社会治理法治前沿
The Frontier of Social Governance Law
2021 年 第 1 卷 第 3 期

首例涉疫侵犯公民个人信息案引发的思考

杨志航

摘　要 | 疫情期间，传统的“告知—同意”的个人信息保护模式受到冲击，以合作行动模式作为疫情防治的行为模式使得基于公共利益的需要，允许特定主体径自收集涉疫个人信息。应当通过场景化的运用，来作为个人信息收集是否“过度”的前提。所收集到各涉疫个人信息应当采取匿名化的方式进行处理。以公共利益作为侵犯个人信息免责事由的“公共利益”范围应当有所限定。

关键字 | 首例涉疫个人信息案；个人信息；“告知—同意”；公共利益；匿名化

作者简介 | 杨志航，中国应用法学研究所博士后。

2020 年初，新型冠状病毒肆虐给社会经济生活带来了巨大的灾难，可以说是百年难遇的重大公共卫生事件。也正因如此，作为全国首例涉“新冠肺炎”侵犯公民个人隐私权案也得到了极大的关注。案例中所涉及的平衡疫情防治与个人信息保护的问题需要从以下几个方面解读：第一，“告知—同意”在涉疫信息收集的实效，其合理性何在；第二，在个人涉疫信息收集问题上，如何确定一个界限，以防止“过度收集”情形的发生？第三，被告辩称的公共利益其所指为何尚需要具体化的阐释，进而需要解决维护公共利益的主体问题。本文拟以此为讨论的重大，以期抛砖引玉，就教于方家。

一、个人信息与个人信息的处理原则之检视

（一）个人信息的概念

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、身份证号码、个人生物识别信息、住址、电话号码等。在现代社会，个人信息对于社会交往活动来说发挥着重要的作用，一个人出生到死亡，个人信息伴随着其终生，离开个人信息，一个人让别人认知自己，则个人的社会属性将无法体现。明确了个人信息的概念及保护对于保护公民的人格尊严，使公民免受

非法侵扰，维护正常的社会秩序具有现实意义。[1] 可以直接或者间接识别个人身份，从而把当事人直接或者间接地认出来，是个人信息的首要特征。因为个人是社会的人，其需要通过一些信息的传递开展社会交往。在交往过程中有一些信息，譬如姓名等其可以直接关联到特定个人，而有些信息则需要同其他信息结合才可以识别到个人。无论直接还是间接识别，都说明个人信息具有识别性。尤其是在大数据背景之下，这种识别性更被凸显，人肉搜索、网络精准营销等行为的出现都说明了互联网技术会对个人信息进行“野蛮”挖掘行为给人带来了恐惧。[2] 基于此，人们认识到个人信息关系着每个人的切身利益，其应当受到法律的调整和保护。

欧盟法律普遍认为个人信息属于公民基本权利的范畴。《欧盟基本权利宪章》认为“每一个人都有权保护自己的个人数据。”[3] 葡萄牙、西班牙也分别在宪法中规定个人信息为基本人权的范畴。在司法实践中，违法个人信息保护可以作为诉由，通过适用保护个人信息的法律规范进行裁判。欧洲法院认为个人数据保护在《欧洲人权公约》第 8 条的“获得对隐私和家庭生活尊重的权利”的司法实践过程中，起着根本性的作用。[4] 可以识别个人身份的个人信息，可以勾勒出个人的人格形象，尤其是在大数据时代背景之下，人们的各种信息都会被记录、留存，并且通过各种数据之间的相关性进行合理预测，形成较为完整的个人人格剖面图。而人格标识的完整性与真实性是主体受到他人尊重的基本条件。[5] 欧盟的这一做法，体现出了个人信息与人的尊严处于同等的地位。

（二）涉疫个人信息处理的规范分析及检视

《中华人民共和国民法典》第 1034 条对个人信息的概念进行了界定。有关于个人信息的处理，包括了个人信息的收集、存储、使用、加工、传输、提供公开等内容。我国《民法典》第 1035 条、1036 条对此进行了原则性的规定。为做好新型冠状病毒感染肺炎疫情联防联控中的个人信息保护，积极利用包括个人信息在内的大数据支撑联防联控工作，中央网络安全和信息化委员会办公室于 2020 年 2 月 4 日发布了《关于做好个人信息保护利用大数据指出联防联控工作的通知》，其中也明确了涉疫工作个人信息保护工作的要求。《网络安全法》第 42 条规定：“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。”针对涉疫信息的规则中，《传染病防治法》第 12 条也规定：“疾病预防控制机构、医疗机构不得泄露涉及个人隐私的有关信息、资料。”《突发公共卫生事件应急条例》第 21 条、第 36 条、第 40 条也有相关的规定。

然而，在事关大家的防控疫情背景下，以防控之名侵犯公民个人信息的情况不时见于舆论。从重庆女孩个人信息暴露到沈阳尹老太的全网人肉，都表明了公民个人信息保护需要在疫情防治语境下重构。

1. 风险社会下“告知—同意”原则的失效

我国有关于个人信息保护的立法，都将取得当事人或监护人的同意作为信息收集的合法事由，这也符合国际上同行的做法。这种模式，旨在强调个人对其信息的控制，通过赋予用户相关控制权，使其能够知晓与支配自己信息的收集、使用与流通。

---

［1］张新宝：《〈中华人民共和国民法总则〉释义》，中国人民大学出版社 2017 年版，第 220 页。

［2］所谓网络精准营销《中国互联网定向广告用户信息保护行业框架标准》规定为“通过收集一段时间内特定计算机或移动设备在互联网上的相关行为信息，例如浏览网页、使用在线服务或应用等，预测用户的偏好或兴趣，再基于此种预测，通过互联网对特定计算机或移动设备投放广告的行为。”

［3］Char-ter of Fundamental Rights of the European Union，2000/C364/01. 欧盟的《数据保护指令》明确规定：“成员国应当包含自然人的基本权利和自由，特别是他们与个人数据处理相关的隐私权。”See Data Protection Directive，95/46/EC，Sec. 1.

［4］Court of Justice of the European Union，Case F-46/09，para，123.

［5］张新宝：《从隐私到个人信息：利益再衡量的理论与制度安排》，《中国法学》2015 年第 3 期。

基于“告知—同意”所获得的个人信息，主体享有税收撤回该项同意的权利。但是，“告知—同意”原则所成立的现实基础是平和的稳定的社会现实[1]，而非是这样的一个影响社会发展、改变人类思维模式的充满风险的社会。在平和的社会中，个人信息收集者与被收集者之间处于相对均衡的地位，因此，人们对自身信息的被收集似乎也并未感到多么地彷徨。这次新冠疫情的爆发，改变了这种和平，人类进入了一个充满风险的社会。在风险社会中，疫情的防控涉及每一个主体，任何一个（感染、疑似病例）主体的行为，都将产生链式反应，给社会造成不可挽回的损失。美国的疫情防控的失败就说明了这一切。如果仍然固守“告知—同意”原则，则人们将受缚其中，在这样的情形下，人们需要选择合作来获得对来自大自然报复斗争的胜利。这就意味着，实际上收集疫情的一方与被收集信息主体的一方产生了不平衡，以国家或者国家授权的机构为代表的收集个人信息方对另一方收集享有实际上的支配权，这也是社会管理的必然之举。在风险社会，权利旨在最大程度抵消风险带来的冲击与侵害。[2]有关于个人信息的“告知—同意”原则不仅受到学者的质疑；[3]在实际的防控措施中，也无法满足防控的要求。例如在全国很多地方，人们如果不扫码将无法乘车、购买等基本生活要求，此时的“告知 – 同意”将成为不得不同意，信息主体同意沦为纸面上的口号。

2. 合作行动模式与个人信息收集

新冠肺炎疫情是百年来全球发生的最严重的传染病大流行，是新中国成立以来我国遭遇的传播速度最快、感染范围最广、防控难度最大的重大突发公共卫生事件。在习近平总书记亲自指挥、亲自部署下，全国各行业、各地区迅速打响疫情防控的人民战争、总体战、阻击战。这体现了社会主义国家合作模式应对危机的能力。“合作”一词可以说代表了人类有史以来一直向往和追求的共同行动的境界，出于增进共同行动中合作行为的目的，人们越来越倾向于在行动者间的关系、行动体的体制以及规则体系等方面去自觉地做出安排，以求合作行为能够获得某种客观上的保障，从而促进合作行为的增长而不是削减。合作行动模式在具有高度复杂性和高度不确定性的风险社会中，最根本的价值是让人们认识到个人的存在与他人、社会的存在是无法区分开来的。独立个人的生存并非其个人的事情，而是与他人的生存紧密相关。个人、社会和国家在风险社会中并不再是利益排斥的关系，而是共生共存的。如果“这种从个人主义视角出发的互惠互利追求会极大地限制合作行动的适用范围，甚至导致这样一种结果，那就是，在看不到互惠互利的时候，人们就不愿意开展合作。如果从逻辑上去演绎的话，……这会让人出于对自我利益的追求而在一切可能的地方破坏互惠互利。”[4]如此一来，以合作模式的视角看待疫情防治中就不应把个人与国家与社会撕裂开，而是将其看作一个利益的整体。在这种合作模式下，公民的个人信息保护将不再受限于“告知——同意”原则，而是可以因为防控疫情的需要，为了公共利益的需要，允许特定的主体径自收集个人信息。国家标准 GB/T 35273–2020《信息安全技术个人信息安全规范》第 5.6 条规定了征得授权同意的例外情形包括“①与个人信息控制者履行法律法规规定的义务相关的；②与国家安全、国防安全直接相关的；③与公共安全、公共卫生、重大公共利益直接相关的……”。可见，个人信息并非必须严格遵循“告知—同意”原则的，这也是在《民法典》未将其作为权利予以规定的原因所在。强调个人信息应当受到所有者完全控制的个人本位理论在疫情防控的要求下，被合作模式所侵蚀、削弱。但是，合作行动模式并非意味着任何粗暴、非正当以及过度地对个人信息的干扰都是允许的，法

［1］通过告知与同意的方式可以使用户知晓自己个人信息的流向，并且其能够实现对信息的控制权。这种对信息控制权的设想是完美的，用户不仅可以在使用之初知晓本人的何种信息被谁收集，还可以在自身信息被使用前，就是否愿意接受分享作出明确选择。

［2］杨春福：《风险社会的法理解读》，《法制与社会发展（双月刊）》2011 年第 6 期。

［3］任龙龙：《论同意不是个人信息处理的正当性基础》，《政治与法律》2016 年第 1 期；吴伟光：《大数据技术下个人数据信息私权保护论批判》，《政治与法律》2016 年第 7 期。

［4］张康之：《论风险社会中人的生命价值的优先性》，《中州学刊》2020 年第 5 期。

律是保障人们“拥有政治上利用交往自由的机会”的规则，在确保每一个人都获得一片最基本的“私人空间”同时，法律还必须确定一个供人们交往和对话用的“公共领域”。[1]在这片“公共领域”内，需要通过遵循一定的法则——合法、正当、必要、不得过度处理等原则来为个人信息收集的行为划定界限，倘若超过了这一限制，则需要承担民事责任。

3. 关于“过度”收集的进一步思考

尽管我国《信息安全技术个人信息安全规范》第 5 条第 2 款明确规定了收集个人信息的最小必要要求：即收集的个人信息的类型应与实现产品或服务的业务功能有直接关联。直接关联是指没有该等信息的参与，产品或服务的功能无法实现；自动采集个人信息的频率应是实现产品或服务的业务功能所必需的最低频率；间接获取个人信息的数量应是实现产品或服务的业务功能所必需的最少数量。但是，却无法准确掌握这个最小必要的尺度。这是由于个人信息问题，尤其是涉及疫情防控的个人信息是高度场景化的。从我们的日常生活中就可以发现，出现在广阔的户外空间、人员密集的商场、需要高度卫生安全的场所如（政府机构、医院）等，在疫情防控背景下，对于个人信息的收集必然是不同的。与场景高度依存是个人信息收集是否过度需要承认的前提。以隐私场景理论著称的 Helen Nissenbaum 教授曾经指出，数据隐私保护的基本原则与关键在于实现数据的“场景性公正”（contextual integrity），即要在具体场景中实现个人数据与信息的合理流通。[2]以场景化的视角来看待本文的案件，在一个超级市场的购物环境之下，作用经营者的超级市场对消费者个人信息的收集，其内容详细到了个人身份证号码、电话等信息，这一场景是一个人所赖以生存的常见场所，其行为也仅仅是购买南美白虾的行为，其收集内容的详细程度突破了作为消费者允许其收集的内容的合理预期。倘若换一个场景，我们也许会得到认同的结果。在疫情防控关键时期，许多住宅试行封闭式管理，人员需要通过志愿者来进行购买获得，由此所获得的小区居民的手机号码、住宅单位号码则不应当认定为过度收集。

总而言之，这个“度”的把握，需要运用场景化的方法来考察所收集的信息与所要实现的目标之间的关系，倘若所收集的信息的内容符合特定场景下为了防疫所要求的最基本的内容，则应当符合最小化的要求。不仅内容需要符合最小化，有关于人员的数量的考虑，也需要通过场景化的视角确定范围，如一例确诊病例，其本身是独自开车去往人员较少的单位之人，则可能涉及的其他人的包括密切接触者的数量——针对这类信息的收集，也必然与一个乘坐地铁出行，到人员密集的单位工作的信息收集不同。

二、涉疫个人信息的公开——匿名化

流行病学调查，是指疾控人员对病例暴露接触情况、活动轨迹、就医情况等展开的调查，能够为判定密切接触者、采取隔离措施及划定消毒范围等提供依据。但是自从疫情暴发以来，诸如一些病例的相关信息被曝光的事件的发生，使得当事人的人格权益受到伤害。一些城市有关于流调报告出现变化：新增确诊病例流调报告中隐去了病例的性别、年龄、籍贯等个人信息，以涉及区域和场所的信息披露为主。应当承认，涉疫个人信息公开是在疫情防控过程中与个人权益最为密切的一个环节。在防疫背景下，包括确诊病例、疑似病例以及密切接触者等群体的信息通过有关部门的收集之后，需要向社会公开，从而防止疫情的扩散并且能够通过相关群体的行程轨迹进行倒查追踪，将疫情损害降低到最低程度。流行病学调查的最新做法，体现了匿名化与去标识化在涉疫个人信息保护中的重要性。

《信息安全技术个人信息安全规范》第 3.13 条对匿名化（anonymization）进行了规定，是指通过对个人信息的技术处理，使得个人信息主体无法被失败或者关联，且处理后的信息不能被复原

[1] 艾四林：《哈贝马斯论“交往行为”》，湖北大学哲学研究所、《德国学论丛》编委会编：《德国哲学论丛》，中国人民大学出版社 1996 年版，第 90 页。

[2] Helen Nissenbaum, Privacy in Context: Technology, Policy, and the Integrity of Social Life, Stanford University Press, 2009, p. 127.

的过程。在 2016 年通过的《统一数据保护条例》的序言部分指出匿名化是指将个人数据中可识别信息进行移除，使数据主体不会再被识别。[1] 欧盟委员会认为，通过匿名化技术之后，可以有效地保护个人数据，匿名化是可能的而且能够以一种隐私友好的方式满足社会对信息的需求。[2] 如此，一项有效的匿名化措施应对防止任何人从数据中识别出单个个人或推断出任何信息。不仅在欧洲，美国也认识到匿名化对于个人信息保护的重要性。由于美国的个人信息是依附于隐私权的保护来实现自身的权利救济的，因此美国学者认为，个人可识别信息的定义，对于任何一项隐私制度都至关重要，因为个人可识别信息的定义类似于一个适用触发机制：如果属于个人信息，法律就会保护。这一机制意味着个人信息的匿名化是一个隐私风险判断的过程，这一判断结果决定了哪些信息将被去除。这一过程中，首先要去除的是直接标识符，其次要通过相应的评估来决定间接标识符的去或留。所谓直接标识符，也被称作直接识别变量、直接识别数据，是指直接识别到单个主体身份的数据，例如姓名、社会保障号和不需要附加信息或与公共领域中的其他信息交叉关联就可以直接识别个体的数据。所谓间接标识符，是指该标识符本身并不能识别特定个人，但可与其他数据的信息聚合和联系起来识别数据的主体。[3] 鉴于间接标识符在个人信息中的变数风险极大，如果去除过多将可能影响数据的使用，因此美国规定对这种标识符的判断需要引入风险评估系统，通过个案去判断匿名的妥当性。

在个人信息急速发展的时代里，匿名化具有极其重要的意义：首先，个人信息蕴含着人格利益与财产利益。在大数据时代下，个人信息不仅包含着个人生活的痕迹体现着个人的尊严和自由，还与其个人的财产利益相关。这就实际上造成了不法主体对于个人信息的非法收集、使用行为的出现；尤其是随着大数据时代的道路，个人信息中的财产利益更加凸显，甚至有学者指出个人信息是一种财产性权利。这种说法正确与否，还值得商榷，但是可以肯定的是，个人信息一定会给特定的群体带来利益，并以此为源头形成利益链条。而产生这种利益的原因就是在于掌握信息者可以通过个人信息与特定的人联系在一起。其次，个人信息流通的需要。个人信息不是为特定人所把持，唯有使信息流动起来，方才体现出其存在的价值。对于个人信息而言，信息业者与国家有驱动其流通的动力，信息业者通过收集、处理、使用个人信息的前提在于个人信息的流动；国家为了满足特定的管理目的，也需要个人信息的流通；现在，我国已经建成了数据交易中心，就足以说明个人信息其内在具有的流通的需求。为了搭建一个运转有序的信息流通渠道，就应当防止对个人信息非法滥用的空间，因此有学者指出“个人信息保护法的立法原则必须遵循信息社会发展的规律，在保证个人信息自由流通的前提下，对个人信息的商业运用加以合理的限制。”[4] 而匿名化则可以使得不可识别出信息主体身份的“被加工过的”信息得以合理流通。在此，大数据时代的客观要求。大数据，其已经从最原初的“大容量数据”的概念发展为一种生活方式的转变，其突出的价值在于改变了人们获取新知识的方式，这对于个人信息而言也是如此，人们即便足不出户，也可以通过键盘来获得他人的信息。个人既成为搜索他人的人，也可能成为被搜索的人，人们仿佛无时无刻被处于监视之中。既有的规则是无法满足个人信息保护的需求的，因为个人信息其一旦出现便已经形成，法律所能提供的保护不是保护个人信息本身，而是保护个人在个人信息

[1] Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL onthe protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), available at: http://eur-lex.europa.eu/legal-content/EN/TXT?uri=CELEX:52012PC0011.

[2] Information Commissioner's Office: Anonymisation code of practice: managing data protection risk, November 2012, p. 5.

[3] Simson L. Garfinkel: De-Identification of Personal Information, October2015, p. 10, p. 19.

[4] 张素华：《个人信息商业运用的法律保护》，《苏州大学学报》2005 年第 2 期。

使用过程中的权益免于受到不合理的使用。如此一来，唯有通过匿名化才可以实现其在使用过程中的利益。最后，通过匿名化，可以有效防止对涉疫群体进行具象限制所获得的识别。对目标群体进行具象限制，是指通过用户画像所确定的推送群体不能够无限制地缩小。《信息安全技术个人信息安全规范》中明确地提出，“除为达到个人信息主体授权同意的使用目的所必需外，使用个人信息时应消除明确身份指向性，避免精确定位到特定个人。”[1]护个人信息的目的是保护信息主体享有的防止因个人信息被不正当使用而致使其隐私权等人格利益遭受侵害的风险。[2]从原理上讲，我们每一个人，都被一些数据来予以标签化的指向。如身高、体重、运行轨迹、年龄等等。上述信息得到的越多，则一个主体被识别的可能性就越高。而通过匿名化的方式，则可以避免上述情况的发生。

三、对“公共利益”免责事由的反思

我国民法典所规定的个人信息并非一项绝对的权利，当与其他利益冲突之际，就有受到限制的可能。“一个国家可以根据许多的理由取消或者限制权利……这些理由中最重要的理由在于如果涉及的权利不受到限制，那么与之冲突的权利就会受到破坏。当它们发生冲突的时候，政府的任务就是要区别对待。如果政府有理由相信对立的权利中有一方是更为重要的，它就有理由限制另一些权利。”[3]在疫情防治过程中，涉疫个人信息之所以需要让步于公共利益的原因正是如此：首先，涉疫个人信息主体自身具有潜在的危害性。人之所以有理由个别地或集体地对其中任何分子的行动自由进行干涉的唯一目的，乃是自行保护。新冠肺炎是一项对患者身体健康影响严重的疾病，其不仅对患者的肺部产生损伤，对肾功能、大脑神经以及心脏等其他重要器官都有损害。其次，新冠病毒确认患者将对他人的身体健康带来危害。根据流行病学研究发现：新冠病毒比 SARS 和 MERS 更具有传染性。在事实上，这次疫情也出现了传染多人的现象。根据《人民日报》报道，2021 年 1 月 17 日出现 1 传 102 的扩散情况。由此可见，新冠病毒已经通过其极强的传播能力，以确认病例为圆心以该病例所涉及的行踪轨迹为半径向外扩散。这些都表明个人信息，尤其是涉疫个人信息需要且必要受到公共利益的限制。在公共利益界定的问题上，韩大元教授认为：“公共利益是基于宪法共同体价值而确定的价值标准，是社会成员物资和精神需要的综合体，体现了社会、国家与个人之间的利益关系。”[4]也有学者认为公共利益是指公众共同而非个别人或者个别人群享有的利益。[5]王利明教授认为：“由于公共利益概念的宽泛性、内容的发展性、内涵的不确定性、层次的复杂性，在法律上规定公共利益的内涵非常困难。”[6]在中国的司法实践中，有学者提出公共利益可分为 5 种类型，分别为：（1）公共健康、公共安全和环境保护，包括突发公共事件、公共卫生、交通运输、环境资源、安全生产、食品药品、产品质量问题等；（2）公共资源配置和基础设施保障，涉及行政守法、征用、土地和房屋征收、许可、社会保障、资助行政等；（3）促进经济社会发展，包括经济运行、职业保障、商业活动监督、消费者保护等；（4）对政府使用公共资金的监督，包括材质预算决算、行政运行经费使用、重大项目建设等的监督；（5）对国家机关及其工作人员公务活动的监督。[7]上述 5 类公共利益，重要性依次递减。

［1］《安全规范》“7.4 关于用户画像的使用限制”部分。

［2］于海涌、郭嵘：《中国民法典的立法特色和时代亮点》，《地方立法研究》2020 年第 6 期。

［3］［美］罗纳德·德沃金：《认真对待权力》，信春营、吴玉章译，上海三联书店 2008 年版，第 258 页。

［4］韩大元：《宪法文本中“公共利益”的规范分析》，《法学论坛》2005 年第 1 期。

［5］齐爱民：《大数据时代个人信息保护法国际比较研究》，法律出版社 2015 年版，第 75 页。

［6］王利明：《中国民法典重大疑难问题之研究》，法律出版社 2006 年版，第 416–419 页。

［7］蔡星月：《个人隐私信息公开豁免的双重界限》，《行政法学研究》2019 年第 3 期。

也有学者这类公共利益应当主要包括国家公权力机关为了制定国家经济、社会政策的需要而处理有关公民的个人信息，或是为了国家安全、公共安全、公共卫生等处理相关个人信息，以及与刑事侦查、起诉、审判和判决执行相关等事务而需要处理的个人信息。[1]

应当看到，公共利益内容上具有不确定性，这就使得在个人信息保护上如何适用公共利益作为免责事由存在了不确定，因此在具体的法律适用中，本文认为应当从以下几个方面注意：第一，需要考虑不同层次的公共利益与个人涉及信息保护的关系，如前所述公共利益在理论上是具有层次性的，不同层次的公共利益所代表的价值取向并不相同，因此让个人信息屈从于所有被“统称为公共利益”的立场是站不住的，只有与个人密切关系的公共利益才允许成为免责事由，就所列举的 5 类公共利益而言，本文认为只有第一类涉及公民个人的生命健康和社会稳定的公共利益才能够承担起这样的重任，而类似于第二、三类涉及公民的财产权，第四、五类涉及一般公务活动的公共利益无法获得免责。第二，需要考虑以“公共利益”作为限定个人信息的行为给全社会带来的利益是否大于所带来的损害。“一个负责任的政府必须准备证明它所做的任何事情的正当性，特别是当他限制公民自由时。”[2] 这就意味着，公共利益的适用范围不应当过大，如果范围过大的话，政府所采取的防疫措施将远远超过其所可能带个全社会的福祉，我们要避免“大炮打蚊子”的情况的出现。欧盟《个人数据保护比例原则指南》也具有类似的表述。[3] 即使是对一个限制个人信息的行为，如果这个行为能够增加全社会的利益，则可以纳入公共利益之中。例如，在疫情严重地区，在人流密集的场所，诸如火车站、医院等，通过获得公民的个人信息的行为就认为是合理的为了公共利益的做法。相反，如果在一个疫情稳定的普通场所，例如开放的公园，则无法通过公共利益的理论获得支持。承认拉伦茨教授所说：“只有在以下情形当中，个人自由及其私法自治才能受到干预，即对于维护更高的利益而言这是必要的，且此种干预既适于实现预期的目标，也是实现该目的的最缓和的方式。”[4]

［1］最高人民法院民法典贯彻实施工作领导小组主编：《中华人民共和国民法典人格权编理解与适用》，人民法院出版社 2020 年版，第 387 页。

［2］［美］罗纳德·德沃金：《认真对待权力》，信春营、吴玉章译，上海三联书店 2008 年版，第 255 页。

［3］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。

［4］Larenz/Wolf，Allgemeiner Teil des Buergerlichen Rechts，9．Aufl．，Beck，2004 § 1Rn．4．