



人权理事会

第四十届会议

2019 年 2 月 25 日至 3 月 22 日

议程项目 3

促进和保护所有人权——公民权利，政治权利，
经济、社会及文化权利，包括发展权

隐私权

隐私权问题特别报告员的报告*

概要

隐私权问题特别报告员在依照人权理事会第 28/16 号和第 37/2 号决议编写的报告中重点讨论情报监督问题，并联系隐私与个性问题工作队关于隐私权与性别问题方面工作的第一份报告以及健康数据问题工作队的第二份报告。

* 本报告迟交，以反映最新信息。



目录

	页次
一. 活动概述.....	3
二. 联系背景看待隐私权.....	3
三. 安全与监控.....	6
四. 隐私权：性别视角.....	10
五. 结论.....	17
六. 建议归纳.....	18
七. 健康数据的保护.....	18
八. 隐私权指标.....	22

一. 活动概述

1. 自 2018 年 3 月以来，隐私权问题特别报告员以若干方式推进了自己的任务：对包括新技术带来的挑战等相关信息进行研究、开展正式和“非正式”国别访问、推动保护隐私权、倡导隐私原则、参加国际活动促进对隐私权采取一致的方针、提高对隐私权和有效补救措施的认识，以及报告指称的侵权情况。
2. 特别报告员于 2018 年 10 月向大会提交了一份关于大数据和开放数据问题的报告(A/73/438)。
3. 特别报告员自提交人权理事会的 2018 年年度报告(A/HRC/37/62)以来开展的活动包括：
 - (a) 与工作队主席一起推进 5 个专题行动系列工作队的工作：大数据和开放数据、健康数据、隐私和个性、安全和监控，以及公司对个人数据的使用；
 - (b) 合计向会员国发出 24 封提出与隐私权有关事项的信函，以及 14 份新闻稿和声明；¹
 - (c) 对大不列颠及北爱尔兰联合王国(2018 年 6 月)和德国(2018 年 11 月)进行正式国别访问；
 - (d) 国际主旨文件和其他文件；²
 - (e) 与一系列机构进行磋商，例如爱尔兰公民自由理事会、日本自由人权协会、日本律师协会联合会、隐私国际、北爱尔兰人权委员会，并参与互联网治理论坛和 RightsCon 等许多机构的多项活动；
 - (f) 与各方交流信息：政府(国家和国家以下各级)、数据保护和隐私专员、欧洲联盟“第 29 条”数据保护工作组主席、欧洲委员会《关于在自动处理个人数据方面保护个人的公约》(第 108 号公约)协商委员会主席、标准制定组织，如：国际电信联盟、电气和电子工程师学会、民间社会组织、常驻联合国日内瓦办事处代表团、特别程序任务负责人、联合国人权事务高级专员办事处、研究人员、学者、专业团体。

二. 联系背景看待隐私权

4. 隐私权可以促进其他人权的享有。同样，侵犯隐私权会限制其他人权的享有。
5. 会员国批准国际人权文书，却缺乏真正意愿采取必要措施执行这些文书，这种情况不乏史例。史例之一就是德意志民主共和国，该国于 1973 年 11 月 8 日批准了《公民权利和政治权利国际公约》，承担了尊重隐私权(第十七条)等权利的义务，同时却维持着一个以广泛和系统侵犯大量公民隐私而闻名的监控制度。

¹ 合计 18 封信函和 6 份新闻稿是与其他特别报告员联合发出的。

² 见 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex1_Keynotes.pdf。

6. 很遗憾，特别报告员今天还经常发现类似的矛盾：虽然大多数会员国明确承诺保护隐私权，但许多会员国的行为方式却越来越使隐私权面临风险，它们采用了与隐私权相悖的新技术，如大数据和健康数据，侵犯公民基于性别或性别认同和表达的尊严，以及任意调查自己的公民。

7. 《公民权利和政治权利国际公约》第一条第一款宣布的自决权允许所有人民决定自己的政治地位并自由追求自己的发展。同样，《公约》中的所有基本自由，包括迁徙自由权(第十二条)或结社自由权(第二十二条)、宗教自由权(第十八条)、言论自由权(第十九条)和隐私权(第十七条)，都保护所有个人的个人自主权。公民选择什么、选择时间、选择地点和方式、选择与谁在一起以及选择想什么和说什么的权利，是各国同意在《公约》之下保护的不可剥夺的权利的一部分。

8. 隐私权是关于个人自主权的讨论的组成部分。早在 1976 年，Paul Sieghart 就确定了隐私、信息流、自治和权力之间的以下联系：

在一个现代信息技术飞速发展的社会，许多其他人可能会发现我们如何行动。反过来，这可能会减少我们随心所欲地行动的自由——因为一旦别人发现我们如何行动，他们可能会认为，劝阻、压制乃至阻止我们做自己想做的事情，设法操纵我们做他们想做的事情，不仅符合他们的利益，而且符合社会的利益，甚至符合我们自己的利益。³

9. 特别报告员以下列方式将这一立场与隐私联系起来：

除去保护一个人的隐私外衣，他就变得透明，因此可被操纵。一个可被操纵的个体，只能听任控制他信息的人支配，而他的自由——通常充其量只是相对的——与控制信息的人给他留出什么性质的选项和替代办法在程度上呈正比。⁴

10. 正因为如此，隐私与有意义的个人自主如此紧密地联系在一起。侵犯隐私通常是威胁其他自由的系统的一部分。国家行为者侵犯隐私往往是为了攫取和保持权力，但非国家行为者也是如此，如希望继续控制他人的个人或公司。所以，在许多情况下，特别报告员必须考虑侵犯隐私权如何与其他侵权联系在一起。

作为限定权的隐私权与民主社会的必要性标准

11. 隐私权不是一项绝对权利，而是一项限定权利。它可以受限制，但限制总是以非常谨慎的方式界定。根据《公民权利和政治权利国际公约》第十七条确立的标准，国际人权法只允许对隐私权既不是任意也不是非法的干涉。人权事务委员会在关于隐私权的第 16 号一般性意见(1988 年)中解释说，“非法”一词的意思是除法律所设想的个案以外不得有干涉情事，而法律本身必须符合《公约》的规定、宗旨和目标。委员会认为，任意性的概念用意是确保即使法律规定的干涉也都符合《公约》的规定、宗旨和目标，而且无论如何要在个别情况中合情合理。

³ Paul Sieghart, *Privacy and Computers* (London, Latimer New Dimensions, 1976), p. 24.

⁴ Joseph A. Cannataci, *Privacy and Data Protection Law: International Development and Maltese Perspectives* (Oslo, Norwegian University Press, 1986), p. 60.

12. 人权事务委员会在关于《公约》缔约国的一般法律义务的性质的第 31 号一般性意见(2004 年)中规定, 缔约国不得侵犯《公约》所承认的权利, 只有在符合《公约》有关条款的情况下才能对其中任何权利进行任何限制。在进行限制时, 缔约国必须说明其必要性, 而且所采取的措施必须与追求合法目标相称, 以便确保不断和有效地保护《公约》权利。委员会进一步强调, 在任何情况下都不能以可能损害《公约》权利实质的方式实行限制。

13. 《公民权利和政治权利国际公约》的两个条款明确引用了“民主社会……必要”一语: 第二十一条(和平集会的权利)和第二十二条(结社自由), 但第十七条没有。

14. 《保护人权与基本自由公约》(《欧洲人权公约》)第 8(2)条明确规定了限定的性质:

公共当局不得干涉这项权利的行使, 除非这是依法进行的, 并且是民主社会为了国家安全、公共安全或国家经济福祉、防止混乱或犯罪、保护健康或道德、或保护他人权利和自由所必要的。

15. 1948 年《世界人权宣言》宣告民主是享受人权的基本背景的一部分, 其中第二十九条提出了“民主的社会中……普遍福利”的概念。1950 年通过的《欧洲人权公约》的作者和签署者与《公民权利和政治权利国际公约》的作者之间的相互作用持续了 15 年的大部分时间, 直到后者于 1966 年出台。“民主社会中的必要”的概念至少出现在《欧洲公约》的 6 个条款中, 包括以上引用的第 8 条, 这个概念之后又融入《公约》, 最好的例证是第二十二条款第二款:

除依法律之规定, 且为民主社会维护国家安全或公共安宁、公共秩序、维持公共卫生或风化、或保障他人权利自由所必要者外, 不得限制此种权利之行使。

16. 然而, 第二十二条款涉及的是集会自由, 而不是隐私权。要由研究《世界人权宣言》和《公民权利和政治权利国际公约》沿革的历史学家解释为什么第二十一条和第二十二条款而不是第十七条明确使用了“民主社会中……必要”一语, 但是特别报告员按理也必须运用同样的标准, 也就是说, 这项权利只能由法律规定的措施限定(第十七条第二款), 而且这种措施必须是民主社会中必要的, 因而需要以符合《公约》第十四条、第二十一条和第二十二条款的方式解读什么是“任意或非法干涉”。

17. 这一解读符合人权理事会第 34/7 号决议第 2 段, 其中重申各国应确保对隐私权的任何干涉都符合合法性、必要性和相称性原则, 反映人权事务委员会判例中使用的术语(CCPR/C/USA/CO/4, 第 22 段)。

18. 故此, 关键的四重判据是, 任何正当侵犯隐私都(a) 不能是任意的, 必须由法律规定; (b) 除用于民主社会所必需的目的之外, 不能用于任何其他目的; (c) 除用于“维护国家安全或公共安宁、公共秩序、维持公共卫生或风化、或保障他人权利自由所必要者”之外, 不能用于任何其他目的; (d) 措施必须与所管理的威胁或风险相称。

19. “必要”和“民主社会中的必要”这两个判据是对会员国采取的任何可能被认为侵犯隐私的措施的基本判据。另外一些权利唯有依靠隐私权才能得以行使, 在审视对这些权利的侵犯时, 也必须考虑到这两个判据。

20. 正因为隐私问题的背景以及自治、隐私和民主国家必要措施之间的联系，所以特别报告员优先考虑拥有坚实民主体制和保障的国家，因为在这些背景下，他的干预更有可能对隐私权的享有产生积极影响。在民主保障较弱的国家，他正在寻找正面干预的机会。

21. 2019 年和 2020 年期间，特别报告员将进一步集中关注非洲、亚洲和南美洲，计划在这些地区各进行一次访问；但是，除其他外，他将在民间社会的协助下，继续监测其他国家的情况。这并不是对世界其他地区的隐私体验无动于衷。由于时间、资源和在实地开展有意义调查的机会这三个因素，不可能以特别报告员希望的详细程度或方式调查这些经历。就此而言，特别报告员将继续监测法治被“以法管治”取代的国家，以及法律成为政权控制和压迫工具的国家。他将评估中东和北非区域网络犯罪立法的制订情况，这种立法可能对隐私权的享有带来风险。⁵

从性别角度看待隐私、技术和其他人权

22. 本报告介绍特别报告员正在进行的隐私与性别问题工作的初步结果。隐私与人格问题工作队将继续开展工作，研究隐私与性别平等之间的联系，不论其形式或表达方式如何。除了就报告进行磋商之外，⁶ 特别报告员计划在未来三年更加关注这一领域，包括隐私、自治和一些国家不同程度的男性监护制度之间的联系。

23. 希望参加隐私与性别问题磋商的会员国应在 2019 年 3 月 31 日前登记参加的愿望。

隐私与健康数据

24. 本报告还详细介绍特别报告员在隐私与健康数据问题上持续开展的工作。像性别问题上的工作一样，还有一些新出现的重大问题，如遗传学、基因组研究和生物银行。特别报告员面临的一个问题是，收集某一特定国家全体人口的 DNA 数据是否必要和相称。特别报告员的任务将是与将此类措施纳入立法的国家一起处理这些问题。

25. 健康数据问题工作队确定了一系列问题，所涉事项包括土著数据主权、囚犯人数、法医数据库、“智能”植入式医疗装置、能随时将实际生活数据传回公司的设备/义肢——从而将“身体定为数据”并在法律诉讼中使用，以及人工智能/机器学习和自动处理。这些问题将在 2019 年的磋商中探讨。

三. 安全与监控

26. 特别报告员的任务产生于国际社会对爱德华·斯诺登揭露情报机构活动的愤怒，特别是在国家安全保护方面。

⁵ Wafa Ben-Hassine and Dima Samaro, “Restricting cybersecurity, violating human rights: cybercrime laws in MENA region”, Open Global Rights, 10 January 2019.

⁶ 见 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf。

27. 为了加强情报领域的隐私保护，特别报告员发起了国际情报监督论坛，该论坛于 2016 年在布加勒斯特、2017 年在布鲁塞尔和 2018 年在瓦莱塔举行了会议。2018 年会议后，特别报告员报告说：

(a) 欧洲联盟《通用数据保护条例》⁷ (2018 年 5 月 25 日生效)和《警务指令》⁸ (2018 年 5 月 6 日生效)等最近的区域举措虽然重要，但不足以将隐私保护扩大到国家安全领域，包括监督为国家安全目的开展的情报活动。⁹

(b) 《第 108 号公约》¹⁰ 的现代化修订是最近于 2018 年 10 月 10 日正式启动的一项全球举措，联合国 193 个会员国中有 70 个参加了该举措，该公约因其第 11 条而受到赞扬，该条载有一套高等级的原则和保障措施，与《通用数据保护条例》不同，这些原则和保障措施也适用于为国家安全目的开展的活动。

28. 特别报告员在提交大会的 2018 年报告(A/73/438)中，建议鼓励所有会员国批准现代化的《公约》(《第 108+号公约》)。联系可能侵犯隐私的情报监督和国家安全活动，联合国会员国立即部署《第 108+号公约》第 11 条概述的标准和保障措施，对于保护基本隐私权是适当的。

29. 这些关键的保障措施和标准，特别是相称性和必要性的保障措施和标准，为欧洲人权法院 2018 年两项里程碑式判决的推理提供了依据，这两项判决都与情报机构的活动密切相关：Centrum för Rättvisa 诉瑞典(2018 年 6 月 19 日)和 Big Brother Watch 等诉联合王国(2018 年 9 月 13 日)。

30. 鉴于欧洲委员会有 47 个成员国之多，而且该区域情报部门触角遍布全球，这些判决具有潜在的全球影响。

31. 特别报告员支持在民主社会中严格适用相称性和必要性判据，认为这是具有全球影响的重要基准。其他地区的情报机构可能会受到欧洲日益严格的标准的影响。因此，包含往来于欧洲的个人信息和其他个人数据的情报分析需被置于相应的严格监督之下，以确保这些尊重隐私的标准在欧洲得到坚持，并成为全球可能的良好做法和典范。

32. 必须指出，在评估任何联合国会员国提供的法律保护时，“民主社会”这个限定词是判据的一个基本部分。许多新技术，特别是互联网、智能手机、大数据分析、可穿戴设备、智能能源和智能城市，使得个人和群体更容易落入政府对本国企业的监控以及外国情报机构和企业的监控范围。

33. 国家以这种方式使用新技术的潜在可能性，对隐私和言论自由、结社自由以及宗教或信仰自由等其他人权构成重大风险。这些技术的离散和累积效应，使国家有能力以新的方式和前所未有的程度严密勾画和监测个人的行为。

⁷ 欧洲议会以及欧盟理事会 2016 年 4 月 27 日(EU)第 2016/679 号条例。

⁸ 欧洲议会以及欧盟理事会 2016 年 4 月 27 日(EU)第 2016/680 号指令。

⁹ 欧洲联盟不具备国家安全领域的权限，因此不能充分将隐私保护延伸到这个领域，包括监督为国家安全目的进行的情报活动。

¹⁰ 《欧洲委员会在个人数据的自动化处理方面保护个人的公约》。

34. 这些技术可能被用以破坏人权和民主。民主或许是一个不完善的机制，但从历史上看，它为培育人权提供了最好的生态系统。因此，对民主的影响是评估侵犯隐私措施的一个关键基础指标。

35. 特别报告员将继续与所有会员国合作执行其全球任务，尽管他意识到，在享有坚实民主体制和保障的国家，他的合作更有可能取得成功，而归根结底对隐私权的尊重也更有可能会取得成功。

36. 2018 年全年，一个关键的关切问题是，一个国家的情报部门或执法机构与另一个国家的情报部门或执法机构共享包含个人数据的情报分析，会发生什么情况。接收国对数据——进而对所涉个人隐私——是否会以与发送国相同的标准加以保护？这一点的重要性值得我们采取所建议的行动。

37. 2018 年 11 月 14 日，比利时、丹麦、荷兰、挪威和瑞士的 5 个监督机构发表了一份联合声明——这些国家都是《第 108 号公约》的缔约国，因此都受到关于对为国家安全目的使用个人数据施加限制的《公约》条款的约束，声明涉及在监督情报和安全部门的国际数据交换时，可能存在的监督空白以及应对这一风险的方法。¹¹ 这是引起国际社会注意的一个重要和受欢迎的事态发展。

38. 2018 年国际情报监督论坛的与会者认为，这一举措是澳大利亚、加拿大、新西兰、联合王国和美国五眼联盟内负责情报监督的机构建立五眼情报监督和审查理事会的一个重要平行发展。特别报告员欢迎理事会的设立和活动，特别是考虑到组成联盟的 5 个国家的地理位置和全球影响力。自 2013 年以来，这些国家都进行了立法改革，以加强与国家安全和相关部门情报活动相关的监督和隐私保障。其中一些国家的改革比另一些国家更加全面；例如，任务负责人从隐私保护的角度认为澳大利亚的最新立法是一个令人关切的因素。¹²

39. 联合王国调查权力专员办公室发表声明¹³，欢迎比利时、丹麦、荷兰、挪威和瑞士监督机构的声明。该办公室有潜力——乃至可能负有其所处地理位置决定的内在特殊责任，在欧洲大陆监督机构和与上述理事会合作的机构之间架起一座桥梁。

40. 特别报告员将促进和支持这一举措和其他举措，只要这些举措最终能够吸收与一国情报机构和执法机构与另一国情报机构和执法机构之间交换个人信息有关的国际人权标准和保障措施。

41. 对情报活动的监督是特别报告员在欧洲数据保护委员会审议日本国家法律和保障措施是否充分的过程中所做贡献的主要焦点。辩论中讨论了特别报告员提交的材料和证据，导致 2018 年 12 月 5 日决定暂不接受¹⁴ 关于日本措施充分性的调查结果。

¹¹ 见 <https://english.ctivd.nl/documents/publications/2018/11/14/index>。

¹² 特别报告员提交澳大利亚议会情报和安全联合委员会的材料，2018 年第 81 号。可查阅：www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/TelcoAmendmentBill2018/Report_1/section?id=committees%2freportjnt%2f024247%2f26914。

¹³ 见 www.ipco.org.uk/docs/IPCO%20Statement%20re%205%20oversight%20bodies.docx。

¹⁴ 见 https://edpb.europa.eu/news/news_en。

42. 2018 年 9 月，欧洲人权法院认定，联合王国批量截收制度违反《欧洲人权公约》第 8 条(尊重私人 and 家庭生活/通信的权利)，原因是对选择截收互联网载体以及过滤、搜索和为审查目的的选择被截收通信的监督不足，以及对选择“相关通信数据”进行审查的保障措施不足：¹⁵

(a) 该法院认为，从通信服务提供商获取通信数据的制度违反《公约》第 8 条；从通信服务提供商批量截收和获取通信数据的制度违反《公约》第 10 条，因为对机密新闻材料的保障措施不足；

(b) 法院还认为，与外国政府分享情报的制度既不违反第 8 条也不违反第 10 条。

43. 虽然这一判决涉及的是先前的联合王国法定监督框架，但其调查结果非常重要，已提请会员国注意，以审查各自做法和框架。

44. 这一动态凸显了详细有效的法律和程序保障在国家法律和情报机构及其监督机构的实践中的重要性。

45. 特别报告员在 2018 年 11 月对德国进行正式访问期间，讨论了行使批量监控权力的良好做法，建议各国考虑新责任基金会(Stiftung Neue Verantwortung)编制的一份此类良好做法的相关汇编¹⁶ (2018 年 11 月)。

建议

46. 特别报告员建议：

(a) 会员国将《第 108+号公约》第 11 条规定的保护基本隐私权的标准和保障措施纳入各自国家法律体系，特别是：

(一) 确保任何和所有侵犯隐私的措施，即使是为国家安全、国防和公共安全，以及预防、调查和起诉犯罪等目的采取的措施，一律在经过适当的公众协商和议会审查制订的法律中加以规定，由此创造法律的确定性；

(二) 确立“民主社会中必要和相称的措施”的判据，作为情报和执法机构内部合规单位必须适用于任何侵犯隐私措施的关键衡量标准，并由相关管辖范围内的独立监督机关和法院对照这个标准衡量这些机构的行动并对这些机构进行问责；

(三) 建立一个或多个由法律授权并由国家提供充足资源的独立监督机关，以便对情报机构和执法机构从事的任何侵犯隐私的活动进行有效审查；

(b) 对于情报部门和执法机构之间在国内和跨界交换的任何个人信息，采用“可交换即可监督”原则¹⁷：

¹⁵ European Court of Human Rights, First Section, *Big Brother Watch and Others v. the United Kingdom*, application Nos. 58170/13, 62322/14 and 24960/15, judgment of 13 September 2018.

¹⁶ 见 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex5_CompendiumBulkSurveillance.pdf.

(一) 所有会员国都应修订自己的法律，具体而明确地为负责监督情报活动的独立机关授权，监督其责任范围内国家情报机构之间交换的所有个人信息；

(二) 在可能和适当的情况下，发送国和接收国的独立监督机关应能立即自动获取各自国家情报部门和/或执法机构之间交换的个人数据；

(三) 所有会员国都应修订自己立法，为国家和政府情报监督机关具体授予法律权力，以便与个人数据被相关情报机构传送或以其他方式交流的国家的监督机关分享信息、进行协商和讨论最佳监督做法；

(四) 当情报机构将载有从另一国收到的个人信息或其他形式的个人数据的情报分析传送给第三国或国家集团时，这种传送应受这些国家情报监督机关的审查。

47. 在考虑使用批量监控权力时，除了适用欧洲人权法院在 2018 年 9 月 *Big Brother Watch* 等(诉联合王国)案中所采用的部署标准和保障措施之外，会员国主管机关还应首先研究、然后优先考虑并尽最大可能采取措施，引入新责任基金会(Stiftung Neue Verantwortung)汇编¹⁸中建议的良好做法。

四. 隐私权：性别视角

48. 人权理事会第 34/7 号决议和大会第 71/199 号决议呼吁各国“在这方面针对在数字时代侵犯和践踏隐私权的行为进一步制定或维持预防和补救措施，这些行为可能影响到所有人，包括对妇女以及儿童和处于弱势和边缘境地的人产生特别影响。”

49. 1994 年，人权事务委员会在 *Toonen* 诉澳大利亚一案中裁定将成年人之间自愿的同性关系定为犯罪属侵犯隐私权。2017 年，委员会重申，隐私权涵盖性别认同(CCPR/C/119/D/2172/2012, 第 7.2 段)。

50. 隐私权虽然不是一项绝对权利，但对个人人格和身份的自由发展至关重要。这是一项既源于、又影响人的与生俱来尊严的权利，有助于行使和享有其他人权。¹⁹ 这是一项不仅限于公共领域的权利。

¹⁷ 设在不同国家的情报机构之间定期交换个人数据，但不一定受到设在发送国或接收国的独立监督机关的监督。此外，某些立法实际上不允许发送国或接收国独立监督机关之间对这个事项的这种监督甚至协商。鼓励各国修订法律，授权本国独立监督机关与其他国家的其他独立监督机关协商，并跟踪与另一国的所有数据交换，无论这些数据是在接收国还是发送国，包括原始未处理的个人数据或情报产品特定分析所载个人数据。情报机构和执法机构都在交换这两种个人数据，两者都应置于发送国和接收国的独立监督之下。

¹⁸ Thorsten Wetzling and Kilian Vieth, *Upping the Ante on Bulk Surveillance: An International Compendium of Good Legal Safeguards and Oversight Innovations*, Publication Series on Democracy, vol. 50 (Berlin, Heinrich Böll Stiftung, 2018).

¹⁹ 大会、联合国人权事务高级专员和特别程序任务负责人承认隐私是享有其他权利的一个途径，见大会第 68/167 号决议、A/HRC/13/37 和人权理事会第 20/8 号决议。

51. 隐私权是保护基本价值观(包括自由、尊严、平等和不受政府干预)的必要先决条件，是民主社会的一个重要组成部分，需要强有力的保护。²⁰ 人权理事会通过了一些决议，强调民主和人权之间相互依存和相辅相成的关系。²¹

52. 特别报告员在整个任务中纳入了性别视角。²² 继三次成功的“隐私、个性和信息流动”问题区域协商后，开展了一次题为“数字时代出现的性别问题及其对不同性取向、性别认同、性别表达和性别特征的妇女、男子和个人的影响”的在线协商。

53. 隐私与人格专题行动系列的第一份完整报告是特别报告员收到的提交材料汇编²³ 以及辅助研究的一部分。除建议外，汇编不一定代表其主要作者——隐私与人格问题工作队主席 Elizabeth Coombs——的观点，也不代表特别报告员的观点。

隐私与人格专题行动系列

54. 特别报告员收到的关于这一议题的材料主张对经济力量、阶级、宗教、种族和性别进行跨部门分析，以确定主流以外的兴趣领域²⁴，并认识隐私权与民主之间的相互依存关系。²⁵

55. 据报告，个人对数字技术和隐私的体验受到性别以及种族、文化、种族、年龄、社会出身、财富、经济自足、教育以及法律和政治框架等因素的影响。²⁶ 有人认为，隐私权对于因性别、性取向、性别认同、性别特征或表达方式而面临不平等、歧视或边缘化的人尤为重要。互联网以其覆盖面和相对匿名性，为男女同性恋、双性恋、变性人、“酷儿”和与双性人(LGBTQI)的互动和相互支持开辟了新的途径。

56. 在提交的材料中，人们认识到数字技术通过扩大非数字世界的体验而对隐私产生相当大的影响。据报告，由于结构不平等和歧视性的性别规范，数字技术的好处在途径上不平等，这些规范沉重压迫妇女、非二元性别和顺性别规范的个人、穷人和少数宗教或文化群体。网络厌女态度²⁷ 和对非二元性别个人的普遍

²⁰ Daniel Therrien, Canadian Privacy Commissioner, Submission to Innovation, Science and Economic Development Canada's national digital and data consultations, 23 November 2018.

²¹ 关于人权、民主和法治的第 19/36 号和第 28/14 号决议。

²² 见 www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx。

²³ 见 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex2_GenderReport.pdf。

²⁴ 例如，进步通讯协会提交的材料，2018 年。

²⁵ 例如，加拿大隐私专员的材料，2018 年。

²⁶ Phoenix Strategic Perspectives, “2016 survey of Canadians on privacy”, final report prepared for the Office of the Privacy Commissioner of Canada, December 2016.

²⁷ West Coast Women's Legal Education and Action Fund (LEAF), *#CyberMisogyny: Using and Strengthening Canadian Legal Responses to Gendered Hate and Harassment Online* (Vancouver, 2014).

网络霸凌是由新技术促成的²⁸，与以前相比，这些新技术具有无限大的接触面、耐久性和影响力。

57. 提交材料中有一种强烈意见认为，这种情况并不是必定的，数字技术可以在享有隐私权方面提供平等。

58. 提交的材料承认智能设备、应用程序、搜索引擎和社交媒体平台的好处，但它们也有可能侵犯用户的性别隐私。例如，LGBTQI 青年比非 LGBTQI 青年更频繁地使用互联网参与社交媒体和互联，比非 LGBTQI 青年更有可能在网上受到欺凌或骚扰(42%比 15%)。²⁹

59. 尽管数字技术带来了好处，³⁰ 但据认为风险最大的是妇女、女孩、儿童和 LGBTQI 个人和群体³¹，特别是变性人、活动人士、同性恋教师、人权维护者、性工作者和女记者。

60. LGBTQI 个人也可能经历特定风险，如“出柜”和与其性别认同直接相关的虐待。³²

61. 加拿大发现，社交媒体在为妇女和女孩提供社交联系的同时，也会放大社会规范的影响，其途径包括商业性监控的强化、现有社会规范的加强以及家庭成员和同龄人监控的增加等。³³

62. 据报道，LGBTI 约会应用程序和其他社交媒体平台上的虚假账户被国家行为者和非国家行为者用于锁定男同性恋者，逮捕他们或使他们面临残忍和有辱人格的待遇，甚至进行勒索。³⁴

63. 据报道，有包括新媒体在内的媒体公布 LGBTQI 人士及人权维护者的个人信息，危及他们的安全。³⁵

²⁸ Eastern European Coalition for LGBT+ Equality submission, “Gender perspectives on privacy in Eastern partnership countries and Russia”, 2018; 另见 www.ucl.ac.uk/steapp/research/themes/digital-policy-laboratory/gender-and-iot。

²⁹ David Brian Holt, “LGBTIQ teens - plugged in and unfiltered: how Internet filtering impairs construction of online communities, identity formation, and access to health information”, 2009.

³⁰ 提交材料(此处隐去姓名)，2018 年，引述 Valerie Horres, “Online and enabled: ways the Internet benefits and empowers women”, *Interface: The Journal of Education, Community and Values*, vol. 10, No. 4 (2010)。

³¹ 2018 年提交材料：哈萨克斯坦女权主义倡议“Feminita”；维权与交叉影响问题办公室；“Stimul” LGBT 群体和变性人法律维护项目(俄罗斯)；Richard Lusimbo；MPact 同性恋男子健康和人权全球行动；欧洲变性人协会；荷兰同性恋者融入社会联合会；以及国际女同性恋、男同性恋、双性恋、变性人和双性人协会。

³² 东欧争取 LGBT+平等联盟提交的“东欧伙伴国家和俄罗斯隐私权问题上的性别视角”。

³³ Valerie Steeves, and Jane Bailey, “Living in the mirror: understanding young women’s experiences with online social networking”, in Emily van de Muelen and Robert Heynen, eds., *Expanding the Gaze: Gender and the Politics of Surveillance* (Toronto, University of Toronto Press, 2016). See also <https://egirlsproject.ca/> and www.equalityproject.ca/。

³⁴ 哈萨克斯坦女权主义倡议“Feminita”，2018 年提交材料。

³⁵ 同上。

64. 互联网不仅创造当代的“故事”，还可以永远延续数字时代之前的“故事”以及与之相关的对隐私的侵犯。³⁶

65. 一些材料谈到对性别认同、自主性和身体完整性的承认及其表达，并对身份证件中姓名和性别变更背景下隐私管理不足表示关切。³⁷ 需要身份证件的普通日常活动，如旅行、银行、医疗预约，经常给变性人带来非常尴尬和苦恼的隐私侵犯，而这种侵犯是只认同性别二元的人没有经历过的。

66. 欧洲人权法院认定，有关国家违反了《欧洲人权公约》第 8 条，因其性别承认程序侵犯变性人的隐私权。³⁸

67. 关于性别认同的公共记录、司法通知和决定的在线可获得性是一个隐私问题，尤其是与大数据和搜索引擎能力相结合。³⁹

68. 对于双性人来说，隐私侵犯直接就是从出生开始，通过变性手术和激素治疗指定特定的性别。对双性婴儿做“正常化”手术会影响人权，包括隐私权，因为这种做法侵犯与医疗有关的个人自主权/自决权。据报道，各国的回应方式各不相同。⁴⁰

69. 提交的材料，包括暴力侵害妇女问题特别报告员提交的材料，提到有关基于性别的数字暴力的国际、区域和国家研究正在不断增多。

70. 数字技术和智能设备为骚扰和控制他人提供了几乎无限的途径。⁴¹ 技术为暴力提供便利问题与性别不平等、性暴力、互联网监管、互联网匿名和隐私等问题交织在一起(见 A/HRC/38/47)。

71. 基于图像的虐待或“报复色情”现象——为伤害对方不经同意公开个人私密性图像和录音——被广泛认为是一种在线虐待形式。澳大利亚的研究发现，男性和女性同样可能遭受基于形象的虐待，而被认定为女同性恋、男同性恋或双性恋的人(36%)比异性恋(21%)更有可能成为受害者。⁴²

72. 家庭暴力越来越多地涉及针对妇女和受抚养人使用智能家庭设备，⁴³ 这就提供了使侵犯隐私、减少家庭⁴⁴ 或通信⁴⁵ 中的自主和自决成为可能的途径。有时法律保护不足⁴⁶，或者警察缺乏对侵权行为的执法。⁴⁷

³⁶ 奥斯古德法学院，机密材料，2018 年 12 月。

³⁷ 东欧争取 LGBT+平等联盟提交的材料，2018 年。

³⁸ 欧洲人权法院，第二庭，L.诉立陶宛，申诉编号 27527/03，2008 年 3 月 31 日最后判决；欧洲人权法院，第五分庭，A.P.、Garçon 和 Nicot 诉法国，申诉编号 79885/12、52471/13 和 52596/13，2017 年 4 月 6 日判决。

³⁹ 哈萨克斯坦女权主义倡议“Feminita”，2018 年提交材料。

⁴⁰ Susan Miller, “California becomes first state to condemn intersex surgeries on children”, *USA Today*, 28 August 2018.

⁴¹ 权利、司法和社会研究中心提交的材料，2018 年 9 月。

⁴² Nicola Henry, Anastasia Powell and Asher Flynn, “Not just ‘revenge pornography’: Australians’ experiences of image-based abuse”, May 2017.

⁴³ Makda Ghebreslassie, “Stalked within your own home”: woman says abusive ex used smart home technology against her”, *CBC News*, 1 November 2018; Nellie Bowles “Thermostats, locks and lights: digital tools of domestic abuse”, *New York Times*, 23 June 2018.

73. 网络厌女态度已经在数字平台上显现出来。⁴⁸ 据报道，推特是推动针对妇女的仇恨运动和传播性内容的主要平台，而脸书上可以看到对维权妇女的最多攻击。⁴⁹

74. 不符合常规传统男性形象的男子以及男女同性恋或双性恋者面临隐私侵犯和网络暴力的比例较高。⁵⁰

75. 不同性别的隐私体验也影响其他权利的享有，例如，在针对女性活动人士和记者的运动中，存在着对妇女的在线压制和性别划线。⁵¹

隐私与人格专题行动系列

76. 监控，除非是合法、相称和必要的，否则就是对隐私权的侵犯。性别、种族、阶级、社会出身、宗教、意见及其表达都可以成为决定谁在社会上被监控的因素，并使某些个人的隐私权更有可能受到侵犯。⁵²

77. 在一些国家，被认定是 LGBTQI 群体成员的人受到较高级别的监控，性别偏向显而易见。⁵³ 一些国家通过立法为国家监控 LGBTQI 群体提供便利。2018 年埃及颁布的《反网络犯罪法》就是一例。⁵⁴

78. 虽然国家监控通常被说成是针对男性的，⁵⁵ 但也有人提到，反恐措施对妇女和变性寻求庇护者、难民和移民的影响大得不成比例。⁵⁶

79. 妇女可以预料，她们私密生活的几乎每一个细节都可能受到国家行为者和私人行为者的多种形式的监控，从家庭暴力到性对象化和生育都是如此。⁵⁷

⁴⁴ Bowles, “Thermostats, locks and lights”.

⁴⁵ Corinne Lysandra Mason and Shoshana Magnet, “Surveillance studies and violence against women”, *Surveillance and Society*, vol. 10, No. 2 (2012); Association for Progressive Communications submission.

⁴⁶ Bowles, “Thermostats, locks and lights”.

⁴⁷ Al-Alosi Hadeel, “Cyber-violence: digital abuse in the context of domestic violence”, *University of South Wales Law Journal*, vol. 40, No. 4 (2017).

⁴⁸ West Coast LEAF, #CyberMisogyny.

⁴⁹ 墨西哥城妇女协会和进步通讯协会提交的材料，2018 年。

⁵⁰ 爱尔兰公民自由理事会。

⁵¹ 权利、司法和社会研究中心提交的材料，2018 年。

⁵² Mary Anne Franks, “Democratic surveillance”, *Harvard Journal of Law and Technology*, vol. 30, No. 2 (Spring 2017).

⁵³ 进步通讯协会提交的材料，2018 年。

⁵⁴ 国际联合提交的材料，2018 年；另见 George Sadek, “Egypt: President ratifies Anti-Cybercrime Law”, *Global Legal Monitor*, 2018 年 10 月 5 日。

⁵⁵ 隐私国际 2017。

⁵⁶ 在打击恐怖主义的同时促进和保护人权及基本自由问题特别报告员的报告(A/64/211)。

⁵⁷ Franks, “Democratic surveillance”; Association for Progressive Communications submission, 2018.

80. 各大平台提供商现在通过在线身份认证提供身份管理。网站、应用程序和服务现在要求通过登陆脸书或谷歌账户后登录详细信息，并接受身份凭证为真实身份。⁵⁸ 脸书拥有这一“社交登录”市场的 60%，⁵⁹ 以此为途径可以获取大量信息用于编辑个人资料，其中性别是一个变量，因而从中能够洞察个人、家庭、群体和社区的行为。

大数据与开放数据专题行动系列

81. 数据收集、存储和操纵的增长增加了侵犯隐私的可能性，这可能会因性别而产生不同的后果。

82. 数据处理可能会嵌入与性别角色和身份有关的偏向，特别是因为社会干预的数据建模越来越超越个人，将重点放在群体或社区上。⁶⁰

83. 数据分析导致根据性别对个人或群体进行推断并导致歧视，违反人权法。

健康数据专题行动系列

84. LGBTQI 人群的一个特别关切是未经同意的健康数据共享，特别是艾滋病毒状况。⁶¹ 例如，应用程序 Grindr 被发现包含跟踪功能，并与各种第三方共享个人信息，包括用户的艾滋病毒状况。⁶²

85. 保健环境中的隐私体验据认为会影响保健服务的使用，从而对个人和公共健康产生影响。

86. 担心因失去隐私而受到羞辱或歧视，会导致变性人回避或限制使用医疗服务。⁶³

87. 在分娩过程中侵犯妇女隐私权可能造成很大影响，以至于不愿意再为以后分娩寻求护理。⁶⁴

88. 谷歌街景等技术会影响女性对医疗服务的使用，因为她们担心自己使用某些医疗服务的情况会被发现。⁶⁵

⁵⁸ “The Economist essay”, *The Economist*, Christmas ed., 22 December 2018.

⁵⁹ 同上。

⁶⁰ Khiara M. Bridges, *The Poverty of Privacy Rights* (Stanford University Press, 2017); David Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk and Digital Discrimination* (London and New York, Routledge, 2003).

⁶¹ 哈萨克斯坦女权主义倡议“Feminita”提交的材料，2018 年。

⁶² 进步通讯协会提交的材料，2018 年。

⁶³ “New health care clinic for transgender people in pipeline”, *Times of Malta*, 7 April 2018.

⁶⁴ White Ribbon Alliance for Safe Motherhood, “Respectful maternity care: the Universal Rights of Childbearing Women Charter”, 2011; and Meghan A. Bohren and others, “The mistreatment of women during childbirth in health facilities globally: a mixed-methods systematic review”, *PLOS Medicine*, vol. 12, No. 6 (2015). 权利、司法和社会研究中心和进步通讯协会提交的材料。

⁶⁵ Melissa L. Davey, “Protect us from anti-abortion protesters, say women’s clinics in WA”, *Guardian*, 25 January 2018.

公司使用个人数据专题行动系列

89. 正如人权与跨国公司和其他工商企业问题秘书长特别代表约翰·鲁格 2008 年提出的保护、尊重和补救框架(A/HRC/8/5)所示,人们越来越认识到私营部门在人权法之下负有义务。⁶⁶

90. 数字平台使用的自动化决策可以产生对性别有不同影响的结果。据报道,针对脸书的法律诉讼仍在进行中,这一起诉讼涉及脸书据称允许房东和经纪人依据用户性别决定排除广告显示。⁶⁷

91. 宣传暴力侵害妇女行为、性别歧视和有害性别成见的社交媒体网页和群组数量不断增多,而需要很大的群体压力才能让有关方面删除这些网页,对此有人表示关切。

92. 以下情况据报尚不清楚:在线平台收到在线暴力投诉后如何做出决定、按国家分列的所报案件类型和数量,以及采取过哪些行动。大赦国际发现推特未能充分调查暴力和虐待的报道,并一再呼吁该公司发布“有意义的信息,说明该平台上所举报的针对妇女和其他群体的暴力和虐待以及该公司如何应对”。⁶⁸

93. 一份提交的材料报告说,应用程序 Grindr 采取了积极行动,减少旨在锁定同性恋男子的不当使用。⁶⁹然而,数字平台(脸书、推特、媒体等)在应对网上性别暴力受害者方面据报往往不闻不问和含糊其辞,受害者普遍感到求助无门。⁷⁰

94. 关于基于性别的技术侵犯隐私权对个人造成伤害的报告包括:各种严重的、有据可查的影响,源于遭受欺诈、丧失就业和受教育机会、限制行动自由和结社自由以及根据自己的意愿穿着打扮的自由、干涉养育子女的能力、丧失名誉和一般信任、暴力(甚至死亡)和监禁等。⁷¹

95. 隐私被侵犯的经历并不一律相同;侵犯隐私可能是导致妇女遭受更多的家庭暴力,也可能是导致 LGBTIQ 人士受到更多歧视。⁷²

96. 侵犯隐私既是对人类人格本身的侵犯,也具有广义的社会影响。著名女性在网上遭受的各种极端形式的侮辱以及她们个人和家庭隐私的被侵犯,有碍于女孩

⁶⁶ Internet Rights and Principles Coalition, “The Charter of Human Rights and Principles for the Internet”, 2014; 进步通讯协会提交的材料, 2018 年。

⁶⁷ 消费者政策研究中心提交的材料, 其中引述题为 “Money” 的文章, CNN News, 2018 年 3 月。

⁶⁸ 见 <https://decoders.amnesty.org/projects/troll-patrol/findings>。

⁶⁹ 哈萨克斯坦女权主义倡议 “Feminita”, 2018 年提交材料。

⁷⁰ 权利、司法和社会研究中心 2018 年提交的材料中指的是电子媒体。

⁷¹ 内部通讯协会提交的材料, 2018 年; N. Pushkarna 和 M.M. Ren, 2018 年提交的材料; 加拿大隐私问题专员办公室, “Online reputation: what are they saying about me?”, 2016 年 1 月; 提交欧洲变性人协会的案例; 欧洲联盟基本权利增进署, *Violence against Women: an EU-Wide Survey – Main Results* (卢森堡, 欧洲联盟基本权利增进署出版物, 2015 年)。

⁷² 男女同性恋和异性恋教育网络, *Out Online: The Experiences of Lesbian, Gay, Bisexual and Transgender Youth on the Internet* (New York, 2013), 国际联合提交材料, 2018 年。

和妇女参与承担公共角色，从而损害妇女参与公共事务的权利，并影响民主机构的代表性。⁷³

97. 提交的材料表明了从性别视角保护隐私的良好做法，包括立法改革、不分性别的循证政策框架、法院判决、民间社会组织的参与并受益于它们的经验，以及性别化隐私社区方案，此外还有教育资源等。

98. 处理性取向和性别认同隐私问题的良好做法被视为已载入补充《日惹原则》的《关于将国际人权法应用于性倾向、性别认同、性别表达和性别特征相关事务的补充原则和国家义务》。⁷⁴

五. 结论

99. 《世界人权宣言》呼吁每个个人和社会机构促进和尊重人权。⁷⁵ 国家、公司、宗教团体、民间社会、专业组织和个人都应发挥重要作用。

100. 个人分享思想和集会的信心也是社会健康和民主的基础。隐私的丧失可能导致这种信心的丧失，包括对代表公共利益而建立的政府和机构的信心，并导致他们退出参与，从而可能对代议制民主产生不利影响和破坏。

101. 虽然隐私权并非没有代价，对政府而言也不是没有风险，但我们在民主制度中的集体利益压倒了这些挑战。出于以上所述和提交材料中报告的所有原因，妇女的隐私权以及儿童和不同性取向、性别认同、性别表达和性别特征的个人的隐私权至关重要。⁷⁶

102. 基于性别的侵犯隐私是剥夺人权的一种系统性形式；这种侵犯在性质上是歧视的，而且往往会固化不平等的社会、经济、文化和政治结构。

103. 处理基于性别的侵犯隐私问题要求在国际、区域和国家各级建立框架。

104. 国家在防止基于性别的隐私侵犯方面，需要在政策制订、立法改革、服务提供、监管行动、支持民间社会组织以及教育和就业框架中积极保护隐私，利用妇女、男子、变性妇女和男子以及两性人和其他认为自己不属于二元性别和顺性别规范的人的经验。

105. 对于非《通用数据保护条例》缔约方的国家而言，保护在线个人信息应是一个优先事项，应采用等同于或优于该条例的规定。性别应该是制订和执行隐私保护框架的一个关键考虑因素。

⁷³ 澳大利亚妇女反暴力联盟提交的材料，2018 年。

⁷⁴ 民间社会组织联合提交的材料，2018 年；Peter Micek and Denis Nolasco, “The gender of surveillance: how the world can work together for a safer Internet”, Access Now, blog, 6 February 2018。

⁷⁵ 大会第 217A(III)号决议，序言部分。

⁷⁶ 联合国人权事务高级专员办事处，《生而自由平等：国际人权法中的性取向与性别认同》(纽约和日内瓦，2012 年)。

106. 私营公司使用用户个人数据⁷⁷和回应网上骚扰报告的方式需要透明。影响在线体验的人具有更多的性别差异，对于提高产品和平台安全度、加强社会责任感和强化问责非常重要。

六. 建议归纳

107. 关于联合国机构，人权理事会和人权条约机构的所有相关特别程序和其他机制应当将性别和隐私纳入各自任务的执行。

108. 建议会员国：

(a) 采取跨部门方针，承认不同性别的隐私权的具体利益、经验和威胁，以及压倒一切的隐私与人权原则；

(b) 对照全球、区域和国家各级的相关法律和条约，评估本国防止和惩处基于性别的侵犯隐私行为的法律框架；

(c) 采取政策、法律和监管框架，为安全数字通信的使用和发展提供全面保护；

(d) 促进有意义的互联网接入，弥合任何数字性别鸿沟；

(e) 采取一切必要的立法、行政和其他措施，防止、调查和惩罚基于性别、性取向或性别认同的侵犯隐私行为。

109. 公司应执行《工商业与人权：实施联合国“保护、尊重和补救”框架指导原则》，并避免侵犯所有受其做法影响的人的人权，同时切实考虑其活动的性别影响。

七. 健康数据保护

110. 健康是每个人生活的最重要基础。健康状况的改变总是意味着生活的改变，很多是永远改变。在生活的某个时刻，我们都会是病人。我们的健康状况对生活有决定性影响的情况也会出现。因此，在与健康数据相关的情况下，通过现有最高标准保护我们的尊严和自主权，是我们所有人的正当利益之所在。

111. 作为数据主体的患者与卫生专业人员之间的关系非常敏感：患者自然处于弱势地位。情况可能是痛苦和危险的，并会带来终身后果。卫生专业人员要发挥自己的作用，要求具备准确完整的患者信息以及以标准化和透明方式使用这些信息的程序。

112. 几千年来，在病人(及其遗传上的亲属)处于根本性脆弱状况的时刻，对他们的保护都有法律和伦理方面的考虑和规则。医疗专业保密、对治疗确立完全知情同意的义务、妥当的治疗记录和自由选择治疗医生等原则，是千百年以来对如何最好保护患者权利进行思考的基本成果之一。

⁷⁷ Australian Competition and Consumer Commission, *Digital Platforms Inquiry: Preliminary Report* (Canberra, Australia, 2018).

113. 每种医疗状况都会产生个人数据。这些数据对于治疗目的很重要，需要按照最高的法律和道德标准进行处理。数字化正在产生越来越多的医疗数据，随着卫生专业人员变得越来越专门化，这些数据将越来越多地在他们之间共享，对此也同样需要按照最高质量标准进行协作。

114. 出于保健目的处理的数据之所以重要，还在于存在着许多其他利益攸关方，而且在卫生专业人员和患者之间可能改变生活的关系以外还存在着许多不同目的。首先，控制这些数据是患者本人的正当利益之所在，患者可以同意在治疗期间和治疗后共享这些数据。第二，其他利益攸关方，如患者的亲属、患者负有义务的机构(如社会保障机构、保险公司或雇主)以及其他较间接的利益攸关方，如依赖高效率 and 有效能的卫生系统的医学研究人员和公众，获取这些数据可能也是他们的利益之所在。

115. 这些不同利益攸关方的利益和需要之间的张力带来了极具挑战性的法律和道德问题。

紧要问题

知情同意

116. 一般而言，患者拥有在被正确告知可能的治疗风险、副作用和替代方案后对治疗表示同意的自由。医疗和医学研究同意程序的要求受到严格、详细和有争议的法规的约束。

117. 这些法规尚未与向数据主体提供信息的要求以及知情同意作为数据处理法律依据的有效性标准取得协调。知情同意的标准往往模糊和矛盾。

118. 当数据保护不是数据主体的当务之急时，各种不同的同意程序可能会让他们无所适从。他们也并非一律都想要和能够完全了解所给予的不同类型同意的全部影响。对化验、治疗、医学研究和数据处理的同意没有明确区分，这些同意通常涉及不同的、可能相互冲突的监管范围和不同的监管机构。这使患者和亲属面临严重压力，削弱了他们自由提供知情同意的能力。

医学研究需要的二次使用

119. 作为医疗的依据，需要收集和处理个人数据。然后，出于治疗记录的原因，要将数据储存起来，有时储存几十年。这些数据通常也可以是医学研究的重要来源。有些重要的论点认为，为了给后代患者带来更好的结果，进一步利用这些数据进行研究是有伦理依据的(甚至是必要的)。

120. 研究的目的不同于治疗，在处理数据方面要求有一个不同的法律依据。第二种法律依据的要求种类很多，而且不明确，因为许多潜在的伦理问题没有得到明确的描述或分析。具体而言，问题之一是，这种二次使用是否再次需要患者的知情同意和/或主管道德委员会和/或监管机构的批准。这些问题包括因身体隐私而产生的个人自主权以及对“集体利益”的责任。

121. 如果这种同意被另一种法律依据所取代，则需要采取进一步措施保护数据主体的基本权利。在这一问题上缺乏国际立法，导致治疗医生需要或认为自己需要来自受影响患者的额外知情同意，而这种同意在某些情况下出于技术或伦理原因无法再度获得。

其他目的需要的二次使用

122. 医疗数据对于其他目的也很有价值，特别是社会保障、公共卫生、就业和商业。国家法律通常对于用于这些目的的数据处理没有明确规定，不清楚这些目的在伦理和法律上是否有正当理据，以及这些二次使用中的哪一种应基于知情同意，还是应有另一种正当法律依据。因此，目的约束原则常常被忽视或违反，该原则要求个人数据二次使用的目的必须与原初目的相一致。

123. 在这一问题上的立法差异导致了一场“逐底”竞赛，即，依赖个人健康相关信息的公共服务乃至企业，竞相把业务放在数据保护低水平地区，以求最大利益。

124. 保护数据主体的权利——特别是包括信息和访问权在内的透明度权利——是一个难题，因为这些二次使用是由数据主体不认识的数据掌握者进行的，而且经常不说明目的。

作为与保护竞争的手段的数据产权

125. 上述情况的后果之一是，一些法律学者(甚至立法者)已经开始主张类似于知识产权的数据产权，认为这样当可缓解个人和非个人数据的共享问题。这些概念与数据保护的现有根本要求的关系很难理顺，需要根据对后果的循证预测进行明确的推理和论证。目前，缺乏一个基本的证据和事实矩阵。

责任分配不明确

126. 医疗和研究由监管机构监督，具体而言就是由专家和利益攸关方组成的道德委员会，其中许多人不是律师，没有数据保护方面的专门知识。

127. 然而，这些机构制订的关于治疗用和研究用数据处理的许多要求都与数据保护有关，例如同意程序的具体(而且往往相互冲突的)要求、向患者/数据主体提供的信息、患者的了解情况的权利和不愿了解情况的权利、撤销同意的后果等。

128. 这些机构提出的条例可能与数据保护规则相冲突，它们的监督可能会干扰专门负责监督数据保护合规情况的数据保护监督员和机构(如独立的数据保护官员和数据保护机构)进行的监督。

应用范围不明：个人数据、假名数据和匿名数据

129. 数据保护法仅对属于特定个人的个人数据适用，这一基本假设很难应用于医疗情景，因为医疗数据很少能完全匿名。例如，尚不清楚什么匿名措施“足够好”，可以将数据保留在数据保护立法的范围之外。

130. 当考虑要求向公众发布(非个人)数据的开放存取/开放数据计划中是否应该包括医疗数据时，这个问题尤其困难。数据掌握者一方面必须将数据置于自己的控制之下，以保护匿名性，但另一方面又必须使数据可以自由访问，从而面临数据身份被重新识别的风险。缺乏清晰度可能有助于数据掌握者对医疗数据进行事实上的财产保护，数据掌握者可以——事实上——决定谁以及在什么条件下获得数据访问权(通过某种方法匿名)。

131. 特别报告员在 2018 年提交大会的报告中明确指出,“除非有确凿证据表明已经进行了安全去识别化,并且能够强有力地防止未来重新被识别,否则不应在网上公布或交换个人的敏感高维单元记录级别数据。”

数据可携带性欠缺和数字化欠缺

132. 医疗数据往往仍以模拟格式收集。病历经常是随机的和不完整的,有些诊断可能依据的是缺陷数据。

133. 医疗数据的数字化、格式和过程的标准化以及数据质量的最低限度标准,可以帮助患者和卫生专业人员控制和负责任地管理健康数据。

134. 然而,有的国家建立自己的国家电子卫生系统往往没有公民和卫生专业人员参与,也没有标准化。这可能使患者无法携带数据,并在没有标准化装置的情况下降低他们控制医疗数据的能力,而标准化装置能够让他们根据自己的规则安全地存储和管理自己的健康数据。

云端

135. 越来越多的医疗信息(像任何其他数据一样)存储在“云端”。后果是多方面的,其中包括:个人数据的跨境传输可能与管辖权冲突、患者缺乏控制,以及发生可能影响数百万人的高影响安全事件。

136. 然而,对云服务提供商的最低限度要求尚不一致,这引发了在数据保护水平低的地区运营的动机。

生活方式产品/可穿戴设备

137. 健康相关数据往往不再(直接)与疾病相关,现在收集这些数据的目的是与治疗或预防疾病的目的大相径庭。具体而言,生活方式相关应用程序和新巧器具(“可穿戴设备”)不论有无数据主体知情同意都在收集大量与健康相关的数据。它们越来越普及,尽管没有明确界定收集的法律依据和进一步使用的要求,也没有适用最低限度透明度标准,而且目的约束原则也没有得到充分考虑。

安保与安全

138. 尽管健康相关数据高度敏感,并且健康数据处理设备故障可能会危及生命,但是没有关于最低限度安全标准的明确和具体的规则。后果就是一系列对所涉数据主体产生严重影响的安保和安全事件。

数据泄露通知,透明度欠缺

139. 尽管影响医疗数据的数据泄露经常发生,但没有标准可以决定何时及如何向相关数据主体和公众通报此类事件。这方面的情况缺乏透明度,没有达到公众期望的问责标准。

诉诸司法

140. 不遵守数据保护立法可能会对数据主体产生威胁生命的影响。然而,从一开始,数据保护立法就缺乏有效的执法手段。数据保护主管机关、法院、监察员、数据保护官员和医疗监督机关之间关于各自权限的规则不明确,信息和知识

分布不均，监管框架复杂，因而受影响的数据主体很难使自己的权利得到执法落实。

141. 这种执法欠缺导致对医疗系统缺乏信任，特别是对医患关系缺乏信任，这会对每个病人产生不利影响。因此，在联合国一级制订最低限度标准具有最大的战略重要性。

接续步骤

142. 特别报告员打算按照《世界人权宣言》第十二条和《公民权利和政治权利国际公约》第十七条的规定，为管理与健康有关的数据提供指导意见，以促进隐私权的保护和个人数据的保护。

143. 载有健康相关数据处理指导原则的指导意见草案⁷⁸ 涵盖上述问题，强调健康相关数据数据处理正当基础的重要性。该指导意见的目的是，第一，作为在国家一级实施的健康相关数据最低限度数据保护标准的共同国际基线，第二，作为一个参考点，以利目前正在进行的辩论，即讨论如何在医疗数据方面保护隐私权，而这种隐私权结合其他人权(如言论自由、公平审判权和财产保护)在全球处理和共享医疗数据的背景下得到进一步发展。

144. 工作队专家目前正在研究该指导意见草案，草案将于 2019 年 5 月 11 日前公开征求书面意见，随后将于 2019 年 6 月 11 日和 12 日在斯特拉斯堡举行一次公共利益攸关方会议。希望参加会议的会员国应在 5 月 11 日前登记参加的愿望。

145. 起草小组在吸收了利益攸关方的意见后提出的最后建议将提交给特别报告员，然后纳入他 2019 年底提交大会的 2019 年年度报告。

八. 隐私权指标

146. 特别报告员还在就“隐私指标”⁷⁹ 进行磋商。请个人、民间社会和政府于 2019 年 6 月 30 日之前提出意见和建议。这方面的意向是，把这些指标用作正式和非正式国别访问中的标准调查工具。

⁷⁸ 见 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex3_HealthData.pdf。

⁷⁹ 见 www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/2019_HRC_Annex4_Metrics_for_Privacy.pdf。