个人身份信息、是否发热、是否去过特定地区等行程信息；并按照行政机关要求上报来访人员等的涉疫信息。为此，出于履行行政机关要求而收集利用个人信息时，非公权力主体不得超越行政机关确定的数据处理范围和方式。

在基于维护重大合法权益如自我防护等收集利用个人信息时，应受到民法基本原则的约束。民法基本原则要求权利不得滥用，此外，还有学者将公法领域的比例原则引入私法领域，介入难以充分协商或体现意思自治的民事行为。〔22〕非公权力主体以维护重大利益为由收集、利用个人信息，可以不经数据主体同意，形成了事实上的单方强制，有以比例原则进行必要矫正的余地。例如，在疫情下，有些企业在入口处安装体温采集装置，自动收集进出人员包括员工的体温信息，如体温异常则自动报警。体温对新冠肺炎具有重要指标作用，非公权力主体出于自我保护的目的可以越过数据主体同意直接收集，具有合理性。但是，对于对疫情自我防控并不必要的信息，如血型、民族等信息，则不得随意采集，否则有滥用权利之嫌，也不符合比例原则的要求。总之，无论是禁止权利滥用原则抑或是将比例原则引入私法领域，从法理根源出发，均是为了防止私权利主体间权利的过分失衡，使优势主体的权利得到限制，被动接受主体的权利和自由不被过度干预。〔23〕

（三）个人信息权利对数据控制主体行为的限制

因为原则的概括性和模糊性，通过个人数据保护专门立法细化和完善个人数据权利，同时实现对数据控制主体行为的有效指引和规范成为了必要选择。例如，我国已经将《个人信息保护法》和《数据安全法》列入了 2020 年立法规划；欧盟早在 2018 年 5 月就出台了 GDPR；澳大利亚发布了《竞争与消费者（消费者数据权）规则 2020》；美国加州制定了《加州消费者隐私法案》

〔20〕 参见《航班管家“新型肺炎确诊患者同乘旅客查询工具”上线》，载 http://www.caacnews.com.cn/1/4/202002/t20200212_1292673.html，最后访问时间：2020 年 3 月 10 日。

〔21〕 参见《郑州市新型冠状病毒感染的肺炎疫情防控领导小组办公室通告》（第 20 号），载 http://www.zhengzhou.gov.cn/html/www/news6/20200219/2367004.html，最后访问时间：2020 年 3 月 10 日。

〔22〕 参见郑晓剑：《比例原则在民法上的适用及展开》，载《中国法学》2016 年第 2 期。

〔23〕 参见李敏：《我国民法上的禁止权利滥用规范——兼评〈民法总则〉第 132 条》，载《法律科学（西北政法大学学报）》2018 年第 5 期；李海平：《比例原则在民法中适用的条件和路径——以民事审判实践为中心》，载《法制与社会发展》2018 年第 5 期。

等等。而其中 GDPR 以其对个人数据保护的周延性和严格性受到全球范围的关注，并成为个人数据保护的标杆。〔24〕

已有的数据管理实践基本都通过对数据控制主体义务的明确规定，达成对公共利益下的个人信息利用行为的规制。从具体义务内容看，主要包括安全技术义务与安全管理义务两大类。〔25〕我国《民法典》第 1035 条就明确规定，处理个人信息应当遵循合法、正当、必要原则，包括公开处理信息的规则；明示处理信息的目的、方式和范围。第 1038 条又进一步明确信息处理者不得泄露、篡改个人信息，并应当采取技术措施和其他必要措施保障个人信息安全。又如，GDPR 第 5 条规定了与个人数据处理相关的原则，实际上也是数据控制主体的义务要求，包括合法性、公平性、透明性原则，目的限制原则，数据最小化原则，准确性原则，存储限制原则，完整性和保密性原则等。澳大利亚 CDR 在第一部分前言中也强调了消费者个人数据处理上的最小化等原则。

即使在紧急卫生情况下出于公共利益目的处理数据，数据控制主体也要提供适当且具体的措施以保障数据主体的基本权利与利益，履行特定数据保护义务，而不能随意处理个人数据。我国有学者认为，即便公共利益可作为限制个人信息权利的合法事由，也并不意味着在任何情况下，为了公共利益等诉求，就必须共享个人信息。基于公共利益收集、使用和共享个人信息，也应当遵循必要性、最小化适用等个人信息利用的基本原则。〔26〕

此外，从域外经验看，鉴于公共利益概念的模糊性和扩张性，GDPR 第 6 条明确要求，当与公共利益目的相关时，各成员国应当对处理行为设立更为精细的具体要求和其他措施，或者成员国法律可以要求数据控制者向监管机构咨询并且征得其事先授权，以确保数据处理的合法与公平。又如，GDPR 第 13 条、第 23 条规定的透明性要求（针对直接从个人处获得数据的主体），包括明确被处理的数据类型，个人数据可能被披露的对象，处理数据的目的，可能的数据权利限制；GDPR 第 89 条规定了目的限制规则，即对个人数据权利的克减是实现特定公共利益目的所必须；GDPR 第 9 条、第 23－25 条、第 32 条等规定，为了保护数据主体的权利和自由，基于公共利益目的而进行的个人数据处理行为应当采取适当的技术和组织保护措施，如可能的匿名机制、数据最小化机制（个人数据的数量、处理规模、存储期限、可访问性）和保密措施等。西班牙数据保护局（AEPD）发布有关新冠肺炎的个人数据处理报告又进一步指出，在应对疫情过程中处理个人数据应当符合合法性、安全性、透明度、目的限制、准确性和数据最小化等原则。〔27〕

四、重大疫情下收集利用个人数据行为的规范化路径

如前所述，不管是基于应急管理的需要，还是个人数据管理的实践，均承认疫情防控目的下处理个人信息的必要性。但基于“比例原则”及“权利不得滥用”的基本法理和国内外个人信息

〔24〕 See EU，General Data Protection Regulation，available at https://gdpr-info.eu/，last visted on Jan. 10，2020.

〔25〕 参见丁晓东：《个人信息私法保护的困境与出路》，载《法学研究》2018 年第 6 期。

〔26〕 参见王利明：《数据共享与个人信息保护》，载《现代法学》2019 年第 1 期。

〔27〕 See AEPD，Report on Processing Activities Relating to the Obligation for Controllers from Private Companies and Public Administrations to Report on Workers Suffering from COVID-19，available at https://www.aepd.es/es/documento/2020－0017－en. pdf，last visited on Mar. 10，2020.

保护的法律实践，重大疫情下处理个人信息应遵循法治路径。具体来讲，结合疫情防控的实践，首先，在疫情中应坚持以比例原则作为判断个人信息处理是否妥当的指导。例如，各地疫情防控指挥部门应在制定涉及个人信息处理的防控措施时考虑比例原则的要求；各类防控主体在进行数据处理时应满足比例原则的要求等。其次，在设定疫情下个人信息处理的具体法律规范时，应细化疫情中信息主体权利的内容，从私权救济出发强化疫情中的个人信息保护；应明确数据控制主体在疫情防控中的个人信息安全保障义务，规制数据控制主体的数据处理行为；应健全疫情中个人信息不当处理的问责机制，倒逼疫情下防控措施和数据处理行为的审慎实施。

（一）坚持疫情下个人信息处理的比例原则

重大疫情防控需要处理好公共利益和个人信息权利之间的平衡关系，比例原则可以成为平衡利益的有益工具。欧盟《个人数据保护比例原则指南》指出，应在适当的数据处理与合法目的间进行平衡，无论是公共或私人领域，都应在所有阶段实现公共利益、个人权利和自由之间的利害关系的平衡，保证对个人数据权利干预的强度与在特定情况下需要达到的目标之间的必要平衡关系。〔28〕比例原则以“手段—目的”的二元均衡结构作为思考和分析工具，〔29〕可使社会公共利益之判断更为具体，进而更好地约束疫情防控中涉及个人信息的防控措施和各类收集利用主体的个人信息处理行为。

在比例原则的指导下，可分步判断处理个人信息的措施是否正当。首先要判断数据处理的适当性，在防控措施的设定和个人信息的处理上，用于防控和处理的个人信息类型应当可以实现防疫目的。目前个人上报信息种类主要包括姓名、身份证号、居住地、行程信息、通行人员、目的地、所乘交通工具及身体健康情况等，各地疫情防控指挥部在制定涉及个人信息处理的防控措施时以及数据控制主体在处理个人信息时，必须具有合理依据证明上述个人信息能够实现防疫目的，对于不为防疫所需要的个人信息，不能纳入防疫措施的范围和数据处理的范围。其次，判断数据处理手段是否可以实现防疫目的。根据 GDPR 的规定，数据处理的手段除了收集外，还包括记录、存储、改编或修改，查询、使用、传播、披露、删除或销毁等操作。各地疫情防控指挥部决定采取的防控措施以及数据控制主体决定采取的处理措施应能实现防疫目的，如果无需共享、披露等即可满足防疫需求，则个人信息不能被共享或披露，否则不符合比例原则要求。再次，要判断疫情防控措施及数据处理的必要性，也即在疫情防控措施的设定及处理的个人信息类型和处理方式的选择上，应采取最为和缓的干预手段，以影响最少的个人信息量和使用最简短的数据处理流程，尽可能使公民权益遭受最小损害。最后，还要进一步在疫情防控措施及个人信息处理方式与所欲实现的公共利益目的之间进行权衡，确定疫情防控措施或数据处理行为对于相对人所造成的负担是否超过维护公共利益带来的效益。

（二）完善重大疫情下收集个人信息的法律规范

1. 进一步细化个人信息类型，提供梯度保护

以可识别性程度及对个人权益的重要程度，可将个人信息进一步划分为一般个人信息和敏感

〔28〕 See European Data Protection Supervisor, Assessing the Proportionality of Measures that Limit the Fundamental Rights to Privacy and to the Protection of Personal Data, available at https://edps.europa.eu/sites/edp/files/publication/19-12-19_edps_proportionality_guidelines2_en.pdf, last visited on Mar. 10, 2020.

〔29〕 参见前引〔22〕，郑晓剑文。

个人信息。通常来讲，对个人敏感信息的保护力度要强于一般信息，对个人敏感信息要提供更强的权利救济，对数据控制主体采取更严格的规制措施。就疫情防控中收集的个人数据而言，健康数据、家庭住址等可以被认定为敏感信息。因为个人健康数据尤其是病毒感染信息及家庭住址等如果发生泄露，将可能严重损害个人尊严和正常的生活安宁，引发歧视和社会的不公正对待，且难以通过有效的救济手段恢复至未受侵害的状态。实际上，在本次疫情暴发过程中，针对未及时自我隔离和如实报告个人信息又被确诊的新冠肺炎患者，出现了被“人肉”、谩骂攻击这样的违法行为；武汉籍的个人即便未被确诊，也会引起其他人的恐慌，出现了“谈鄂色变”的自保式歧视，侵害了数据主体的权益。另外，部分携疫人群或密切接触者由于惧怕群体歧视而选择隐匿瞒报个人信息，带来公共关系中的一系列“次生问题”，不利于抗疫工作的开展。相较而言，个人行程信息包括乘坐交通工具信息、出发地和目的地信息、同行人员等，即便泄露，对个人的人身权益影响也较小，可以被认定为一般数据。然而，在大数据技术下，可能很难对某些数据进行准确的定性分类，如在此次疫情防控中已经开始利用的个人位置信息而言，短时间的个人位置信息不至于严重侵害个人隐私，可以认定为一般个人数据，而较长时间的个人位置信息就可能认定为敏感个人数据。例如，美国最高法院在 Carpenter 案中就认为，较长时间范围内的手机位置将暴露个人行踪的全部记录，与 GPS 信息一样，带有时间标记的数据提供了一个关于人们生活的私密窗口，可能揭露了“家庭、政治、专业、宗教和性关系”。〔30〕

通过立法的形式进一步明晰个人信息可能体现的不同权益，并提供分层保护，有利于防疫工作的规范化和对个人权益的保障。具体而言，疫情防控指挥部在制定涉及个人敏感信息的防控措施时应当采取更为审慎的态度，数据控制主体在处理个人敏感信息时也应采取更周全的安全保障措施。但信息本身表现为复杂的利益纠缠，如前所述有些种类的信息如健康数据、基因数据等，单独就构成了敏感信息，而有些数据如个人位置信息、网页浏览记录等，还需要具备一定的时间跨度条件才可能构成敏感信息，想要进行准确定性，不但考验立法技术，同时也需要在信息保护的实践中不断进行总结。

2. 进一步明确疫情防控下个人信息的权利内容

尽管国家市场监督管理总局、国家标准化管理委员会发布了《信息安全技术 个人信息安全规范》（GB/T 35273—2020），对公共利益下个人数据的处理作出了规定，但该规范作为行业标准，仅具有推荐参考意义，并不具法律强制力。此外，该规范的有关规定过于原则，缺乏灵活性，“一刀切”地将公共利益保护作为“知情—同意”原则的例外（包括数据收集、使用、共享、转让、公开披露的告知义务），难以满足个人信息保护的多样化需求。如前所述，即便基于公共利益目的，数据主体也不能随意处理个人信息，而应符合比例原则和保护信息主体权利的要求。GDPR 第 21 条第 1 款就规定，数据主体有权反对控制者为了执行公共利益领域的任务或行使控制者既定的公务职权之必要，对其个人数据进行的处理，包括根据这些条款进行的用户数据画像。除非控制者能够证明其合法利益高于数据主体的利益、权利和自由，或者法定请求权的确

〔30〕 参见楼恺毅：《Carpenter v. United States——论卡彭特诉美国案带来的重要变革》，载微信公众号“清华大学智能法治研究院”，2019 年 11 月 22 日。

立、行使和抗辩有强有力的法律依据。

然而原则本身具有抽象性特质，在疫情防控中要求疫情防控指挥部门和数据处理主体反复以比例原则对涉及个人信息的防控措施和数据处理过程进行审视，难免会增加疫情防控主体和数据控制主体的负担，影响疫情防控的效率，减损疫情信息共享带来的效益，即会引发对疫情防控措施和数据处理行为的合法性质疑，也不利于数据主体依法主张合法权益。为此，应当通过立法的形式进一步完善疫情防控下个人信息权利的具体内容。具体来讲，如果信息主体行使个人信息权利不会严重阻碍防疫目的实现，或是不必要地增加疫情防控主体或数据控制主体的负担，那么就应当赋予信息主体疫情防控背景下的数据权利。例如，个人信息主体查询、更正权利和数据控制主体的告知义务本身不会影响防疫目的实现，且对数据的及时更正反而有利于防疫措施的精准实施。当然，信息主体在行使数据权利时应当秉持诚实信用原则，不得通过反复查询、要求重复告知和故意上报虚假个人信息，不当增加数据控制主体的合规负担。对于删除权应视个人信息可能的作用而区别对待：如果个人信息可以持续用以防疫及相关公共利益目的，如确诊患者的健康数据可用于疫苗的研发、医学研究、传染病持续追踪调查等，则不应允许信息主体行使删除权；如果个人信息如个人行动轨迹信息在疫情消除后没有继续存储的必要，则应当及时删除或应信息主体的要求删除。特别是非公权力主体对其收集的个人信息，原则上在疫情结束后应主动销毁，除非存在其他合法继续存储个人信息的理由。而数据可携带权主要是为了便利数据主体对个人信息的进一步使用或者转移给其他控制者，丰富供给数据主体的服务内容，提升用户体验。〔31〕我国《信息安全技术 个人信息安全规范》（GB/T 35273—2020）通过规定数据主体有权获得个人信息副本来表征数据可携带权。数据可携带权服务于个人信息在不同控制者间的重复利用，对商业主体而言，由于其已经从个人信息的处理中获得了商业利益，要求其满足数据可携带请求具有利益衡平上的合理性。而在疫情防控下，基于公共利益目的收集个人信息的控制者，额外要求其提供结构化、通用化和可机读的个人信息，难免不当增加其负担，不符合比例原则的衡量基准。在疫情防控的背景下，随着个人数据信息内容的不断完善，对于其他各种类型的个人信息权利如拒绝权、限制处理权等，能否以及在多大程度上得到回应，应当结合数据对信息主体的重要程度、对防疫目的实现的关键作用等，在比例原则的指导下进行情景化确定。

（三）完善疫情中个人信息安全管理的组织与技术保障

1. 设立专门机构监督疫情中个人信息的处理行为

目前我国对于个人信息的保护偏重于司法救济（民事诉讼或刑事追责），而欠缺有效的行政救济。〔32〕这一方面是因为，我国没有专门细致的个人信息安全管理规定，行政追责的可操作性不强；另一方面，我国并无专门的个人信息保护机构，而主要由各行业主管部门负责本领域的个人信息保护工作，但不同部门的执法资源、执法手段相差巨大，容易产生监管漏洞。为此，在完善疫情中个人信息保护规范的同时，还应确立专门的个人信息保护机构，从法律层面及时、有效指引和规范疫情中个人信息的利用行为。我国的网信办在个人信息保护执法领域已经积累了一定

〔31〕 参见卓力雄：《数据携带权：基本概念，问题与中国应对》，载《行政法学研究》2019 年第 6 期。

〔32〕 参见郭春镇、马磊：《大数据时代个人信息问题的回应型治理》，载《法制与社会发展》2020 年第 2 期。

经验，可以考虑通过立法的形式确立其在疫情中保护个人信息专门机构的地位，负责保护个人隐私，限制个人信息的收集、披露、处理和共享等数据处理行为，授予其制定配套细则的权力及必要的执法手段包括调查、行政强制和行政处罚等，以及时制止或限制疫情中数据控制主体的不当个人信息处理行为。

除了行政执法外，个人信息保护机构还应向疫情防控指挥部门和数据控制主体提供政策咨询、指导；制定疫情中有关隐私、数据保护的指南；推广隐私增强技术并监督和评估疫情防控措施和数据控制主体的合规性。此外，个人信息保护机构还应承担起受理疫情中个人投诉的职责，并可以要求数据控制主体做出相应回应；在必要时支持并指导个人提起民事诉讼，如果存在潜在犯罪的证据，应将相关情况通报至公安机关进行刑事追责；对于疫情防控指挥部门和公权力数据控制主体，还应当赋予个人信息保护机构向有关机关发出监督建议的权力，督促其及时纠正不当的疫情防控措施和个人信息处理行为，必要时启动行政追责。

2. 引导疫情防控指挥部门和数据控制主体开展内部评估和外部咨询

基于风险控制的考量，不论是疫情防控指挥部门制定涉及个人信息的防控措施，还是数据控制主体处理个人信息，都应履行个人信息保护风险的自我评估和必要时的咨询义务。具体而言，疫情防控指挥部门在制定疫情防控措施时，应当考虑到个人信息保护的要求，防控措施应符合比例原则的要求；数据控制主体要明确个人信息处理生命周期各环节的具体操作规范，加强内部监控，避免不当操作；建立定期测试、评估、评价技术和管理措施是否有效的体系，进一步落实数字控制主体的个人信息保护自查责任。从国际经验看，澳大利亚采取了“创始人”（生成数据的人）的制度，利用数据保护性标识督促数据控制主体履行数据保护义务。当数据生成时，创始人需要评估未经许可访问或不当使用数据所带来的损害及后续影响。〔33〕欧盟采用数据保护影响评估（DPIA）机制，内容包括：个人数据处理行为的性质、范围、内容和目的可能会对自然人的权利和自由产生的风险；基于处理目的对处理行为的必要性和相称性的评估；处理这些风险的预想方案，包括安全和保障措施是否充分；考量个人信息主体尤其是敏感信息主体的权利和合法利益的实现。在疫情中制定防控措施或收集、利用个人信息尤其是个人敏感信息，应当进行充分的合法性和适当性评估，确保个人信息权利的实现。

此外，鉴于公共利益对个人信息权利的克减，尤其是公共利益本身在概念上具有抽象的特质，在防疫工作中不可避免地要进行敏感信息的处理，不当的处理行为难免会造成公共利益与个人信息权利的失衡。为此，当疫情防控指挥部门制定的防控措施涉及个人敏感信息或数据控制者进行个人敏感信息处理时，或者经自我评估发现可能已经造成不相称的后果时，就应当采取更为审慎的态度，及时向个人信息保护监管机构咨询防控措施或个人信息处理行为的妥当性并征得其事先授权。世界范围内，如欧盟数据保护主管部门（European Data Protection Supervisor，EDPS）和新加坡个人数据保护委员会（Personal Data Protection Commission，PDPC），就相关个人信息保护规范的执行已经接受过多次的咨询，并发布了一系列指南，以协助有关机构和个人

〔33〕 See Asia Business Law Institute，Regulation of Cross-Border Transfers of Personal Data in Asia，available at https://www.abli.asia/UploadPDF/DP_Compendium_May_2018.pdf，last visited on Mar. 10，2020.

了解及遵守数据保护法令。〔34〕为此，在疫情防控中，除了数据控制主体应积极向个人信息保护机构咨询以满足个人信息处理的合法性要求外，还应要求疫情防控指挥部门等应急管理责任主体在制定涉及个人信息处理的疫情防控措施的过程中，充分征求个人信息保护机构的意见，实现依法行政与个人信息保护的有机结合。

3. 对疫情中的个人信息采取加密和脱敏措施

基于疫情防控需要，已经形成了公路、铁路、民航、通讯、医疗等疫情相关方多源数据监测、交换、汇聚、反馈机制。〔35〕个人信息需要在公权力主体内部不同部门间以及公权力主体和非公权力主体之间存储、传输、共享，容易导致个人信息的泄露，为此，数据控制主体应当加强个人信息的保密措施。尤其是线下收集及共享个人信息的过程中，应当建立周密的保密组织安排，如：确定专门保密人员负责个人信息的管理，尽可能减少个人信息的不必要接触主体范围；采取合理的保密措施，包括个人信息记录的集中保存等；组织开展个人信息安全培训等。此外，对于广泛利用扫码等进行线上个人信息收集以及利用“重大疫情联防联控网格化管理信息系统”进行不同部门间的个人信息共享、传输，有必要强化数据安全的技术安排，通过数据加密如哈希加密或设定特定访问权限等技术手段，限制个人信息的随意获取，从源头确保个人信息安全。此外，针对疫情预警的需要确需向公众披露个人信息时，应当事先做好屏蔽（或截词）等脱敏处理，包括通过隐藏局部信息令个人信息无法完整显示，或者使用匿名、差分隐私等技术对真实信息等进行处理，以避免个人信息直接暴露于外，进一步落实个人信息收集、利用的安全保障制度。

（四）健全个人信息不当处理的问责机制

数据防疫下，合理的问责机制是确保数据控制主体落实个人信息保护主体责任，维护个人合法权益，实现防疫法治化的重要内容。从责任主体类别上看，主要涉及数据控制主体、数据处理主体等。根据 GDPR 的定义，数据控制者（controller）是指单独或与他人共同确定个人数据处理的目的和方式的自然人、法人、公共权力机关、代理机构或其他机构；数据处理者（processor）是指代表数据控制者处理个人数据的自然人、法人、公共权力机关、代理机构或其他机构。不同身份的主体需要承担不同的数据管理义务。

对于数据控制主体来说，应严格落实疫情中个人信息保护的第一责任人义务，采取合理和必要的措施保障个人信息安全和个人信息权利的实现。如前所述，数据控制主体可以进一步划分为公权力主体和非公权力主体两大类。对于公权力主体，主要是指行政部门，由于疫情应急管理工作面对的是灵活、多变、难以预期的传染病突发事件，为了有效处理危机、防害降损，数据控制主体可能会选择在相对僵化的规则之外行事，如果以此追究其违规的法律责任，不利于应急管理工作的顺利进行。〔36〕为了实现防疫目的，对于法律规范明确规定的数据合规要求，数据控制主体应当严格遵守，否则应承担过错责任；而对于法律规范授予数据控制主体数据处理中自由裁量的事项，固然应当要求数据控制主体遵照比例原则的要求实施具体行为，但在法律评价上不应过

〔34〕 参见刘秀丽：《新加坡〈个人数据保护法〉立法研究综述》，载微信公众号“互联网法治研究”，2020 年 3 月 10 日。

〔35〕 参见李张光：《为打赢疫情防控阻击战提供大数据支撑》，载 http://www.ccdi.gov.cn/yaowen/202002/t20200211_211194.html，最后访问时间：2020 年 3 月 10 日。

〔36〕 参见林鸿潮：《公共危机管理问责制中的归责原则》，载《中国法学》2014 年第 4 期。

分苛责，只要有利于疫情的防控且未严重侵害个人的权利（包括信息自主权和隐私权等），即便存在违反比例原则的不当行为，亦可免责。对于非公权力主体而言，应严格按照行政机关的要求，落实个人信息的收集处理义务，限定个人信息的收集范围，采取适当的信息安全保障措施等，否则应当承担过错责任。如果非公权力主体自行决定以其他合法事由收集利用个人信息（如出于维护个人信息主体或其他个人的生命、财产等重大合法权益等），〔37〕该非公权力主体除了应当履行相应的数据技术和组织安全保障外，还应当进一步举证证明处理个人信息的合法性，否则应当承担过错责任。

对于数据处理主体来说，如在疫情下为数据控制者提供个人信息采集接口的软件运营商，除了应当采取必要的安全技术和组织措施外，如假名化或加密，保障处理系统和服务具备风险应对能力，制定安全措施有效性的测试、评估和评价流程等，还应当严格按照数据控制主体的指示处理个人信息，不得超出数据控制主体委托或授权处理个人信息的内容、性质和目的处理个人数据，否则应当承担相应的过错责任。此外，如果数据处理者超出授权范围自行决定疫情中个人信息的处理目的和方式，则其应当被视为数据控制者，并履行疫情中数据控制者的合规要求并承担相应责任。

Abstract：Big data plays an important role in epidemic situation analysis，transmission path analysis，precise prevention and control and follow-up management，which is conducive to tracing the root of the epidemic in time and effectively cutting off the spread of the epidemic. However，improper data processing may lead to the disclosure of personal information，invasion of personal privacy and damage of personal rights and interests. Therefore，we must follow the path of rule of law in the prevention and control of major epidemics，and deal with the balance between the maintenance of public interests and the protection of personal privacy. In principle，epidemic prevention and control can be used as a legal reason to exempt the obligations of data control subjects and reduce the rights of information subjects. However，the data control subject should still bear the necessary responsibility of personal information security，and follow the basic principles of data processing such as “purpose limitation” and “necessity”. In addition，based on the abstract characteristics of the concept of public interest and the principle of “proportion”，we should further improve the specific legal arrangement of personal information processing in the public interest，and jointly promote the standardized use of personal information in the prevention and control of major epidemics from two aspects of data utilization regulation and private right relief.
Key Words：major epidemic prevention and control，personal information，standardized utilization

（责任编辑：王叶刚　赵建蕊）

〔37〕 参见《信息安全技术 个人信息安全规范》（GB/T 35273—2020）第 5.6 条。