联合国 A/76/220

大 会

Distr.: General
23 July 2021
Chinese
Original: English

第七十六届会议

临时议程* 项目 75(b)

促进和保护人权：人权问题，
包括增进人权和基本自由
切实享受的各种途径

隐私权

秘书长的说明

秘书长谨向大会转递隐私权特别报告员约瑟夫·卡纳塔西根据人权理事会第28/16号决议编写并提交的报告。

* A/76/150。

21-10203 (C) 110821 190821

隐私权特别报告员约瑟夫·卡纳塔西的报告

摘要

在本报告中，隐私权特别报告员约瑟夫·卡纳塔西旨在进一步阐明如何就隐私权问题管理大流行疫情。这是在特别报告员 2020 年提交给大会的报告(A/75/147)的基础上进行的一项更确切的分析，因为有更多证据可供更准确地评估当前的 2019 冠状病毒病(COVID-19)疫情。特别报告员特别审查了抗击 COVID-19 的措施对数据保护、技术和监视的影响，并指出，各国正在采取的控制 COVID-19 传播的措施继续对隐私权、人格权和其他相互关联的人权的享有产生负面影响。本报告载有对国家和非国家行为体加强隐私和人格、保障儿童在线教育机会、保护信息隐私以及确保透明度和衡量标准的建议。

一. 导言

1. 虽然 2019 冠状病毒病(COVID-19)大流行仍在肆虐，但现在有更多材料显示当前的疫情管理如何可以更好地将隐私权纳入有效的公共卫生措施。

2. 特别报告员在2020年提交给大会的报告(A/75/147)中提出大流行疫情对隐私权的侵犯是否(以及在多大程度上)合法、相称和必要的问题，其目的是弄清应对当前和未来疫情的最佳做法。这个问题仍然没有答案。缺乏准确、可比数据，各国对疫情准备不足，问责存在缺口，再加上各国的政治环境，造成了这种模糊不清的状况。

3. 无论如何，本报告的目的是进一步阐明如何就隐私权问题管理大流行疫情。报告在很大程度上是基于特别报告员与全球隐私大会和经济合作与发展组织(经合组织)2021 年 6 月 21 日至 23 日共同召集的关于 COVID-19 的公众咨询[1] 以及其他研究。

二. 隐私、人格与冠状病毒病

4. 各国为控制 COVID-19 传播而采取的许多措施对隐私权和其他人权的享有产生了负面影响。而现有的结构性不平等、社会排斥和剥夺加剧了负面影响。这场公共卫生危机暴露了国家与企业部门之间的相互依存，以及性别、种族、族裔和社会经济地位与健康结果之间的相互关系。遏制病毒传播的措施涉及对公民具有普遍影响的人权限制措施，但对社会各阶层的影响不成比例。[2]

5. 特别报告员倡导从超越信息隐私[3] 和监控的角度更广泛地理解隐私，强调隐私权对于人与生俱来的尊严积极、促进性的一面，隐私对享有其他人权的促进作用，以及它对任何一个人人格发展的重要性。这与以下方法是一致的：这种方法不是将隐私视为一种处于真空中的人权，而是将其置于与其他权利、特别是它促进或以其他方式帮助实现的权利的关联中加以审视。因此，隐私是 1948 年《世界人权宣言》第二十二条所明确承认的人格发展不受阻碍的权利的一个基本先决条件：“每个人……有权享受……尊严和人格的自由发展所必需的……各种权利的实现。”《宣言》第二十九条还保护个人人格的发展权：“人人对社会负有义务，因为只有在社会中……个性才可能得到自由和充分的发展。”自《宣言》发表以来，在联合国的讨论中将隐私权和人格权联系起来的最重要的一个例子，可以在人权理事会关于数字时代的隐私权的第 34/7 号决议中找到，理事会在该决议中确认，“隐私权可促进个人享有其他权利，自由发展个人的个性和身份特征，

[1] 特别感谢 Elizabeth M. Coombs 教授、Ketan Modh 先生和 Halefom Abraha 先生协助编写和编辑本报告。

[2] “Epidemics have gendered effects” Clare Wenham, Associate Professor of Global Health Policy, London School of Economics and Political Science, cited by Martha Henriques, 13 April 2020. 见 www.bbc.com/future/article/20200409-why-covid-19-is-different-for-men-and-women。

[3] 有时错误地与其子集“数据隐私”互换使用。

培养个人参与政治、经济、社会和文化生活的能力；关切地注意到侵犯或践踏隐私权可能影响个人享有其他人权，包括自由发表意见和持有主张不受干涉的权利以及和平集会和结社自由的权利”。因此，衡量抗疫措施是否成功的综合人权标准必须考虑到多种权利，这些权利由于多种技术特别是互联网接入技术、摄影技术和电话技术而日益复杂地紧密交织在一起，在智能手机的使用中最为集中。

6. 正如文中明确强调的那样，特别报告员关于 COVID-19 大流行的第一份报告[4] 与本文件一样，必然只是一份临时报告，其依据的仅仅是在经历了四个月的疫情之后获得的证据。因此，其主旨是概述公共卫生措施和隐私权的相关主管机构和法律依据。该报告并未涵盖抗疫措施对隐私各个方面的影响，也未涵盖抗疫措施对社会不同群体、特别是弱势和边缘化群体的不同影响。这些重大问题反映了一个社会及其治理机构的质量。是否成功地将所有人权纳入疫情管理就是这种质量的一种衡量标准。

7. 特别报告员 2021 年提交人权理事会的报告(A/HRC/46/37)强调了 COVID-19 对儿童隐私的影响。学校的关闭影响到全球大约 90%的学生。与 2019 年底的周平均水平相比，2020 年的教育应用程序下载量增加了 90%。

8. 转向在线教育扩大了教育技术公司与儿童之间、政府与儿童和家长之间现有的权力不平衡。一些政府放弃了儿童数据隐私法。而在其他地方，例如澳大利亚的一些州，尽管非国家行为体通常控制着儿童的数字教育记录，但政府学校对儿童的隐私权没有保护。这些数字记录包括思维特征、预计学习轨迹、参与度分数、响应时间、阅读页数和观看的视频。

9. 人们不能将大流行病管理与教育分开，同样，也不能忽视教育、隐私和大流行病管理之间的联系。当大流行疫情迫使越来越多的教学转到网上时，对隐私的影响可能被隐藏起来，但却可能是显著的。这一点尤其正确，因为在大多数国家，教育从很小的时候起就是强制性的，大多数儿童和父母并不能质疑教育技术公司的隐私安排，也不能拒绝提供数据，尽管存在合理的担忧。例如，2020 年底对 22 个国家的 496 款教育技术应用程序的分析发现，许多应用在收集设备标识符，27 款应用在获取位置数据，123 款手动测试的应用中有 79 款在与第三方(如广告合作伙伴)共享用户数据。分析指出了数据安全风险。例如，微软报告称，2020 年 8 月 24 日至 9 月 24 日，发生了 570 万起影响其教育软件用户的恶意软件事件。[5]

10. 看似简单的遏制冠状病毒的措施产生了意想不到的后果，其中一些涉及到保护个人隐私。为男女离家从事基本活动(例如获取食物和保健服务)指定不同的日

[4] A/75/147。

[5] 见 Quentin Palfrey and others, “Privacy considerations as schools and parents expand utilization of Ed Tech apps during the COVID-19 pandemic”, International Digital Accountability Council, 1 September 2020. 可查阅 https://digitalwatchdog.org/wp-content/uploads/2020/09/IDAC-Ed-Tech-Report-912020.pdf。

子，[6] 对跨性别群体产生了负面影响。[7] 根据性别限制人们的自由行动增加了男女同性恋、双性恋、跨性别者、性别奇异者和间性者(LGBTQI)在安全部队和警察身份检查期间遭到“揭发”和虐待的风险。疫情开始以来，往往挽救生命的性别确认医疗服务也被许多国家视为“非必要”。

11. 身体的健全和自主关系到隐私。家庭空间本质上更为私密，但在疫情期间被限制在家庭空间内可能会因其他原因而产生问题。据报告，在封锁期间，亲密伴侣和家庭成员基于性别的家庭暴力事件有所增加。[8] 对一些儿童来说，封锁措施增加了他们在家中遭受身体或心理暴力的风险，并限制了他们与可向之报告此类暴力的成年人接触的可能性。[9]

12. 疫情之前和疫情期间的人权评估本可减轻上述风险，因此是未来政策方向的重要组成部分。

三. 隐私、其他人权与冠状病毒病

13. 疫情引发了关于权利及其在民主中的地位的疑问。在 2020 年和 2021 年调查的 13 个国家中，有 10 个国家的社会分裂感自疫情开始以来显著增加。[10] 例如，虽然疫苗护照旨在改善获得权利的机会并放宽旅行限制，但这排除了那些无法获得疫苗、因健康原因无法接种疫苗或选择不接种疫苗的人。目前世界人口中累计属于这些类别的比例非常大。[11]

14. 为了遏制冠状病毒，世界各地的人向政府让出了自己的部分隐私和自由。各国采取的措施影响了表达自由(57 个国家)、集会自由(147 个国家)和隐私权(60 个国家)。[12] 早就应当评估这些侵入现象的相称性和必要性。

15. 随着 COVID-19 监控措施的继续实施甚至扩大，各国政府将有更多机会获得与位置、病史和其他涉及人们生活和财务的敏感信息有关的个人数据。一旦卫生

---

[6] 例如巴拿马和秘鲁等。见 www.reuters.com/article/us-health-cronavirus-peru-idUSKBN21K39N，2020 年 4 月。

[7] 性别认同属于隐私范畴。见人权事务委员会，*G.*诉澳大利亚，(CCPR/C/119/D/2172/2012)，第 7.2 段。

[8] 见“COVID-19 与性别暴力和歧视妇女行为的增加”，暴力侵害妇女行为和妇女权利问题联合国及区域专家独立机制 EDVAW 平台关于在 COVID-19 危机期间抗击针对妇女的性别暴力大流行的联合呼吁，2020 年 7 月 20 日。可查阅 https://rm.coe.int/edvaw-statement-covid-19-and-vaw-final/16809efd2c。

[9] A/HRC/46/19 第 17 段。

[10] 见皮尤研究中心于 2021 年 2 月 1 日至 5 月 26 日对 17 个发达经济体 18 850 名成年人进行的调查。可查阅 www.pewresearch.org/fact-tank/2021/06/24/eu-seen-favorably-across-17-advanced-economies-but-views-vary-on-its-coronavirus-response/。

[11] 见经合组织, “Access to COVID-19 vaccines: global approaches in a global crisis”, 经合组织冠状病毒病(COVID-19)对策(2021 年 3 月 18 日)。

[12] 见国际非营利法中心，“COVID-19 公民自由追踪”。可查阅 www.icnl.org/covid19tracker/?issue=5。

危机消退，一些国家似乎不太可能放弃新的权力和大规模监控工具。在中国，一些城市正在将一款用于追踪冠状病毒的应用程序永久化。更令人担忧的是，“一种新系统使用软件来强制检疫隔离，并似乎向警方发送个人数据，这是自动化社会控制的一个令人不安的先例”。[13] 据说这些风险在亚洲最为突出，[14] 但是在所有国家、包括民主国家，当局都可以利用数据达到政治目的，同时导致人权受损。紧急抗疫措施带来了风险，需要紧急的、高质量的保护。[15]

四. 数据保护、技术、监控与冠状病毒病

16. 与 COVID-19 有关的数据是健康数据，是国际、区域和国家法律规定受特殊级别保护的第一类个人数据。保护健康数据的总体框架已是特别报告员于 2019 年 10 月向大会提交的综合建议[16] 和一份详细的解释性备忘录[17] 的主题，但据估计，约 75%的联合国会员国远未达到这些文件规定的标准。所有现有证据表明，COVID-19 大流行进一步加剧了这些不足。

17. 有效应对卫生危机需要收集和管理敏感数据，并需要强有力的隐私保护。然而，在许多情况下，将数据处理严格限制在具体卫生目的所必需的范围内的制度过去没有，现在也没有。

18. 许多国家缺乏对数据处理的透明度保障和应对数据泄露的保障措施。而在另一些国家，并没有遵循现有的数据保护要求，例如，欧洲联盟委员会在 2020 年 3 月宣布疫情，一年之后，于 2021 年 3 月 17 日提出欧洲联盟数字 COVID 证书，但没有进行影响评估：“鉴于情况紧急，委员会没有进行影响评估。”[18]

19. 这些不足破坏了公共卫生努力和公众对这些努力的信心。例如，60%的美国人认为，即使政府通过手机跟踪人们的位置，对遏制 COVID-19 也不会有太大影响。[19]

20. 数据是许多抗疫措施不可或缺的一部分，随着时间的推移，COVID-19 也变成了一场“数据危机”。政府和科技公司都在处理个人数据和健康相关数据，这引起了人们对所收集数据的必要性和相称性、收集方法、安全性以及这些数据的

[13] Paul Mozur, Raymond Zhong and Aaron Krolik, In Coronavirus fight, China gives citizens a color code, with red flags, *The New York Times*, 1 March 2020, updated 28 January 2021.

[14] 见 Sofia Nazalya, “Human Rights Outlook 2020”, 30 September 2020。

[15] 见 Graham Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight”, 23 June 2021。

[16] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/UNSRPhealthrelateddataRecCLEAN.Pdf。

[17] www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/MediTASFINALExplanatoryMemoradum1.pdf。

[18] 见 Explanatory Memorandum to European Union Commission’s proposal, sect. 3. 可查阅 eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0130。

[19] 见皮尤研究中心2020年4月进行的调查。可查阅 www.pewresearch.org/fact-tank/2020/05/04/how-americans-see-digital-privacy-issues-amid-the-covid-19-outbreak/。

二次使用的关切。[20] 对于 LGBTQI 群体来说一个特别的关切是健康数据的非自愿共享。[21] 由于 COVID-19，现在近一半(48%)的澳大利亚人更关切自己位置信息的保护问题，四分之三(75%)的人认为，COVID-19 并不能作为企业或政府可以不根据隐私法履行其通常义务的借口。[22]

技术

21. 用于管理疫情的技术分为四大类：

(a) 依靠蓝牙近距离追踪的接触追踪和社交距离工具；

(b) 用于登记进入场馆的二维码或条形码；

(c) 通过使用手机信号塔历史或全球定位系统获取地理定位数据，以找出哪些地方的人由于可能靠近 COVID-19 检测呈阳性者而必须得到提醒；

(d) 登记接种疫苗或下载疫苗证书的应用程序。

22. 目前缺乏显示某些技术准确性的数据。有迹象表明，正在使用的技术不可靠。例如，在以色列，人们成功地对通过用手机信号塔三角测量法适用于他们的检疫隔离措施提出质疑。在对隔离令提出上诉的 20 000 人中，54%(约 12 000)的人胜诉。[23] 在美利坚合众国，美国公民自由联盟报告称，手机信号塔的数据不准确。[24]

23. 人们发现，蓝牙近距离追踪也缺乏可靠性。在对德国、意大利和瑞士在欧洲轻轨电车上实施蓝牙近距离追踪情况的研究中，发现探测的可靠性与通过随机选择触发通知差不了多少。[25] 可靠性涉及信号强度，受以下因素影响：手机不同型号/品牌的差异；手机相对方位的波动；人体或容器吸收情况；墙壁、地板和家具的无线电波反射。

数据支持下的疫情监控

24. “监控”是一个用于流行病学研究和疾病防控的术语。它也用于指与情报收集和执法等目的相关的安全活动。两种用途，即医疗和安全用途，均必须必要和相称。

---

[20] 同上。

[21] A/HRC/40/63 2019，第 84 段。

[22] 澳大利亚信息专员办公室，2020 年。

[23] “Over 12,000 mistakenly quarantined by phone tracking, Health Ministry admits”, *The Times of Israel*, 14 July 2020。

[24] 见 Jay Stanley and Jennifer Stisa Granick, “The limits of location tracking in an epidemic” (8 April 2020)。

[25] 见 Douglas J. Leith and Stephen Farrell, “Measurement-Based Evaluation of Google/Apple Exposure Notification application programme interface for Proximity Detection in a Light-Rail Tram” (2020) PLOS One, vol. 15, e0239943。

25. 出于保护公民健康的需要，各国通过以下方式利用监控来跟踪感染的传播：

(a) 人工追踪接触者，如在马耳他；[26]

(b) 在专门设计用于流行病的系统中使用移动电话中的蓝牙、全球定位系统、手机信号塔跟踪和条形码/二维码技术以及可穿戴技术，如在大韩民国；

(c) 使用手机信号塔和其他数据三角测量来源，这些来源最初是作为秘密反恐措施设计的，但被转用于疫情监控，例如在以色列；

(d) 强制使用条形码和二维码办理登记，[27] 如在澳大利亚；

(e) 疫苗护照，例如自 2021 年 7 月 1 日起实施的《欧洲联盟数字 COVID 证书条例》。[28]

26. 这些来源数据的收集和处理在世界各地各不相同，包括收集的类型、存储位置、谁有权访问以及数据被收集者的自主权。许多数据是技术反应的产物，同时也是对它们的输入。技术结构对于公民可以有哪些备选方案来管理其隐私权各方面很重要。

27. 无论是接触者追踪还是疫苗登记，追踪接触者的应用程序都遵循集中式或分散式数据处理方法。集中式和分散式方法的主要区别在于数据的存储位置和数据的处理方式。在集中式方法下，无论用户数据是在哪里生成的，都存储在公共卫生主管部门运营的中央服务器或政府选择的私营公司的服务器上处理。

28. 在追踪接触者的应用程序方面，服务器计算所有相关用户的最新风险分数，并决定联系哪些受影响的用户。在疫苗登记方面，服务器存储关于计划接种周期、接种类型和每个人状态的数据，用于管理目的。

29. 对当局来说，集中式系统可以对收集的数据进行分析，以便除其他用途外，深入了解疫情的传播、受影响最严重的地区和疫苗覆盖率等。这有助于根据既定的优先事项分配资源。

30. 澳大利亚有两个集中式处理的例子：一款蓝牙近距离应用程序(COVIDSafe)和一款用于活动登记的二维码跟踪程序。COVIDSafe 应用程序是通过颁布含隐私保护措施的具体立法来实施的。但二维码追踪程序没有特别立法的支持，而是依赖于以前的卫生条例和现有的《1988 年隐私法》。这一不足是有问题的，因为澳大利亚没有对隐私权的宪法保障。

---

[26] Jessica Arena, “What is contact tracing and how is Malta doing it?” *Times of Malta*, 23 March 2020。

[27] 例如，见南澳大利亚州政府, “COVID SAfe Check-In” (可查阅 www.covid-19.sa.gov.au/business-and-events/covid-safe-check-in)和新南威尔士州政府, “Setting up electronic check-in and QR codes” (可查阅 www.nsw.gov.au/covid-19/covid-safe/customer-record-keeping/setting-up-electronic-check-and-qr-codes)。

[28] 见 https://ec.europa.eu/info/live-work-travel-eu/coronavirus-response/safe-covid-19-vaccines-europeans/eu-digital-covid-certificate_en。

31. 大韩民国通过使用医疗设施记录、全球定位系统数据、银行卡交易记录和闭路电视形成了集中式方法，[29] 这参考了该国早先应对 2015 年中东呼吸综合征爆发的经验。该方法确定患者的行进路线、对附近其他人的接触风险，将接触者分为密切接触者和一般接触者，并通过检疫隔离措施对这些接触者进行管理。

32. 阿根廷也实施了一个中央数据库，通过由 2020 年 3 月 23 日的一项行政决定创建的 Cuidar 应用程序收集数据。[30] 虽然对阿根廷居民来说是自愿的，但对来自国外的旅行者是强制性的，国家和省级政府可以访问蓝牙数据。

33. 集中式架构，包括澳大利亚、以色列和大韩民国的集中式架构，引起了人们对敏感信息(包括健康数据)的保护和安全存储的关切，并担心集中式数据库有极大可能被政府和公司重新用于其他目的(包括政治和商业监控)。

34. 公民对政府建立关于他们的大规模数据库有疑虑。例如，大多数(60%)澳大利亚人同意，为了更好地防控 COVID-19，必须在隐私保护方面做出一些让步，只要这是暂时的。然而，由于 COVID-19 的管理，现在超过一半(54%)的人更关切自己个人信息的保护，其中 26%的人尤为关切。[31]

35. 分散式应用程序可以让用户对自己的信息有更多的控制。信息保存在他们的手机上，而不是保存在政府或其他实体可以访问的中央数据库中。广泛采用的分散式方法的例子包括谷歌-苹果暴露风险通知系统应用程序接口，使用该接口，警告不通过中央数据库处理，而是在用户的手机上自动在本地触发。

36. 各国采用了集中式和分散式措施相结合的办法。新加坡发布了可穿戴跟踪设备，用蓝牙记录与附近跟踪设备的所有交互，这些数据保存 25 天再删除。[32] 这种混合办法促使开发了用于追踪接触者、执行检疫隔离措施、监控症状和提供疫情信息的各种手机应用程序，早在 2020 年 8 月就发现了 46 款应用程序。[33]

37. 这些技术架构共有的一个问题是所采用的技术是强制性的还是自愿性的。如果用户能够通过以下方式选择不接受，则可以认为该应用是自愿性的：

(a) 根本不安装该应用；

(b) 关闭蓝牙/全球定位系统功能；

(c) 使用该应用，但拒绝报告阳性诊断结果。

---

[29] 见“Contact transmission of COVID-19 in South Korea: novel investigation techniques for tracing contacts” *Osong Public Health and Research Perspectives*, vol. 11, No. 1 (2020), pp. 60–63。

[30] 可查阅(西班牙文) www.boletinoficial.gob.ar/detalleAviso/primera/227116/20200324。

[31] 见 2020 年澳大利亚社区隐私态度调查。可查阅 www.oaic.gov.au/engage-with-us/research/australian-community-attitudes-to-privacy-survey-2020-landing-page/2020-australian-community-attitudes-to-privacy-survey/。

[32] 见“TraceTogether, safer together”。可查阅 www.tracetogether.gov.sg/。

[33] 见 Hanson John Leon Singh, Danielle Couch and Kevin Yap, “Mobile health apps that help with COVID-19 management: scoping review”, *JMIR Nursing*, vol. 3, No. 1 (2020), e20596。

38. 在以色列和澳大利亚，尽管对自愿性接触追踪应用的最初反应是积极的，但最终只有一小部分人使用了这些应用。在澳大利亚，《2020 年隐私修正(公共卫生接触信息)法案》(“《COVIDSafe 法案》”)将强制使用 COVIDSafe 应用定为犯罪，[34] 而且最初的公众评估是积极的，得到 70%的受访者支持，但该应用现在“几乎被抛弃”。[35] 澳大利亚各州政府似乎更依赖于使用二维码对进入场馆强制登记。大韩民国制定了一项国家政策倡议，从一开始就采用强制性位置跟踪，一些人认为成功遏制疫情就是因为该政策的强制性。[36]

39. 给予同意和撤回同意的能力是隐私权不可或缺的组成部分。如果接触追踪应用程序是强制性的，则不可能有这种能力。强制性措施还增加了政府和企业通过“监控异变”滥用为抗击疫情而收集的数据，或在数据提供者没有任何能力从数据库中删除其数据的情况下重新调整数据用途的风险。

越线了？

40. 许多国家在应对不断增加的感染和死亡方面准备不足。一些国家认为，必须通过一切可用的手段解决其公民健康和生命面临的风险。无论是有意还是无意，一些政府采取的行动在人权法方面以及民主社会中适当和可接受的程度方面“越线”了。

41. 出于“公共卫生原因”和出于情报或安全目的的监控渠道有时混在一起，失去了重要的分隔和区分。在采用得到公民支持的自愿性方案的背景下，国家的这种行为表明了隐私权和公民自主权是如何被规避的。

以色列

42. 为了说明试图规避权利的问题，人们注意到，以色列政府于 2020 年 3 月 19 日凭借 1940 年《公共卫生法令》宣布紧急状态。[37] 卫生部采用了一款名为“HaMagen”的应用程序，该程序收集用户的移动和位置信息，并将其存储在手机设备的内部存储器中(除非用户选择将该数据发送给卫生部)，而在卫生部，员

[34] 见《2020 年隐私修正(公共卫生接触信息)法案》第 94H 款：

第 94H 款规定 COVIDSafe 的使用

(1) 如果发生以下行为是犯罪行为——要求另一人：

(a) 将 COVIDSafe 下载到通信设备；或

(b) 让 COVIDSafe 在通信设备上运行；或

(c) 同意将 COVID 应用程序数据从通信设备上传到国家 COVIDSafe 数据库。

刑罚：有期徒刑 5 年或 300 个单位的罚款，或两者并处。

[35] Paul M. Garrett and Simon J. Dennis, “Australia has all but abandoned the COVIDSafe app in favour of QR codes (so make sure you check in)”, *The Conversation*, 1 June 2021。

[36] 见 Kyung Sin Park, “Korea’s COVID-19 success and mandatory phone tracking” (opennet, 20 October 2020)。

[37] Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight” (见脚注 15)。

工、代表和服务提供商可以访问该数据。因此，这款应用既是分散式的，也是(自愿)集中式的。

43. 除这一安排外，以色列政府还授权以色列安全局向电信服务提供商索取并收集手机信号塔数据，而无须征得被监控者的同意。根据 2020 年 3 月中旬接连发布的两项紧急法令，电信服务提供商必须根据手机信号塔的记录追踪已知感染者的活动，法令授权警方索取此类数据，以定位患者，对被隔离者进行随机检查，并追溯他们在长达 14 天的时间内的活动。[38] 以色列最高法院于 2020 年 4 月废止这种监控方法，迫使政府通过一项新法律，为授权安全局根据以色列安全机构法继续追踪提供正确的法律依据。随后在 2020 年 7 月，颁布了临时的以色列安全机构授权法。

44. 2021 年初，1940 年《公共卫生条例》的临时修正案授权将未接种疫苗者的个人信息转移给市政当局以及教育和福利官员。2021 年 3 月初，该国最高法院禁止使用授权法进行大规模监控，随后暂停了该修正案的适用。

45. 此外，据报道，疫苗数据被用于：未经同意的大规模人口研究；公开披露感染路径；使用无人机监控居家检疫隔离；利用基因数据公司进行 COVID-19 检测，并公布向警方传递流行病学信息的法案草案。[39]

46. 卫生部发布的分散式 HaMagen 应用最初受到积极评价，并确定了 30%的初始病例，但由于公众对该应用的隐私保护措施失去信任，使用率大幅下降。[40] 该机构的接触者追踪措施似乎效果有限，原因是：

(a) 缺乏关于该机构方案绝对和比较效益的明确数据；

(b) 该技术往往提供假阳性。

47. 以色列采用的系统模仿并使用了反恐技术。据报道，自 2020 年 3 月中旬以来，以色列安全局一直在协助以色列政府进行流行病学调查，向卫生部提供冠状病毒携带者的路线和与其有密切接触的人的名单。这些信息来自该局的通信元数据库。自 3 月以来，以色列政府一直试图加强议会对其情报活动的审查。与法国、荷兰和大不列颠及北爱尔兰联合王国不同，以色列没有一个独立的法定“专家机构”能够作为独立的监督机构来补充议会委员会的工作，因此，人们对是否有能力对情报部门的此类活动进行详细有效的审查仍然十分关切。在以色列部署这种侵犯隐私的技术应对疫情大约一年后，其越线行为于 2021 年 3 月 1 日被最高法院最终宣布为不合法，最高法院禁止政府全面使用手机追踪冠状病毒携带者，称

[38] 见 David M. Halbfinger, Isabel Kershner and Ronen Bergman, “To track Coronavirus, Israel moves to tap secret trove of cellphone data”, *The New York Times*, 16 March 2020。

[39] Prof. Yuval Shany, Israel’s response to the COVID-19 pandemic: Right to Privacy Aspects, Federmann Cyber Security Research Centre, Hebrew University of Jerusalem; “COVID-19: the available evidence … and a little bit of hindsight” (see footnote 15)。

[40] 例如，见 Mitnick J, “How Israel’s COVID contact tracing app rollout went wildly astray” (CIO, 7 November 2020)。

这一措施严重侵犯了公民自由。[41] 特别报告员注意到，有报告称，就以色列而言，这些行动还扼杀了有利于隐私的应用程序的开发和流行病学调查，并认为在纯粹的医疗保健环境中使用反恐权力违反了国际人权法，树立了一个危险的先例。

大韩民国

48. 大韩民国等其他国家政府也迫使电信服务提供商追踪已知感染者的动向。[42] 所实施的监控将智能手机应用程序的使用与传统上在执法和反恐中使用的技术汇集在一起，并结合若干个人数据来源构建一个人的行动画面，包括：

(a) 信用卡和借记卡交易——可以显示一个人在哪里购物或吃饭，以及他们如何通过交通网络旅行；

(b) 从移动运营商处获得的手机位置记录——当一个人连接到不同的塔台时，可以大致了解他在哪个街区；

(c) 大量监控摄像头网络捕捉到的细节。

49. 首先应指出，在大多数已查明的情况下，在大韩民国境内采取的有关 COVID-19 大流行的侵犯隐私措施是有法律依据的。它们是由法律规定的。因此，像以前那样仍然存在一个悬而未决的问题：这些措施在民主社会中是否必要和相称？

50. 要准确回答这个问题，必须详细研究大韩民国究竟发生了什么。所采用的技术似乎确实成功地大大缩短了确定感染地点及其传播方式所需要的时间：

51. 随着 COVID-19 开始传播，大韩民国政府将其正在开发的“智慧城市”数据平台转变为公共卫生追踪工具。韩国疾病控制和预防署开发了流行病调查支持系统，这是一个使公共卫生当局能够快速收集和分析数据以跟踪 COVID-19 确诊病例的平台。该系统于 2020 年 3 月 26 日开始运行，仅在该国首例 COVID-19 病例确诊的两个月后。使用该系统，一旦该署确认一个 COVID-19 病例，获得授权的调查人员就调取每个患者的位置数据，这些数据由各相应实体根据该国的《传染病控制和预防法》输入该系统。然后，该系统进行实时跟踪分析，辅以追踪接触人员的传统人工访谈，实现快速接触追踪和疫情热点识别。该系统使得可以在不到 10 分钟的时间内跟踪和调查 COVID-19 确诊病例，而不是系统运行前的一天或更长时间。通过确保只有具有必要法律权限的该署调查人员才能访问该系统，并记录下每一次系统访问以防安全事故，确保了数据隐私和安全。为了最大限度地减少对个人信息的收集，每个病例的最长数据收集期设定为 14 天，即疾病的

[41] 见 Maayan Lubell, *Israeli Supreme Court bans unlimited COVID-19 mobile phone tracking*. Available at www.reuters.com/article/us-health-coronavirus-israel-surveillanc-idUSKCN2AT279。

[42] 见 Park, “Korea’s COVID-19 success and mandatory phone tracking” (见脚注 36)。

潜伏期。此外，该系统是临时性的：在 COVID-19 疫情结束时，所有个人信息都将被销毁。[43]

52. 上述流行病学调查支持系统是政府采取的几项技术相关措施中的第一项。其次，大韩民国一直在使用智能手机应用程序来监测那些被隔离或检疫者(那些确诊患 COVID-19 者、与确诊病例密切接触者以及国际旅行者)的遵守情况。在整个大流行期间，大韩民国没有对任何进入该国的国际旅行者关闭边境。而是实施了特别入境程序，要求进行 14 天的自我检疫隔离和免费的 COVID-19 检测，以防止传播。自我检疫安全防护应用程序是一个双向应用程序，被检疫隔离者可以报告任何症状，指定的病例管理人员也可以在征得同意后通过基于全球定位系统的位置数据监控个人的检疫隔离合规情况。虽然强烈建议通过该应用程序进行检疫合规性监控，但这并不是强制性的。那些没有智能手机或不想使用这一应用的人可以由病例管理人员通过传统的电话方式进行监控。尽管如此，截至 9 月 1 日，该应用的采用率为 91.8%，大韩民国公民和旅行者都因知道那些有传播 COVID-19 风险的人会遵守自我检疫隔离措施而感到放心。[44]

53. 以下摘要解释了为什么特别报告员认为在某些时期，特别是在 2020 年 1 月至 6 月期间，以抗击 COVID-19 大流行的名义收集大量个人数据既不必要也不相称的一些原因：

> 所披露的接触者追踪数据(例如“地点、时间和持续时长”)有助于人们自我识别与被确认感染者的潜在密切接触者。然而，踪迹泄露可能会带来隐私风险，因为可以推断出一个人的重要地点和日常行为。隐私风险在很大程度上取决于一个人的活动模式，这种模式受到多个区域和政策因素的影响(例如，居住类型、附近的便利设施和社交距离令)。此外，结果显示，大韩民国披露的接触追踪数据往往包括多余的信息，如详细的人口统计信息(例如年龄、性别、国籍)、社会关系(如父母的房子)以及工作场所信息(如公司名称)。披露已确定身份者的此类个人数据可能对接触者追踪没有帮助，因为接触者追踪的目的是找到可能与确认者有密切接触的身份不明的人。换句话说，对于接触者追踪而言，披露被确认者的个人资料及其家庭或熟人等社会关系用处并不大。工作场所的详细位置可以忽略，因为在大多数情况下，很容易通过内部通信网络联系到员工；一个例外的情况是当人们担心潜在的继发群体感染时。同样，也没有必要透露海外入境者的详细旅行信息(这在主要结果中没有报告)，例如抵达航班号和国外旅行的目的/持续时间。[45]

---

[43] 见 Jiyeon Kim and Neil Richards “South Korea’s COVID success stems from an earlier infectious disease failure”, 29 January 2021。可查阅 https://slate.com/technology/2021/01/south-korea-mers-covid-united-states-democracy.html。

[44] 同上。

[45] 见 Gyuwon Jung and others, “Too much information: assessing privacy risks of contact trace data disclosure on people with COVID-19 in South Korea”, *Frontiers in Public Health*, 18 June 2020。可查阅 www.ncbi.nlm.nih.gov/pmc/articles/PMC7314957/ and www.frontiersin.org/articles/10.3389/fpubh.2020.00305/full。

54. 特别报告员在谴责上述明显不必要和过度收集个人数据行为的同时，也提请注意，大韩民国政府和机构尽管采取了 COVID-19 措施，但仍在不断试图加强隐私保护，例如：

(a) 2020 年 6 月和 10 月，疾病控制和预防中心发布了不公布患者年龄、性别、国籍、工作场所、旅行史或家庭居住地点的指导意见，但一些地方政府仍披露一些个人旅行史，尽管有人反对这样做。对收集和处理敏感个人信息的关切依然存在，这些信息可能会泄露个人的性取向和私人关系等隐私信息；

(b) 2021 年 3 月，大韩民国政府要求公众作为防止 COVID-19 传播措施的一部分在餐馆和咖啡馆等地必须写下登记信息时使用其加密的个人号码，而不是电话号码，以保护隐私。2021 年 2 月，政府推出了一项新的隐私保护措施，允许人们使用加密的私人号码访问这些地方：加密号码由四个数字和两个字母组成，不能用于电话或短信。只有在因病毒相关原因迫切需要联系号码持有人时，当局才能将其转换。

55. 特别报告员得出结论认为，大韩民国政府在抗击 COVID-19 的努力中采取了一些侵犯隐私权的措施，这些措施有时既不必要、也不相称。然而，在大多数情况下(如果不是全部)，政府意识到犯了错误，并试图通过纠正措施来改正错误(见上面的例子)。

56. 下图显示了 2020 年 3 月至 2021 年 7 月 19 日大韩民国 COVID-19 大流行期间三波疫情的模式。

统计数字

来源：约翰·霍普金斯大学。

57. 该图显示，尽管感染水平在 2021 年 1 月第三波后明显下降，但到 2021 年 3 月和 4 月，感染水平与 2020 年 3 月第一波期间的前一个最高峰值持平，即每天约有 530 例新病例。然而，到 2021 年 7 月 19 日，这一数字达到了有史以来的最高水平，每天约有 1 300 例新感染病例。尽管实施了各种针对侵犯隐私的保障措施，但在提交本报告时(2021 年 7 月 20 日)，造成这种水平感染的确切原因尚不清楚。这一阶段的结论只能是初步的，因为需要更长时间跨度的更多数据才能确定最终结果。因此，仍无法就大韩民国针对 COVID-19 大流行采取的任何或所有侵犯隐私的措施是否必要和相称作出最终判断。这使得很难确定政府在疫情背景下处理隐私的方法中可能存在哪些良好做法(如果有的话)，除了那些与减少个人数据收集有关的做法，这些做法是作为一项补救措施在 2020 年和 2021 年推出的。

58. 在尼日利亚，全国性的封锁措施导致了致命的镇压和对人权的侵犯，与其他严重的负面影响相比，侵犯隐私可能还算是不那么要命的。除了限制行动自由外，尼日利亚安全部队据报还实施了非法逮捕和拘留，并勒索、扣押和没收财产。[46]

59. 新加坡也提供了一个越线而且是不必要的越线的例子，非常引人注目地说明了功能异变问题。“当局于(2021 年)1 月披露警方在谋杀调查中使用了该应用程序的数据后，公众支持受到了打击——就在几个月前，主管部长才发誓该应用程序只会用于遏制 COVID。政府罕见地发表了道歉声明。但并没有退缩，而是计划将警方在特定案件中获取此类数据的能力正式化，在议会提出拟议的立法。”[47] 根据新加坡议会 2021 年 2 月通过的《2020 年 COVID-19(临时措施)法》新修正案，数字大流行病接触者追踪程序收集的个人数据只能用于接触者追踪，除非执法部门需要这些数据调查“严重犯罪”。[48]

这里谁说了算？

60. 2020 年 4 月，谷歌和苹果公司宣布共同努力，利用蓝牙技术帮助政府和卫生机构减少病毒传播。该解决方案使用了应用程序接口和操作系统级技术，通过分散模式提高了用户隐私和安全性。[49] 由于谷歌和苹果在智能手机市场的主导地位，这两家公司的暴露风险通知倡议为采用分散式方法通过手机进行技术接触追踪划定了议程。该应用已被世界各国使用，包括澳大利亚、美国多个州和大多数欧盟成员国。2020 年 6 月，联合王国政府被迫大转弯，放弃了当时的冠状病毒追踪应用程序的运行模式，转而采用基于苹果和谷歌技术的模式。

---

[46] 见 Simisola Akintoye, “Privacy implications of national responses to COVID 19 in Nigeria”; De Montfort University; Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight” (see footnote 15); “Coronavirus: security forces kill more Nigerians than COVID-19”, BBC News, April 2020。

[47] 见 Jamie Tarabay and Bloomberg, “Countries vowed to restrict use of COVID-19 data. For one Government, the temptation was too great”, *Fortune*, 1 February 2021。

[48] 见 Kirsten Han, “COVID app triggers overdue debate on privacy in Singapore”, Al-Jazeera, 10 February 2021。

[49] 见 www.apple.com/mt/newsroom/2020/04/apple-and-google-partner-on-covid-19-contact-tracing-technology/。

61. 2021 年 4 月，英格兰和威尔士接触者追踪应用程序的一次更新因违反与苹果和谷歌达成的协议条款而被阻止。[50] 各卫生主管部门为了使用苹果和谷歌以隐私为中心的接触者追踪技术而签署的协议规定，不能通过该软件收集位置数据。然而，在拟议的更新中，如果用户的病毒检测呈阳性，则需上传场馆签到记录(海报条形码扫描)。

62. 这些事件彻底暴露了大型科技公司的实力。不管所涉及的合法性问题以及关于哪个机构最具隐私保护立场的问题如何，都需要就政府依赖私营部门向公民提供公共卫生工具的适当性，以及私营部门自行决定提供此类工具的条件的权力进行辩论。不过，法国证明了该国在很大程度上可以采取自己的方式，到 2021 年 5 月，该国在 2020 年 6 月推出的应用已经被超过 25%的法国人下载。[51]

五. 捷径和其他疫情应对机制

63. 许多国家没有做好准备在短时间内采取公共卫生行动，如社交距离、旅行限制和戴口罩。以不同形式采取了捷径，产生了不同的影响。

64. 这些机制包括：第一，宣布紧急状态。迄今为止，已有 108 个国家宣布紧急状态，[52] 以便实施强制性接触者追踪等举措。例如，南非根据其 2002 年《灾害管理法》宣布了紧急状态。

65. 第二：制定规避数据保护和安全的规章。奥地利于 2020 年 3 月对《2012 年健康信息处理法》进行了修订，允许卫生专业人员通过传真或电子邮件等不安全的方式传输健康和遗传数据。[53]

66. 第三：出台新的立法。丹麦于 2020 年 3 月通过了《流行病法》，限制：

(a) 集会权，方法是实施宵禁、限制进入某些地区，并在 2020 年 3 月 18 日至 6 月 8 日期间禁止超过 10 人的集会和聚会；

(b) 人身自由权，方法是强制住院、隔离和接种疫苗，在没有确诊感染的情况下将人拘留；

(c) 尊重隐私的权利，方法是实施接触者追踪应用程序，强制要求个人、企业和公共主管部门提供 COVID-19 相关数据，并采用数据驱动的解决方案来评估活动模式，包括个人的活动模式。

[50] 见“Apple and Google block NHS Covid app update over privacy breaches”, *The Guardian*, 20 April 2021)。

[51] 见 Reuters, “French COVID tracing app downloaded by 25 per cent of the population – minister”, 23 May 2021。

[52] 截至 2021 年 7 月 14 日，国际非营利法中心，“COVID-19 公民自由追踪”(见脚注 12)。

[53] 见修正案：www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20008120。

67. 2021 年 2 月对《流行病法》进行了修订，引入了议会程序和控制机制，以便通过：侵入性规则和措施；提高透明度，减少政府的专断权力；减少针对个人的强制措施，例如，使疫苗接种成为自愿行为；以及对导致监禁处罚的强制措施进行司法控制。

68. 第四，在其他国家，执法部门和民间实体成为执行公共卫生条例的行动人员。2021 年 4 月，根据《马耳他公共卫生法》，公共卫生总监将执行抗疫措施的职权授予：

(a) 警察和地方执法系统机构官员；

(b) 马耳他武装部队；

(c) 马耳他交通运输部；

(d) 马耳他旅游局；

(e) 环境卫生局。

69. 清单上的官员被授权进入住宅并进行检查，只要“有报告或合理怀疑有人违反规定聚集在一起”。这些措施在挑战必要性和相称性原则的同时似乎没有足够的保障。通常，进入私人住所需要司法许可，这个例子表明了卫生紧急权力的巨大范围。

70. 英国等其他国家的执法部门也呼吁获得授权进入涉嫌违反封锁者的家中，认为这是执行封锁措施的“有效手段”，这也凸显了解决公共卫生和执法部门作用和责任的必要性。[54]

六. 其他考虑

71. COVID-19 大流行疫情仍在发展，辩论也将随之改变。当前辩论的一部分包括欧洲联盟从人权角度处理隐私问题，相对于美国以及在某种程度上澳大利亚所采取的保护消费者的角度。美国联邦贸易委员会最近强调了视频会议、教育技术和卫生技术领域的隐私执法，在工作和学校教育转向以数字方式进行后，发布了关于身份盗窃的警告信和诈骗警报。[55]

72. 以往的公共卫生危机影响了各国应对当前疫情的方式。例如，大韩民国由于 2015 年爆发过中东呼吸综合征，使用了强制性、集中式接触者追踪机制。先前的经验导致修订了《传染病控制和预防法》，以保护性别、年龄、教育和国籍信息不被公开披露，但要求强制披露感染状况。

[54] 见“Police Chief calls for power of entry into homes of suspected lockdown breakers”, Vikram Dodd, *The Guardian*, 5 January 2021。

[55] 见 *Federal Trade Commission*, “One year into COVID-19 pandemic, new Federal Trade Commission staff report highlights agency’s ongoing efforts to protect consumers” (19 April 2021)。

73. 国家的地理面积影响了某些措施的隐私保护。较小的国家在应对疫情的某些方面具有优势：例如，尽管新加坡人口密度很高，但却能向个人发放硬件令牌，供那些无法使用智能手机应用程序的人使用，为 TraceTogether 智能手机应用程序的使用提供补充。[56] 另一方面，像印度这样的国土面积和人口规模都很大的国家，通过 CoWIN 应用程序(与个人电话号码相连)推出了在线和基于智能手机的疫苗注册，这没有照顾到许多无法使用智能手机或互联网的人。提供硬件令牌(或者变通或匿名的注册方式)需要发行成百上千万的令牌，但如果不这样做就是歧视。

74. 据报，非洲、拉丁美洲、澳大利亚和印度等区域和国家缺乏宪法保护和(或)强有力的国家数据保护法律和监督机制(虽然不是仅有的这样的区域和国家)，这种缺乏损害了政府为确保公民对公共卫生措施的必要信任所做的努力。

75. 健全的国家级数据保护法和强大、独立的数据保护机构(或世界某些地区的其他监督机构)，有助于开展接触者追踪和疫苗接种登记举措，同时适当考虑保护公民数据的必要性，并将这一必要性传达给社区。

76. 大多数措施收集了大量敏感数据，很难估计这种收集是否相称。即使是公认的强有力的数据保护法律，如欧洲联盟的《一般数据保护条例》，也要求对公共卫生状况进行更多的规范和指导。

77. 新系统建立在现有的、已经很复杂的信息技术基础设施上。正如奥地利数据保护委员会在评估区域举措时指出的那样，由于时限、资源或专业知识，许多国家的数据保护部门无法对这些系统的技术方面以及伴随而来的冗长和高度技术性的描述进行评估。[57]

78. 总的来说，世界各国采用的战略不可避免地导致基本人权和自由被搁置。紧急措施促进了快速反应，但不一定经过深思熟虑。智能手机应用程序或其他形式的监控应该是法律上可接受、技术上可靠、社会能认可的，并经过人权评估方法的测试，在本报告所述期间，人权评估的缺失在很大程度上是显而易见的。

79. 公众信任影响抗疫措施的有效性。尽管在任何政府举措的成功中，对政府的信任都会起作用，但在 COVID-19 大流行等非常情况下最为需要。这对于有效性依赖于公民参与的自愿性措施尤为重要。

80. 隐私侵犯的措施遭到了抵制。在美国，位置跟踪工具和集中式系统遭到了坚决的反对；截至 2021 年 7 月，只有两个州推出了疫苗护照，许多州已禁止使用疫苗护照。[58] 公民担心抗疫措施不会取消。同样，大多数澳大利亚人(60%)同意，

[56] “Token Go Where”. See https://token.gowhere.gov.sg/。

[57] 见 www.bmj.gv.at/dam/jcr:c4b7569c-46c3-4772-bb07-9085f61412a8/Stellungnahme_des_Datenschutzrates_Epidemiegesetz.pdf。

[58] 见 Elliott Davis, “Which States Have Banned Vaccine Passports?”, *US News*, 1 June 2021。

为了更大的利益，必须在隐私保护方面做出一些让步，以抗击 COVID-19，只要这些让步不是永久性的。[59]

81. 技术在政府管理公共卫生问题方面发挥着关键作用。然而，其使用可能会使疫情后的未来监控正常化。例如，政府强制要求的接触者追踪应用程序也可作为政府监控工具用于获取用户个人数据。侵入性技术的正常化为更多侵犯隐私的措施铺平了道路。例如，企业在表面上推出社交距离监控应用和密钥令牌的同时扩大了对员工的监控。

82. 各国政府不愿意或没有能力确定措施的相称性和必要性，这可能与技术功能的悄然异变和所收集的数据以及(或)这些工具无效有关。

83. 由于转向混合工作环境，疫情造成了迄今无法预见的问题，工作人员受到雇主的集体监控。公司实施的监控员工社交距离的措施影响了员工的隐私。虽然许多企业不得不暂停活动，但其他企业则通过要求员工佩戴提供物理近距离警报的设备来绕过这种暂停。许多企业现在有意通过使用软件记录击键情况、截屏和其他计算机活动来监控远程工作的员工。这些技术面临“监控异变”的风险，而其他技术则表现出“任务异变”，不再将可穿戴监控设备的记录数据存储在本地，而是在没有正当理由的情况下将其提供给中央数据库。

84. COVID-19 疫情暴露了现有数据保护法的局限性，无法涵盖这些新出现的对个人数据和隐私的风险。《一般数据保护条例》本来被认为是为全世界的数据保护设定了标准，但该条例没有提供集体索赔的能力，因为主要涉及的是个人权利。[60]

七. 结论

85. 危急关头才能得见国家、政府和私人行为者、包括个人的真本色。

86. 国际条约和大多数国家宪法允许各国在危机、例如应对 COVID-19 大流行期间临时扩大权力。疫情将健康、监控和个人影响交织在一起。因此，需要在为这些领域限定的范围内进行管理。

87. 从隐私权的角度来看，疫情使政府和企业得以更多地侵入人们的生活，侵犯了他们的隐私权。尽管可以预计到出于公共卫生目的，在疫情期间可能会出现一些侵权行为，但迄今为止，事实已证明无法衡量这些侵权行为在多大程度上是必要和相称的。

88. 不幸的是，许多国家将隐私保护与拯救生命的必要措施对立起来。这是一种简单化的观点，忽视了人们对自身隐私，以及对限制政府和商业部门对其生活无端侵犯的重视。其结果是政府疫情管理工作受到阻力。

[59] 澳大利亚信息专员办公室。

[60] 见 Andrew Pakes, “High Visibility and COVID-19: returning to the post-lockdown workplace” (Ada Lovelace Institute, 19 May 2020)。

89. COVID-19 大流行使世界各地在实施国家公共卫生战略方面采取了捷径。一些政府利用紧急状态法出台强制性接触者追踪举措；另一些政府则利用缺乏强有力的国家级数据保护法律的情况迅速推出解决方案，如接触者追踪和接种疫苗者登记，而不理会隐私权或其他人权。危机应对措施(其中一些是“下意识”的)包括利用紧急状态法和薄弱或不存在的数据保护法。迫在眉睫的选举似乎已经并将继续是一些国家和政府的重要考虑因素。[61]

90. 会员国使用了技术工具来跟踪感染情况、执行检疫措施、维持社交距离规则、跟踪疫苗管理。这些工具是政府机构和企业实体开发的。

91. 在这种背景下，各国对科技公司发挥独立性和权力的情况准备不足，比如苹果和谷歌在接触者追踪应用程序用户隐私方面的立场。与此同时，有必要承认，这两家公司的做法似乎对隐私提供了合理的保护，在某些情况下可能比一些热衷于使用所收集的数据的国家更保护隐私。

92. 当前持续的疫情意味着促进和保护隐私权和相关权利需要国际、区域和国内各级机构的持续监测和公开报告。

93. 集中式方法，包括澳大利亚、以色列和大韩民国所采用的方法，存在隐私风险，例如敏感信息包括健康数据的保护和存储、这些集中式数据库被政府和企业重新利用的很大可能性，以及数据很大程度被保留的风险。分散式应用程序为用户提供了对其信息的更多控制，因为所有接触信息都只保存在用户的手机上，没有可供政府或当局访问的中央数据库。

94. 强制性接触者追踪应用程序对隐私的影响是显而易见的——在许多(尽管不是全部)情况下，同意和撤销同意的能力已被法律认定为隐私权的内在组成部分。强制性措施还增加了政府和企业通过“监控异变”，或者在用户没有任何能力将其数据从数据库中删除的情况下调整数据用途，从而滥用为抗击疫情而收集的敏感数据的风险。自愿性的接触者追踪应用程序的使用率很低，这通常是因为公众对政府保护其数据安全的能力缺乏信任。

95. 技术还存在多种实施问题，包括某些技术缺乏能展现其准确性的数据。所讨论的大多数措施收集大量敏感数据，很难估计这种收集是否相称。虽然技术在疫情中发挥了关键作用，但未来也可能使监控正常化。密集而无处不在的技术监控并不是应对 COVID-19 等大流行病的灵丹妙药。

96. 其他相关问题包括平等和工人隐私保护。数据保护法、包括《一般数据保护条例》中存在漏洞。需要对其条款的解释和修正提供更好的指导。这些法律通常是关于个人权利，而不是集体隐私主张，随着人工智能的出现，例如越来越多的工人转向混合工作环境，这一点将变得较为重要。

97. 迫切需要共同的隐私数据原则，可以适用于所有规定在应对疫情时采取数据收集举措的立法。这些原则将为当前以及未来的疫情设定一个共同、可互操作的

[61] 见 www.idea.int/news-media/multimedia-reports/global-overview-covid-19-impact-elections。

标准。Graham Greenleaf 已提出了这样一套标准，这里对这套标准进行了调整，从原初设计上就将隐私包含在内。[62]

98. 现在是为未来疫情做准备的最佳时机。[63] 这些教训不仅适用于 COVID-19，也适用于其他应通报的传染病和未来可能出现的大流行病。

八. 建议

99. 这些建议旨在确保每个人在当前和未来的公共卫生危机期间享有隐私权，不受任意干涉，正如《世界人权宣言》(第十二条)、《公民及政治权利国际公约》(第十七条)和条约机构结论所规定的那样。

100. 以下建议旨在涵盖国家和非国家行为体。

隐私和人格

101. 国家和非国家缔约方应落实《工商企业与人权指导原则：实施联合国“保护、尊重和补救”框架》及其性别问题指导意见(A/HRC/41/43，附件)。

102. 采纳隐私权特别报告员关于防止隐私受到基于性别的侵犯的建议(A/HRC/43/52，第 33 和 34 段)。

103. 鼓励与民间社会和工业界建立伙伴关系，共同制定战略和技术对策。

104. 让社区中尤其面临风险的群体参与关于具体公共卫生措施的协商。

105. 要求在推行措施、战略和立法之前进行对性别问题具有敏感认识的隐私人权影响评估，从而减少疫情防控对隐私的基于性别的侵犯。

106. 定期评估所采取的措施的有效性，以便将弱势和边缘化群体纳入应对和恢复工作。

儿童

107. 根据《儿童权利公约》第二十九条第 1 款和欧洲委员会关于教育环境中儿童数据保护的准则，制定全面的在线教育行动计划。

108. 确保为在线教育建立并维持适当的法律框架。

109. 为非商业性教育和社会空间建立公共基础设施。

110. 确保根据合法的法律依据，利用代表最佳做法的数据保护框架、如《一般数据保护条例》和《第 108+号公约》，公平、准确、安全地处理儿童的个人数据。

[62] 见 Greenleaf, “COVID-19: the available evidence … and a little bit of hindsight” (见脚注 15)。

[63] 见“现在是预防下一次大流行病的最佳时机：各国共同呼吁更好地做好应急准备”(世卫组织，2020 年 10 月 1 日)。

信息隐私

111. 将人权纳入应对疫情的技术方法的设计、开发和部署。

112. 各种应对疫情的卫生措施都需要基于共同原则、针对具体情况提供指导的立法保护。特别报告员建议在评估世界各地的疫情防控政策时，对于集中式和分散式公共卫生监控系统、针对传染病的立法措施及其运用，采用 11 项共同原则：[64]

(a) 从一开始就从“原初设计”和“默认”角度确立隐私，以总体人权评估与数据保护评估相结合的方式对公共卫生措施进行评估，特别关注流行病和大流行病；[65]

(b) 防控任何流行病或大流行病从一开始就应考虑隐私问题。事实上，这应是任何关于如何应对疫情的国家战略的基石，经过深思熟虑，作为不可或缺的一部分提前多年准备并很好地纳入——这是上述总体人权评估的一部分；

(c) 在区域或各国数据隐私法中加入明确、详细的控制措施；

(d) 以比授权法案或条例更有效的方式提供必要的明确性和法律基础，并在管辖上实现更大的统一性；

(e) 保障进入和参加场所、活动、设施、教育等的机会，避免歧视；

(f) 必须保护受疫情监控措施不利和不同影响的弱势群体；

(g) 最大限度地减少和界定 COVID 数据的授权使用，以确保 COVID-19 数据在收集后不会用于其他目的；

(h) 像许多现有的数据保护法一样，确立“目的规范”；

(i) 尽量减少数据收集；

(j) 为确保数据收集措施相称，制定普遍接受的风险管理方法，并协助限制因数据泄露、网络事件和功能异变造成的损害；

(k) 反胁迫条款：应立法加以防止或严格界定和制止关于使用或出示使用证据的要求。应通过将这种行为界定为法律规定的犯罪行为来防止提出其他要求，或要求查看使用证书。执行是必要的，补救措施也是必要的；

(l) 防止“监控异变”：避免仿效新加坡的做法，新加坡在 2020 年承诺“仅用于追踪”，然后在 2021 年食言，允许开展刑事调查；

(m) 大多数疫情预防措施所要求的自愿参与需要公众信任才能发挥作用。未来作为一种监控措施扩展到刑事调查等其他领域的做法必须被定为非法，才能使这一信任存在下去；

[64] 可查阅 https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3875920。

[65] 见欧洲委员会“2020 Digital Solutions to Fight COVID-19 2020”, Data Protection Report October 2020。可查阅 www.coe.int/en/web/data-protection/-/digital-solutions-to-fight-covid-19-council-of-europe-report-on-data-protection-2020。

(n) 持续删除方案(如果收集了数据)：立法本身应要求在短时间内持续删除任何收集的数据——例如个人的传染期或其他一些基于证据/科学的时间段；

(o) 必须在法律中确立整个系统的“日落条款”和所有疫情数据系统的强制性独立“关闭审计”，并加以严格执行：确定一个固定期限或对必要性的独立评估，以确保疫情监控系统关闭，并实施一项基于法律的独立审计规定，确保确实进行了审计；

(p) 由独立的数据保护机构进行监督和定期公开报告：对这些监控系统的监督必须由外部进行并且是独立的；

(q) 透明度：应与专家和民间社会协商确定必要的条件。其形式可以是发布任何用于构建监控系统的源代码(如接触追踪应用)，进行全面的数据保护影响评估，以及发布疫情监控技术的有效性数据。

113. 关于大型科技公司在疫情中发挥隐私保护作用的角色和责任的正式和非正式的公开辩论，应以与大型科技公司的持续对话来加以补充。

透明度和衡量标准

114. 卫生紧急权力需要在必要性和相称性方面加以评估。作为这一定期评估的一部分：

(a) 隐私权特别报告员应单独并与其他任务负责人一道，至少每 24 至 36 个月重新审视一次应通报的传染病情况，特别关注 COVID-19 但不限于 COVID-19，以便确定现有和新出现的风险，并了解可用于在保护人权的整体性办法范围内预防大流行的最有效且有利于隐私的政策举措；

(b) 如果一国决定技术监控是应对 COVID-19 大流行的必要措施，它必须证明具体措施的必要性和相称性，并制定一项法律明确规定这种监控措施，其中包含强制性、明确而具体的保障措施；

(c) 鉴于数字技术对广泛的权利、特别是隐私权的巨大影响，各国和各企业应在设计、开发和部署应对疫情的技术方法中纳入人权；[66]

(d) 各国和各企业应采用以用户为中心、尊重权利的技术设计，从而(以“疫苗护照”为例)使旅行者可以自己携带数据，以备出示；

(e) 需要对各国的疫情应对措施进行外部审查，并应在联合国一级的定期审查中评估各国的疫情管理及其他内部人权责任。

[66] 见 A/HRC/46/19。