



大会

Distr.: General
17 October 2018
Chinese
Original: English

第七十三届会议

议程项目 74 (b)

增进和保护人权：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问题特别报告员约瑟夫·卡纳塔西依照人权理事会第 [28/16](#) 号决议编写并提交的报告。

* 本报告在截止期限之后提交是为了反映最新事态发展。



隐私权问题特别报告员的报告

摘要

本报告分为两部分：2017-2018 年期间开展的活动概要；特别报告员所设大数据和开放数据工作队的最后工作报告。

一. 隐私权问题特别报告员的活动概览

1. 2017 年 10 月至 2018 年 10 月这一期间对隐私权问题特别报告员来讲非常富有成效，其特点是与民间社会、各国政府、执法机构、情报部门、数据保护机构、情报监督机构、学术界、公司和其他利益攸关方进行了互动协作。

2. 2018 年 3 月，作为理事会 2015 年 3 月所定任务的首位负责人，特别报告员向人权理事会提交了他的第一个三年任期全面审查报告。¹ 他在该报告中说明了他在任务的每个专题领域开展的活动。特别报告员想表示，他的任期已延长到 2021 年，可继续开展这项任务的重要工作，这令他感到十分荣幸。

3. 特别报告员于 2018 年 4 月接受了外科手术，导致他的工作时间表被打乱。他感谢人权事务高级专员办事处(人权高专办)在此时期提供支持和协助。特别报告员已全面康复，于 2018 年 6 月继续履行职责。

A. 卫生数据隐私工作队的工作

4. 卫生数据隐私工作队在美利坚合众国得克萨斯大学戴尔医学院的 Steve Steffensen 领导下研究各种问题。虽然起草报告草案的工作已经启动，但意外事件导致计划于 2018 年进行的协商推迟到 2019 年。副主席 Nikolaus Forgo 已同意承担起主席的职责。

B. 公司对个人数据的使用问题工作队的工作

5. 由于安全、企业商业模式和隐私之间的矛盾仍然占据中心位置，隐私权现在比以往任何时候都更加处于政治、司法或个人意识的前沿。

6. 针对过去一年发生的事件，包括剑桥分析公司违反数据规定，出台立法，比如美国《澄清海外合法使用数据法》、澳大利亚 2018 年电信法案和其他立法修正案，以及美国最高法院审理的美国诉微软公司案，特别报告员提前启动公司对个人数据的使用问题工作队的工作。

7. 2018 年 9 月，该工作队首次在马耳他举行会议。其成员来自引领数字时代的大公司和在技术界促进保护隐私权的主要行动者。工作队将就在促进隐私权方面新出现的挑战和机遇，包括这些问题的性别影响，向特别报告员提供咨询意见。

¹ [A/HRC/37/62](#)。

C. 更好地理解隐私工作队的工作

8. 更好地理解隐私工作队探讨人权理事会承认隐私权推动个人发展的问题以及在推动个人发展方面遇到的障碍。它将与世界各地的举措合作，比如澳大利亚人权委员会审查数字时代对人权影响的举措。²

9. 虽然所有人都有权享有国际人权法规定的保护，但有报告指出，对隐私权的享有即不平等，也不普遍。性别问题是人们对隐私的保护和促进作用以及侵犯和破坏隐私的行为可能有不同体验的一个领域。

10. 在这方面，印度最高法院在一项承认印度男女同性恋、双性恋、跨性别者、性别奇异者和双性者群体权利的判决中，废除了《印度刑法典》第 377 条，该条将成人之间的自愿性活动定为刑事罪。这项判决将对印度的性别和隐私问题讨论产生重大影响，其依据是 2017 年在 *Puttaswamy* 案中对隐私权作出的判决。³

11. 特别报告员还发起了关于从性别观点来看待数字时代隐私权的在线协商活动，以征求对以下等问题的反馈意见：

(a) 数字时代出现哪些性别问题？有哪些挑战需要解决，有哪些积极的经验可以更广泛地推广？

(b) 数字时代是否对隐私有新的或显著不同的基于性别(包括性取向、性别认同、性别表现和性特征方面的经历)的体验？如果是，这些体验是什么？

(c) 隐私遭侵犯对男女两性以及具有各种各样的性取向和性别认同、性别表现和性特征的个人造成哪些基于性别的影响，包括健康问题、就业歧视或其他方面？

(d) 法律和服务提供模式中有哪些良好做法可消除在享有隐私权方面产生的基于性别的差异？

12. 要求在 2018 年 9 月 30 日前提交资料，以便于 2019 年向人权理事会提出报告。特别报告员也乐意在 2018 年 11 月 30 日前接受会员国迟交的资料。

13. 这一举措是在 2016 年 7 月、2017 年 5 月和 2017 年 9 月于世界各地举行的主题为“隐私、人格和信息流动”的协商活动后采取的。因特别报告员无法旅行，计划于 2018 年 5 月在拉丁美洲举行的第四次关于性别问题的活动推迟到 2019 年年中举行。

D. 安全和监视问题工作队的工作

14. 在爱德华·斯诺登揭露美国和大不列颠及北爱尔兰联合王国情报部门运作的监视和情报共享方案的细节后，就大量拦截通信、同外国政府共享情报以及根据联

² 澳大利亚人权委员会，“Major project to focus on human rights and technology, 2018 年 5 月 22 日。可查阅：www.humanrights.gov.au/news/stories/major-project-focus-human-rights-and-technology。

³ Smitha Krishna Prasad 的信函，印度新德里国立法律大学，2018 年 9 月 24 日。

合王国 2000 年《调查权力规管法》从通信服务提供商处获取通信数据的问题向欧洲人权法院提出了申请。

15. 欧洲人权法院最近认定，联合王国的大量拦截制度违反了《保护人权与基本自由公约》(《欧洲人权公约》)第 8 条(私人 and 家庭生活/通信受到尊重的权利)，理由是对选择因特网公司进行拦截的工作和对为审查而拦截的通信的过滤、搜索和选择，都没有进行充分监督，对选择“有关通信数据”进行审查，也没有采取充分保障措施。

16. 法院认定，从通信服务提供商处获取通信数据的制度违反了第 8 条；大量拦截的制度和从通信服务提供商处获取通信数据的制度均违反了《公约》第 10 条，理由是对机密新闻材料没有采取充分的保护措施。该法院还认定，同外国政府共享情报的制度没有违反第 8 条或第 10 条。⁴

17. 虽然该判决涉及联合王国先前监视方面的法律框架，但其裁决非常重要，已提请会员国注意审查其做法和框架。

18. 关于欧洲联盟法院 2016 年 12 月就保留通信数据问题作出的裁决和联合王国政府就拟议对策进行的协商，特别报告员在 2018 年初提供了投入，这一投入将可在人权高专办任务负责人专门网页上查阅。⁵

19. 2018 年 9 月，澳大利亚政府提出了电信和其他立法修正法案，该法案在国际和国内对人权和网络安全产生了深远影响。

20. 该法案存在致命缺陷。它是一个考虑不周全的国家安全措施，同样可能危及安全；该法案是否能实现其目标，并避免对所有设备的网络安全造成弱点，不论是手机、平板电脑、智能手表、汽车还是闭路电视网络，这在技术上有疑问的，而且，它还过度破坏人权，包括隐私权。虽然保证该法案不会为加密通信开“后门”，但这种保证并不可靠，因为它可能会实际造成有更多钥匙可以打开“前门”，甚至有更多前门。

21. 该法案在特别权力的使用方面赋予过高的酌处权。责任不在于议会，而是在于各机构和总检察长。该法案缺乏司法监督或独立监测，缺乏透明度的情况极其令人不安，除其他行动外，所建议在设备上安装软件的能力类似于政府实施黑客攻击，令人不安。该法案没有经过足够长的协商期就向议会提出，尽管据报告在协商结束后仅两周时间内就收到超过 14 000 份资料。⁶

⁴ 欧洲人权法院，First Section, *Big Brother Watch and Others v. the United Kingdom*, Applications Nos. 58170/13, 62322/14 and 24960/15, Information Note on Judgment of 13 September 2018. 可查阅 [https://hudoc.echr.coe.int/eng#{\"itemid\":\[\"002-12080\"\]}](https://hudoc.echr.coe.int/eng#{\)。

⁵ www.ohchr.org/EN/Issues/Privacy/SR/Pages/SRPrivacyIndex.aspx。

⁶ Justin Hendry, “Decryption laws enter parliament”, 《信息技术新闻》，2018 年 9 月 20 日。可查阅：www.itnews.com.au/news/decryption-laws-enter-parliament-512867?eid=1&edate=20180921&utm_source=20180921_AM&utm_medium=newsletter&utm_campaign=daily_newsletter。

22. 令特别报告员的关切加重的是，澳大利亚政府在针对严重侵犯隐私行为提供补救这一问题上的立场，以及澳大利亚对人权和隐私提供的有限保护——也就是说，宪法不保护隐私；没有珍视隐私的权利法案；没有规定侵犯隐私的行为；而且，与其邻国新西兰不同，澳大利亚的《隐私法》没有通过欧洲的适当性评估。

23. 必须采取一种新的办法来应对加密给执法和国家安全带来的挑战。虽然技术给执法和情报部门带来挑战，而且必须打击网上儿童性虐待和消除恐怖主义威胁，但在民主社会中，保护公民的人权也是合法和必要的。技术增强犯罪分子和恐怖分子逃避侦查或发起恶意攻击的能力，但也对网络安全、隐私和经济带来巨大好处。⁷ 削弱加密技术会使现代信息经济的安全面临风险。⁸

24. 要应对加密给执法调查和情报收集造成的困难，必须采取办法，避免削弱加密措施，由此避免削弱其他国家的国家安全。

25. 我向会员国推荐荷兰政府的做法，该国认识到，不能脱离国际背景来看待国家行动，并认识到缺乏削弱加密产品、同时又不影响使用加密技术的数字系统安全的备选办法。⁹

26. 特别报告员的国际情报监督论坛将于 2018 年 11 月底在马耳他举行会议。很多人对参加论坛感兴趣，以至于预订人数过多。

E. 来文

27. 2017 年 9 月 22 日以来，特别报告员提交了 17 份来文，包括 8 份“指控信”，7 份“其他信件”，2 份“紧急呼吁”。在 17 份来文中，15 份是与其他特别程序任务负责人共同提交的，2 份是特别报告员单独提交的。

F. 促进隐私权

28. 特别报告员通过发布联合新闻稿和声明以及交流意见和信息，与其他特别程序任务负责人合作。特别报告员感谢暴力侵害妇女及其原因和后果问题特别报告员与他进行建设性的协商。

⁷ James A. Lewis, Denise E. Zheng and William A. Carter, *The Effect of Encryption on Lawful Access to Communications and Data* (华盛顿特区，战略和国际研究中心，2017 年)。可查阅：https://csis-prod.s3.amazonaws.com/s3fs-public/publication/170221_Lewis_EncryptionsEffect_Web.pdf?HQT76OwM4itFrLEIok6kZajkd5a.rE。

⁸ 新美国，“Coalition raises serious concerns about Australian draft bill and encryption backdoors”，新闻稿，2018 年 9 月 10 日；Michelle Mosey and Adam Henschke，“Defining thresholds in law – sophisticated decryption and law enforcement”，国家安全学院备选政策文件，第 8 号(澳大利亚国立大学，2018 年 4 月)。

⁹ 荷兰安全与司法部长 G.A. Van der Steur 及经济事务部长 H.G.J. Kamp，“Cabinets view on encryption”，2016 年 1 月 4 日提交议会众议院议长的立场文件。

29. 特别报告员发布了 11 份新闻稿和声明。其中 2 份是与其他任务负责人联合发布的：一份涉及环保人士在即将举行的联合国气候变化框架公约缔约方大会第二十四届会议上的权利；¹⁰ 另一份涉及墨西哥安全法草案。¹¹

30. 2018 年 2 月 19 日和 20 日，人权高专办在日内瓦举办了关于数字时代隐私权的专家讲习班，在此期间，特别报告员介绍了隐私权在人权框架中的作用和对保护公民空间的作用，并主持了一场关于新的和正在出现的趋势的分会。

G. 国家访问

31. 2018 年 6 月，特别报告员访问了联合王国。特别报告员在访问结束时所作的声明中提供了初步意见。¹² 最后报告将提交人权理事会第四十届会议。

32. 2015 年，特别报告员严厉批评了加强联合王国政府监视权力的立法提案。自那时以来，情报监督制度取得了重大改进，包括建立了资源更充分的调查权力专员办公室和双锁制度，相当于由五名专职司法专员审查内政大臣和外交大臣等政府高级官员签署的最敏感的授权决定。积极的一面是，不受任意或非法监视的保障措施对联合王国当局在本国领土内监视的所有人平等适用，不根据国籍或住所加以任何区别。

33. 特别报告员仍然感到关切的是，2016 年新的《调查权力法》可能存在不足之处，包括要求调查权力专员办公室执行双重任务，即授权监视和监督这一监视工作。这可能会影响到事后监督的独立性。

34. 特别报告员确定，国家医疗服务体系的任何数据共享协议均需明确、有力的准则和监督，并强烈建议尽早公布这些准则。与国家数据保护组织的讨论表明，可能在今后 12 至 24 个月内公布准则。特别报告员建议尽早通过法律形式规定数据保护组织的作用。

35. 在访问结束时发表的声明中提到的其他问题包括反激进措施和“预防方案”及其对穆斯林的影响；将查阅极端主义材料定为刑事罪的建议；民间社会组织提出的问题。

计划进行的国家访问

36. 下一个正式访问的国家是德国，访问时间是 2018 年 10 月 29 日至 11 月 9 日，访问前将在人权高专办的有关任务负责人专门网页上呼吁有关方提供资料。

非正式访问和国际活动

37. 在前往澳大利亚参加关于大数据和开放数据的协商活动期间，特别报告员访问了三个州，会见了民间社会组织、一名政府部长和影子总检察长、政府官员、

¹⁰ 联合国人权事务高级专员办事处(人权高专办)，“联合国专家敦促波兰确保自由、充分参与气候会谈”，2018 年 5 月 7 日。可查阅：www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=23042&LangID=E。

¹¹ 人权高专办，“联合国权利专家警告说，墨西哥安全法草案威胁权利，应予以否决”，2017 年 12 月 14 日。可查阅：www.ohchr.org/en/NewsEvents/Pages/DisplayNews.aspx?NewsID=22535&LangID=E。

¹² 见 www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=23296&LangID=E。

公司、专业协会和学术界代表和其他人员。特别报告员还会晤了澳大利亚人权专员和委员会主席，并在以下大学发表了公开演讲：悉尼新南威尔士大学；墨尔本大学；乐卓博大学；埃迪斯科文大学。Optus Macquarie 大学网络安全中心举行了特别报告员与最大上市公司的简报会。国际隐私专业人员协会澳大利亚和新西兰分会与隐私从业者举行了会议。

38. 特别报告员还参加了下列会议：2017 年 11 月在捷克举行的第十六次国际网络空间会议；2018 年 1 月在布鲁塞尔举行的第十一次国际计算机、隐私和数据保护会议；2018 年 2 月在日内瓦举行的关于数字时代隐私权的专家讲习班；2018 年 2 月在渥太华举行的全球因特网和管辖权会议；2018 年 2 月在马耳他举行的隐私、财产和因特网治理替代管理方案会议。

H. 隐私权方面的动态

寻求补救的能力

39. 特别报告员继续提请相关会员国注意有关侵犯隐私权的指控，并在其 2018 年报告中就违反《世界人权宣言》第十二条和《公民权利和政治权利国际公约》第十七条的问题为人权理事会提供咨询意见。

40. 特别报告员仍然深信，要弥补侵犯隐私行为造成的损害，必须有信心获得公平的审理和可能的补救。获得补救的能力对保护人权至关重要，而且仍然是特别报告员的一个重要优先事项。

人工智能

41. 由于越来越多的影响所有人生活的决策是采用算法和机器学习作出的，必须不断认真评估它们对人权的影响。

42. 这些技术如此普遍，甚至在法庭诉讼中把它们作为证据信赖。但复杂算法运作的方式在很大程度上是未知的，它们在机器学习方面的逐步发展也同样是未知的。有必要在制订政策以鼓励和推动人工智能产品的发展和部署之前，或与此同时，从所有人权角度对此进行审查。¹³ 强有力的法律和道德框架对保护受影响的人权至关重要。

全球隐私和数据保护立法简介

43. 出台隐私法或数据保护法的国家数目已大幅增加；¹⁴ 在世界各地，2018 年是在这方面尤其活跃的一年。

¹³ Priyanar Bhunia, “Taskforce recommends establishment of national mission for coordinating AI-related activities across India”, OpenGov, 2018 年 4 月 9 日。

¹⁴ Graham Greenleaf, “Global data privacy laws 2017:120 national data privacy laws, including Indonesia and Turkey–145 privacy laws and business international report 10, 2017”, 新南威尔士大学法律研究丛刊, 第 45 期(2017 年)。

44. 特别值得注意的是在最高法院对 *Puttaswamy* 案作出裁决¹⁵ 后提出的印度法律草案。该法案草案于 2018 年年中发布，拥有《欧洲联盟通用数据保护条例》(第 2016/679 号)的许多积极特征，比如数据保护影响评估、被遗忘的权利和适当的惩处措施。但也有一些问题，比如对研究可能再识别本应匿名处理的数据集中的人员的工作施加限制。此外，尽管执法部门对个人数据的使用应该是“必要和适当的”，但在很多例外情况下可在法律诉讼程序中披露这些数据。¹⁶ 特别报告员敦促印度政府与提出这些问题的学术界、研究人员和民间社会组织互动协作。

45. 印度最高法院在 2018 年 9 月 26 日的一项判决中维持《Aadhaar 法》的宪法效力，但撤销了：(a) 第 57 条，其中规定私营公司可要求消费者在使用 Aadhaar 方案时提供详细资料，用于识别身份；(b) 第 33(2)条，内容是以国家安全为由与安全机构共享数据；(c) 第 47 条，其中规定只有政府才能够在 Aadhaar 数据失窃的情况下提出申诉。¹⁷ 法院要求政府出台强有力的数据保护立法。

46. 欧洲联盟内部实行了重大改革。《通用数据保护条例》于 2018 年 5 月 25 日生效，一项关于在警务和司法领域保护数据的具体指令于 2018 年 5 月 6 日开始适用。2002/58/EC 号关于隐私和电子通信的指令将被新的电子隐私条例所取代。¹⁸ (EC)45/2001 号条例规定了欧洲联盟各机构的数据保护规则和欧洲数据保护监督员的职责。2017 年 1 月 10 日，欧洲联盟委员会通过了一项提案，该提案废除了上述条例，并使之与《通用数据保护条例》一致；这两项措施预计将从 2018 年末起适用。经过这次改革，欧洲联盟将完成 20 多年内的首次隐私保护和数据保护框架现代化的重大工作。¹⁹

47. 欧洲联盟内部的这些重要巩固措施适用于所有部门，但隐私和“国家安全”不在此列——这个问题根据《欧洲联盟条约》第 4.2 条被排除在欧洲联盟的权限外。通过比利时、法国、荷兰和联合王国等国更新其立法的努力，欧洲联盟内部对国家安全(而不是执法)职权范围内的监视进行管制的方式更加迥异。

¹⁵ 印度最高法院，Civil Original Jurisdiction, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*, Writ Petition (Civil) No. 494 of 2012, Judgment, 24 August 2017. 可查阅：[http://supremecourtindia.nic.in/pdf/jud/ALL%20WP\(C\)%20No.494%20of%202012%20Right%20to%20Privacy.pdf](http://supremecourtindia.nic.in/pdf/jud/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf)。

¹⁶ Richard Chirgwin, “India mulls ban on probes into anonymized data use—with GDPR-style privacy laws”, *The Register*, 2018 年 7 月 31 日。可查阅：www.theregister.co.uk/2018/07/31/india_privacy_boffin_ban/。

¹⁷ 印度最高法院，Civil Original Jurisdiction, *Justice K. S. Puttaswamy (Retired), and Another v. Union of India and Others*; *Economic Times*, “This is what the Supreme Court did not like about Aadhaar”, 26 September 2018. 可查阅：http://economictimes.indiatimes.com/articleshow/65961697.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst。

¹⁸ 见欧洲联盟委员会，“Proposal for a regulation of the European Parliament and of the Council concerning the respect for private life and protection of personal data in electronic communications repealing Directive 2002/58/EC (Regulation on Privacy and Electronic Communications)”，2017 年 1 月 10 日。

¹⁹ 见 https://edps.europa.eu/data-protection/data-protection/legislation_en。

48. 在更广泛的区域层面，我们深受鼓舞地注意到，《关于在处理个人数据方面保护个人的现代化公约》(亦称“《第 108 号现代化公约》”)于 2018 年 6 月定稿，其授权法律文书(《欧洲委员会条约汇编》第 223 号议定书)，于 2018 年 10 月 10 日开放供签署。这是一个重要的里程碑，因为该《公约》与《通用数据保护条例》不同，也涵盖国家安全，已得到超过 55 个联合国会员国的批准，越来越多的非欧洲国家也即将加入。

49. 在巴西，参议院批准了《通用数据保护法》，该法将于 2020 年 2 月生效。关键要素包括：20 跨境管辖权；隐私原则和基于风险的方法；新的个人权利；为处理个人数据提供更多法律依据；数据映射和数据保护影响评估；强制性违约通知和数据保护干事；对跨境转移个人数据的限制。

50. 对不合规行为的罚款可能最高为公司或公司集团销售总额的 2%，或每次违规最高罚款大约 1 290 万美元。

土著人民和数据

51. 特别报告员多年来研究了澳大利亚土著人的隐私文化。鉴于这种文化是个人、家庭和集体隐私的最微妙、最鲜活的表现，通过行为、仪式以及私人 and 共同空间等做法得到落实，特别报告员感到高兴的是，关于大数据和开放数据的协商会议探讨了土著人的数据主权问题，尽管讨论不算太深入。

52. 特别报告员鼓励各国政府和公司承认土著人民对关于他们的数据或向他们收集的数据的固有主权，这些数据涉及土著人民的知识体系、习惯或领土。

二. 就特别报告员上次提交大会的报告进行协商

53. 特别报告员在 2017 年 10 月提交大会的报告(A/72/540)中审查了在结合数字时代的一个决定性特征(大数据和开放数据)确保隐私这一人权方面遇到的挑战。自那时以来，出台了《通用数据保护条例》，涉及脸书和剑桥分析公司的事件被揭露。

54. 2018 年 7 月 26 日和 27 日，在澳大利亚与政府官员、民间社会组织、公司和个人就该报告进行了协商。在协商之前，要求各方提交资料，这项工作于 2018 年 4 月 28 日完成，为进行协商汇总了这些资料。更多投入来自澳大利亚隐私基金会与民间社会组织举办的会议和协商后收到的资料。

A. 反馈意见汇总

55. 在公开协商期间审议了大数据和开放数据的由来和使用情况；各自的潜在好处和危害；使用个人数据对其他人权的影响；去识别化方法是否适当；使用个人数据的良好做法；人权和道德在自动化决策技术中的重要性；土著人的数据主权；消费者和性别平等问题；非欧洲国家的观点。²¹ 讨论大多涉及开放数据以及开放数据与大数据相互作用对隐私造成的后果。

²⁰ 见 www.onetrust.com/what-is-the-brazil-general-data-protection-law-lgpd/。

²¹ Amanda Lo, “The right to privacy in the age of big data and open data”, 新南威尔士大学，安德慎技术、法律和创新中心，2018 年 8 月 21 日。

B. 开放数据

56. 大数据分析和基于人工智能的计算方法会带来惠益，同时也会给个人和社区以及民主社会的结构带来潜在的隐私风险。开放政府信息，特别是反复公开发布载有个人信息的数据集，需要更细致、更密切的审查。²²

57. 协商会议审议了这样一种看法，即尽管进行了去识别化，大数据解析仍能够识别个人身份。²³ 与会者了解到，确定数据或数据解析项目的结果是否包含个人信息如何取决于使用或披露的背景，以及这一点如何能随其他因素而变化。因此，再识别最好是从风险水平角度来阐述，而不是作为一个绝对事物来阐述。风险水平取决于谁可获取数据、数据粒度如何(数据中最小的组的大小)、有哪些其他数据集可以准确地与数据和相关外部环境联系起来。

58. 数据内部的“个人信息”涵盖广泛的领域，不同司法管辖制度有不同说明。大多数定义的共同点是，个人信息的范围可能非常广，关注识别个人身份的能力，而不仅仅是数据本身是否识别个人身份。

59. 对于识别载有个人信息的数据很关键的两个方面是：(a) 数据本身必须识别个人身份；或者(b) 必须有识别个人身份的合理可能性。

60. 三个主要的数据共享机制(明确、衍生和推断)中的每一个都考虑所含个人信息的程度，以及获取、使用和储存这一数据的组织的义务。

61. 在线浏览和购买数据可日益用于在不了解用户身份的情况下对服务进行个性化。不过，有人担心的是，特别有针对性的匿名识别信息是否构成个人信息。移动网络数据已用于网络优化以外的其他目的，从而得以预测客户流失率，甚至可在不了解所涉个人身份的情况下显示与其他移动用户的关系。²⁴

62. 数据共享面临的一个关键挑战是目前无法明确确定汇总数据内是否含有个人信息，或分类数据是否能重新汇总。再识别的风险取决于有关数据集的存取(以及将其链接的能力)、去识别所用的方法以及数据汇总或扰动水平。因此，不同组织采用不同的方法和不同的数据汇总水平，取决于与所分享数据有关的认知风险。

63. 制定标准来确定哪些数据构成“去识别化”数据有助于解决在处理隐私方面遇到的挑战。关于“去识别化”的含义，在国际一级，目前只有很高级别的指导，当然都不是定量指导，因此很多组织必须根据不同的数据集和如何合理使用这些数据集或将其与其他数据合并，针对具体情况确定“去识别化”对它们的含义。

64. 2017 年，澳大利亚计算机协会发表了一部技术白皮书，其中探讨了共享数据方面的挑战，并重点强调，创建智能服务方面的一项基本挑战是一套数据集是否

²² 莫纳什大学的 M. Paterson 提交的资料，2018 年 8 月。

²³ 见维多利亚州信息专员办公室，“Protecting unit-record level personal information: the limitations of de-identification and the implications for the Privacy and Data Protection Act 2014”，2018 年 5 月。可查阅：<https://ovic.vic.gov.au/resource/protecting-unit-record-level-personal-information/>。

²⁴ Ian Opperman 提交的资料，澳大利亚新南威尔士州政府数据分析中心，2018 年 8 月 31 日。

载有个人信息的问题。回答这一问题是一个重大挑战，因为合并数据集的行为创建了信息。该文件还提出了数据共享方面“五个安全”框架的修改版，以量化不同的“安全”门槛。这项工作澳大利亚标准公司的支持下继续进行，旨在启动制定保护隐私和共享数据的国际标准的工作。第二部白皮书计划于 2018 年 10 月发表，预计该书将成为国际标准化活动的基础，目标是最终制定保护隐私和共享数据的强有力框架。²⁵

65. 2016 年 8 月在线公布了一个大型纵向数据集，其中载有 10% 的自 1984 年以来领取医疗福利或自 2003 年以来领取药品福利的澳大利亚人样本，这个例子说明去识别化对保护单元记录级别记录的局限性。²⁶ 这影响了大约 290 万澳大利亚人的医疗数据，包括处方、手术、化验(不包括结果)以及找全科医生和专科医生就诊的情况(不包括医生说明)。²⁷ 该数据集在下线前已被下载 1 500 次，此前，有报告称，医生身份证明很容易被解密，²⁸ 后来又有报告称，可识别患者的身份。²⁹ 澳大利亚卫生部公布资料是为了促进医学研究。

66. 这些例子引起的重要问题包括：再识别造成大规模侵犯隐私的风险日益增加，部分原因是可获得公开发布的其他信息，以及组织技术能力不足，在这种情况下，政府持有的个人信息数据集是否应对外公布；应采取何种适当对策来防止此类事件再次发生。

67. 从协商会议收集的资料来看，要发布政府持有的信息，显然必须适当保护隐私，并采取监管对策。有人坚决认为，无限制地获取单元记录级别的数据以及无法以汇总形式安全披露的其他个人数据的情况与隐私权发生矛盾。反馈意见不支持把为检验所发布数据集的安全性而进行的再识别定为刑事罪的监管对策。³⁰

²⁵ 同上，包括澳大利亚计算机协会，*Data Sharing Frameworks*，技术白皮书(2017 年，悉尼)。可查阅：www.acs.org.au/content/dam/acs/acs-publications/ACS_Data-Sharing-Frameworks_FINAL_FA_SINGLE_LR.pdf。

²⁶ Vanessa Teague 在 2018 年 7 月 26 日和 27 日关于“大数据-开放数据”的协商期间提交特别报告员的资料，澳大利亚悉尼新南威尔士大学。另见澳大利亚信息专员办公室，“Publication of MBS/PBS data”，专员启动的调查报告，2018 年 3 月 20 日，第 7-9 页。可查阅：www.oaic.gov.au/resources/privacy-law/commissioner-initiated-investigation-reports/publication-of-mbs-pbs-data.pdf。

²⁷ Vanessa Teague, Chris Culnane and Ben Rubinstein, “The simple process of re-identifying patients in public health records”，墨尔本大学，Pursuit，2017 年 12 月 18 日。可查阅：[错误!超链接引用无效。。](#)

²⁸ Chris Culnane, Benjamin Rubinstein and Vanessa Teague, “Health data in an open world”，report on re-identifying patients in the MBS/PBS dataset and the implications for future releases of Australian Government data，墨尔本大学，2017 年 12 月 18 日。可查阅：<https://arxiv.org/ftp/arxiv/papers/1712/1712.05627.pdf>。

²⁹ 澳大利亚信息专员办公室发现，医生的身份可识别，患者的身份也可识别，但从《澳大利亚隐私法》角度来讲不可“合理识别”。据了解，受影响的人没有得到通知。

³⁰ M.Paterson 等人提交的资料。

68. 与会者介绍了允许将可识别的个人数据用于研究目的的现有机制，³¹ 指出这些机制可酌情扩大，用于更多公益用途。³²

69. 问题似乎是，如果有用的数据被视为有限资源，而不是无限的未开发资源，我们是否会有更可持续的做法？³³

70. 目前脱离数据主体的做法被比喻为“杀死下了金蛋的鹅”，因为对政府或私人行为体适当管理个人信息的能力的不信任导致人们或者不使用服务——这反过来有可能造成负面社会影响，例如在公共卫生领域——或者提供不全面或不准确的信息。³⁴ 这些行动还影响数据质量，最终影响机器学习算法的准确性。

71. 在协商会议上，压倒性的观点是，如果数据主体是数据业务方面的完全成熟的伙伴，数据做法的可持续性会加强。³⁵ 与会者了解到，这一点对土著人民而言比任何其他群体都更为显著、更为重要。

C. 土著人的数据主权

72. 对土著人民来讲，数据是一种文化、战略和经济资源。然而，土著人民仍基本上未能参与收集、使用和适用关于他们、他们的土地和文化的的海数据。³⁶ 现有数据和数据基础设施未能承认土著知识和世界观或对此给予特权，也无法满足土著人民目前和今后的数据需求。目前围绕大数据和开放数据采取的做法，无论是政府支持的，还是公司支持的，都可能使决策机构在作出影响土著人民数据的决策时不考虑土著人民的数据权益。

73. 土著人的数据主权是一项全球运动，涉及土著人民拥有、控制、获取和掌握源于他们的、并且与它们的成员、知识系统、习惯或领土有关的数据的权利。³⁷ 它靠《联合国土著人民权利宣言》所述的土著人民的自决权和管理其土地、资源

³¹ 这些机制通常受道德委员会监督，仅限研究人员根据保密义务加以利用。

³² 例如，根据“五个安全”框架等机制：见澳大利亚统计局“Managing the risk of disclosure: the five safes framework”, Confidentiality Series, part 3, 2017年8月。可查阅：www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=S。

³³ 澳大利亚悉尼技术大学的 Theresa Dirndorfer Anderson 提交的资料。

³⁴ 澳大利亚信息专员办公室，*Australian Community Attitudes to Privacy Survey, 2017* (2017年，堪培拉)。可查阅：www.oaic.gov.au/engage-with-us/community-attitudes/australian-community-attitudes-to-privacy-survey-2017；澳大利亚，澳大利亚信息专员办公室，*Community Attitudes to Privacy Survey: Research Report 2013* (2013年，堪培拉)。可查阅：www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-reports/2013-community-attitudes-to-privacy-survey-report.pdf。

³⁵ Theresa Dirndorfer Anderson 提交的资料。

³⁶ Tahu Kukutai and Maggie Walter, “Recognition and indigenizing official statistics: reflections from Aotearoa New Zealand and Australia”, *Statistical Journal of the IAOS*, vol. 31, No. 2 (2015)。

³⁷ Tahu Kukutai and John Taylor, “Data sovereignty for indigenous peoples: current practice and future needs” and C. Matthew Snipp, “What does data sovereignty imply: what does it look like?”, 二者均载于 Kukutai and Taylor (编), *Indigenous Data Sovereignty: Towards an Agenda, Research Monograph, 2016/38* (澳大利亚大学出版社, 2016年, 堪培拉)。可查阅：<https://press.anu.edu.au/publications/series/centre-aboriginal-economic-policy-research-caepr/indigenous-data-sovereignty>。

和文化的权利支撑。土著人的数据主权中隐含了土著人民的愿望，即应以支持和加强土著人民集体福祉的方式使用数据。

74. 土著人的数据主权作为一项基本原则在与大数据和开放数据有关的管理安排中占有一席之地。它是通过土著人的数据管理行使的，这种管理包括各种原则、结构、问责机制、与数据管理、隐私和安全有关的政策以及法律文书。土著人的数据主权框架可适用于内部控制和拥有的民族/部落数据，以及外部储存或管理的数据。澳大利亚和新西兰的土著人数据主权网络正在围绕土著人的数据管理问题制订规程。³⁸

75. 土著人的数据主权说明，要采取有关大数据和开放数据的良好做法，就必须认识到有些数据缺失、未被充分代表或被歪曲，³⁹ 并认识到此类做法符合或不符合的利益。

D. 性别问题

76. 协商期间有人提出，不同性别或性别认同的人可能会有不同的隐私体验。

77. 例如，对于男女同性恋、双性恋、跨性别者、性别奇异者和双性者来说，隐私是他们高度关切的问题，对于逃离家庭、家族或宗教暴力者(通常是妇女)的安全来说，隐私也是必不可少的。

78. 包容性数据收集做法能够体现接受和尊重，而侵入式收集可能成为获取服务的一个重大障碍，因为男女同性恋、双性恋、跨性别者、性别奇异者和双性者等群体在遭受歧视、污名和有针对性的暴力之后，有理由担心隐私问题。

79. 隐私和人格工作组将更加深入地探讨这一问题。然而，就大数据和开放数据而言，良好做法需要审查数据收集方式，并了解不良隐私做法可能产生的影响以及对不同性别或性别认同的人产生的不同后果。

E. 消费者权利与个人数据的收集和使用

80. 在数据驱动的消费者市场中，越来越多的数据用于开发、销售和推广消费产品，这意味着许多数据保护问题也成为了消费者问题，反之亦然。现在，消费者法和数据保护法之间的区别不再那么鲜明。⁴⁰

81. 金融服务和其他部门对消费者个人数据的使用引起了公共政策和个人层面的关切。⁴¹ 个人数据的公平处理日益成为消费者对其所使用服务和产品的合理期望之一。⁴²

³⁸ 澳大利亚塔斯马尼亚大学的 Maggie Walter 提交的资料。

³⁹ Theresa Dirndorfer Anderson 提交的资料。

⁴⁰ Natali Helberger, Frederik Zuiderveen Borgesius and Agustin Reyna, “The perfect match? A closer look at the relationship between EU consumer law and data protection law”, *Common Market Law Review*, vol. 54 (2017).

⁴¹ Lee Rainie and Maeve Duggan, “Privacy and information sharing”, 14 January 2016 (人们的舒适程度取决于对可信度的感知、收集后的情况以及保留时间)。Phuong Nguyen and Lauren Solomon, *Consumer Data and the Digital Economy-Emerging Issues in Data Collection, Use and Sharing* (Consumer Policy Research Centre, 2018) (认为消费者希望在收集哪些数据、使用数据以及政府参与改善消费者对数据的控制和防止数据滥用方面有更多的选择)。

⁴² Helberger, Zuiderveen Borgesius and Reyna, “The perfect match?”。

82. 协商期间有人比较了消费者法和隐私/数据保护法采用的方法，并指出一些国家正在实行消费者隐私举措。

83. 在发生剑桥分析公司丑闻之后，2018 年 6 月，美国加利福尼亚州颁布了《消费者隐私法》。该法将于 2020 年 1 月生效，通过对收集、使用和共享个人数据的公司实施新规则来保护技术用户和其他人的数据隐私。⁴³ 该法规定个人享有四项基本权利：有权了解企业掌握的个人信息以及这些个人信息来自何处或发往何处；有权删除企业向他们收集的个人信息；有权选择不出售其个人信息；有权从企业获得平等服务和定价，即使他们根据该法行使隐私权。⁴⁴ 根据加利福尼亚州现行的数据泄露通知法，该法还为消费者规定了起诉企业数据安全违规行为的有限权利。

84. 然而，据报告称，该法规定的权利需要得到加强，原因如下：

(a) “企业”一词定义狭隘。⁴⁵ 在数字时代，小型技术机构和个人也可能由于不具备实施适当数据保护的知识、技能或资源，以各种形式破坏隐私；⁴⁶

(b) 企业仍然可以向行使隐私权的用户收取更高的价格；

(c) 由于例外情况有限，用户无法轻易将违规者告上法庭；

(d) 只有在出售数据时才需要用户同意，收集数据时不需要，而用户必须主动选择才能表示其不同意出售数据；

(e) “知情权”没有规定具体的来源或接收者，“删除权”是针对从个人那里收集的信息，而不是针对关于个人的信息；

(f) 大多数执法责任归属于加利福尼亚州总检察长，而不是独立实体。

85. 根据欧洲联盟数据保护法，《通用数据保护条例》的各个方面为欧洲联盟消费者提供了新的保护。与欧洲联盟消费者保护指令可能提供的保护相比，该条例提高了公司收集的有关消费者数据的透明度，并对数据加强了控制。⁴⁷

86. 澳大利亚正在确立“消费者数据权利”，即数据可移植性权利，⁴⁸ 这项权利没有得到根据隐私法或数据保护法为澳大利亚消费者提供的更广泛的保护，而对

⁴³ 见 https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375。

⁴⁴ Adam Schwartz, Lee Tien and Corynne McSherry, “How to improve the California Consumer Privacy Act of 2018”, Electronic Frontier Foundation, 8 August 2018.

⁴⁵ 同上，“该法将‘企业’定义为符合以下条件的营利性法律实体：(一) 年度总收入为 2 500 万美元；(二) 每年收到或披露 50 000 个消费者、家庭或设备的个人信息；或(三) 通过出售个人信息获得其年收入的 50%或以上(第 140(c)条)”。

⁴⁶ 澳大利亚悉尼新南威尔士大学 Roland Wen 提交的意见。

⁴⁷ Helberger, Zuiderveen Borgesius and Reyna, “The perfect match?”。

⁴⁸ Australian Competition and Consumer Commission, “Consumers’ right to their own data is on its way”, press release, 16 July 2018。可查阅 www.accc.gov.au/media-release/consumers-right-to-their-own-data-is-on-its-way。

消费者数据的收集、共享和使用每天都在进行。⁴⁹ 有人在协商中指出，这项数据可移植性权利不但不能保护消费者数据，反而可能会使第三方更多地使用这些数据。⁵⁰

87. 在消费者法和隐私法之间建立牢固联系是有利的，例如在共同协调的法律诉讼中。⁵¹ 消费者法可以成为维护消费者与供应商之间商业关系总体平衡的有用工具，也可用于评估公司要求消费者同意处理过多数据并(或)与第三方共享数据的情况是否公平。

88. 关于帮助实体改善与用户信任关系的实际措施，收到了一些反馈，包括采用与六项标准化知识共享许可类似的标准许可来通报数据使用条款。这一手段被认为有可能缓解复杂隐私政策带来的一些挑战，同时可简化与不同国家用户的沟通并使其标准化。⁵² 许可证类型草案可辅以更详尽的“标准条件”隐私政策。

89. 通过使用隐私评级标签来标明隐私风险，可以使消费者更容易作出隐私选择，提高隐私风险的透明度，加强数据控制者对这种隐私的披露。⁵³

F. 人工智能

90. 机器学习和人工智能使用大量数据，反过来又创造更多数据。将数据可用性、计算能力和使用复杂算法的分析能力结合起来，再加上机器学习和人工智能，有可能使社会产生积极变革，但也有可能深刻地改变我们的世界和我们的生存机会，而不一定是朝着更好的方向改变。⁵⁴

91. 产生后一种结果可能是由于人工智能对人权(包括隐私权)造成潜在的负面影响。人工智能方法可以并且正在用于识别希望保持匿名的人；实现消息精准投放；从非敏感数据中生成有关人员的敏感信息；根据全人群数据对人员进行特征类型分析；使用这些数据作出决策，从而深刻地影响人们的生活。⁵⁵

92. 随着越来越多的行动和决策转移到机器上，迫切需要确保机器学习和算法在逻辑和假设方面是透明的。机器学习和人工智能中使用的算法越来越复杂，透明

⁴⁹ Nguyen and Solomon, *Consumer Data and the Digital Economy*。

⁵⁰ 澳大利亚悉尼新南威尔士大学 Katherine Kemp 于 2018 年 7 月 26 日和 27 日在关于大数据和开放数据的协商期间向特别报告员提交的意见。

⁵¹ 美国和欧洲联盟的消费者团体联合要求消费者机构和数据保护主管部门调查联网玩具违反数据保护法和消费者法的情况。见 Helberger, Zuiderveen Borgesius and Reyna, “The perfect match?”。

⁵² 安德慎技术、法律和创新中心提交的意见，2018 年 8 月 14 日。

⁵³ 见 Lorrie Faith Cranor, “Necessary but not sufficient: standardized mechanisms for privacy notice and choice”, *Journal on Telecommunications and High Technology Law*, vol. 10, iss.2 (Summer 2012)。

⁵⁴ Toby Walsh, 2062: *The World that AI Made*, (Carlton, Victoria, Australia, La Trobe University Press, 2018)。

⁵⁵ Privacy International and Article19, “Privacy and freedom of expression in the age of artificial intelligence”, April 2018。

性将难以实现。然而，这种复杂性不应妨碍进行审计以确定合法性。⁵⁶ 目前，对于大数据相关技术的使用是否符合国际人权法、数据保护条例、部门隐私条例、道德准则或行业标准，尚未实行充分问责。⁵⁷ 有人认为，机器应该遵守比人类更高的道德标准，并且通过做出正确的选择，隐私不会是历史的异常，而是通过技术赋予的权利。⁵⁸

93. 《通用数据保护条例》限制了在某些情况下使用自动化决策，并要求向个人提供信息，说明自动化决策的存在、所涉逻辑以及处理该数据对个人的重要性和预期后果。⁵⁹ 除了少数例外情况外，全面禁止在决策具有法律或其他重大影响时仅通过自动化流程作出决策。

94. 《条例》将“特征类型分析”定义为自动化处理数据以分析个人或对个人作出预测，并规定了设计数据保护和默认数据保护的义务。数据隐私影响评估对于许多侵犯隐私的人工智能和机器学习应用程序是强制性的。这些应用程序属于数据保护法的范围，具有巨大的预期风险，例如敏感数据的处理。就人工智能而言，数据隐私影响评估可以——也许应该——使各实体能够模拟其算法的效果，就像气候科学家模拟气候变化或天气模式一样。⁶⁰

95. 欧洲联盟基本权利机构建议，确保有效问责的一种方法可能是建立专门机构，专职负责监督大数据相关技术，其作用与数据保护主管部门类似。⁶¹

96. 虽然手段仍有待确定，但在整个二十世纪，新技术已要求加强国际人道主义法，这一点是非常重要的。⁶²

G. 大数据和开放数据原则

97. 特别报告员在 2017 年 10 月的报告中提出了制定大数据和开放数据监管原则的问题。协商表明，任何制定此类原则的工作都应尽可能借鉴被视为代表“最佳做法”的国际数据保护协定。目前，这些协定包括《通用数据保护条例》和现代化《第 108 号公约》，后者出自欧洲委员会，但已颁布一致原则的全球各国均可加入。⁶³

⁵⁶ European Union Agency for Fundamental Rights, #BigData: Discrimination in Data Supported Decision Making (Luxembourg, European Union Publications Office, 2018)。

⁵⁷ Lee Rainie and Janna Anderson, Code-Dependant: Pros and Cons of the Algorithm Age (Pew Research Center, 2017)。

⁵⁸ Walsh, 2062: The World that AI Made。

⁵⁹ 《欧洲联盟通用数据保护条例》(第 2016/679 号)，2016 年 4 月 27 日，第 13、14 和 22 条。

⁶⁰ Andrew Smith, “Franken-algorithms: the deadly consequences of unpredictable code”, The Guardian, 30 August 2018. 可查阅: <https://www.theguardian.com/technology/2018/aug/29/coding-algorithms-frankenalgos-program-danger>, quoting Neil F. Johnson and others, “Population polarization dynamics and next-generation social media algorithms”, 2017 年 12 月 16 日。可查阅: <https://arxiv.org/pdf/1712.06009.pdf>。

⁶¹ 欧洲联盟基本权利机构。

⁶² Walsh, 2062: The World that AI Made。

⁶³ 悉尼新南威尔士大学 Graham Greenleaf 提交的意见，2018 年 8 月。

98. 《通用数据保护条例》不仅仅通过地方立法或域外适用来发挥影响力。欧洲以外的公司(微软是最突出的例子)正在其整个企业活动中自愿采用遵守《条例》的方式,无论其是否有这样做的法律义务。这种自愿采用可能与法律规定采用一样重要。⁶⁴

99. 从另一个角度看,拥有广泛数据本地化法律的国家正在为其管辖范围内收集的数据制定新的隐私标准。在中国,《网络安全法》对跨境数据传输实行的限制不同于《通用数据保护条例》和自愿性质的《亚太经济合作组织跨境隐私规则》等国际隐私制度。⁶⁵ 虽然《条例》和《网络安全法》似乎有类似的跨境传输测试,但后者没有像前者一样对克减作出规定。⁶⁶ 《网络安全法》也不包含《条例》规定的某些机制,例如为使公司获得核准而制定的具有约束力的企业规则或标准数据保护条款。

100. 特别报告员 2017 年 10 月提交大会的报告中的初步建议是独立于《通用数据保护条例》和现代化《第 108 号公约》制定的,但与这些文书保持一致(见表格)。⁶⁷ 考虑到更广泛的国际背景,实现这种一致非常重要:现代化《第 108 号公约》正在稳步走向全球,包括了《条例》的许多(尽管不是全部)新内容。⁶⁸ 在未来 5 到 10 年内,随着《公约》缔约国不断增加,《条例》的域外影响可能会对深化全球隐私文化产生重大影响。这种演变的确切性质仍在显现,其与进一步发展(如大数据和开放数据独立原则)的必要性之间的关联也在显现。

101. 虽然需要一致的国际框架来监管大数据和开放数据,但在有足够的时间确定《通用数据保护条例》和现代化《第 108 号公约》的稳健性和国际影响之前,开始研究专门针对大数据和(或)开放数据的独立原则还为时过早。

102. 因此,应该本着现有隐私和数据保护原则(而不是任何新的独特规则)的精神来理解大数据和开放数据建议。

⁶⁴ Graham Greenleaf, “Global convergence of data privacy standards and laws: speaking notes for the European Commission events on the launch of the General Data Protection Regulation in Brussels and New Delhi”, University of New South Wales Law Research Series, No. 56, 25 May 2018. 可查阅: www.austlii.edu.au/au/journals/UNSWLRS/2018/56.html。

⁶⁵ Sam Sacks, Paul Triolo and Graham Webster, “Beyond the worst-case assumptions on China’s cybersecurity law”, blog post, New America, 13 October 2017; 安德慎技术、法律和创新中心提交的意见, 2018 年 8 月 14 日。

⁶⁶ Xiaoyan Zhang, “Cross-border data transfers: CSL vs. GDPR”, The Recorder, 2 January 2018; 安德慎技术、法律和创新中心提交的意见, 2018 年 8 月 14 日。

⁶⁷ Graham Greenleaf 提交的意见, 2018 年 8 月。

⁶⁸ 自 2011 年以来,除了 47 个欧洲委员会成员国外,阿根廷、布基纳法索、佛得角、毛里求斯、墨西哥、摩洛哥、塞内加尔、突尼斯和乌拉圭通过申请加入成为了《第 108 号公约》缔约方。其他 11 个国家或其数据保护主管部门是该公约协商委员会的观察员。

特别报告员 2017 年 10 月报告所提建议以及这些建议与《通用数据保护条例》和
现代化《第 108 号公约》的一致性

特别报告员 2017 年 10 月报告(A/72/540)的段落	《欧洲联盟通用数据保护条例》的章节	现代化《第 108 号公约》的条款
131(a), 问责	5(2), “问责”	10(1)
131(b), 透明度	12, “透明度”; 22(3), “自动化决策”和 透明度	5(4)、8(1)
131(c), 质量	5(1)(c), “数据最小化”、(d) “准确性”	5(1)
131(d), 机器学习的可预测性	22, “自动化决策”	8(1)、(2)
131(e), 安全	32-34, “安全” (包括泄露通知)	7(1)
131(f), 风险识别和缓解工具	35, “数据保护影响评估”; 36, “预先协商”	10(2);
131(g), 雇员培训	37-39, “数据保护官”	—
131(h), 隐私监管的明确重点	52, 数据保护主管部门的“独立性”	15(5)
131(i), 对“大数据”的足够监管权力	57, “任务”; 58, “权力”	12、15
131(j), 适合处理技术进步的隐私法	4(1), “个人数据”; 4(4), “特征类型分析”; 4(5), “匿名化”; 22, “自动化决策”; 25, “设计数据保护和默认数据保护”;	8(1)和(2); 10(3)
131(k), 正式协商机制	36, “预先协商”; 57(b)、(c)、(d)和(g), 数 据保护主管部门的“任务”	—
131(l), 危险做法协商	36, “预先协商”;	—
131(m), 新技术	57(i), 数据保护主管部门的“任务——监 测新技术”; 25, “设计数据保护和默认数 据保护”	10(3)
131(n), 公民认识	12, “透明度”; 13-15, “通知数据主体”; 57(b)、(c)、(e), 数据保护主管部门的“任 务”	15(2)(e)
126, 关于开放数据去识别化的约束性要 求和强有力执行	25, “设计数据保护和默认数据保护”; 4(1), “个人数据”; 4(5), “匿名化”	10(3)
127, 如果在开放数据中使用单元记录级 别数据, 则进行严格的隐私影响评估	35, “数据保护影响评估”	10(2)
128, 如果没有强有力的去识别化, 则不提 供开放数据或交换单元记录级别数据	4(1), “个人数据”; 4(5), “匿名化”	2(d)
129, 确保对敏感数据的额外保护	9, “特殊类别”	6

资料来源: Graham Greenleaf 在协商后提交的意见, 2018 年 8 月 7 日。

H. 结论

103. 与资本或劳动力一样，数据目前是、并将仍然是一项重要的经济资产。数据从根本上依赖于个人信息，因此需要与隐私法和数据保护法相适应。

104. 国际人权法规定，对隐私权的任何干涉必须合法、必要和相称。有时，对隐私的挑战可能是合法的，但是否合乎道德则是另一个问题。这里讨论的一些例子是否合乎道德、合法、必要和相称，是有疑问的。最近发生了一些私营和公共实体对个人数据管理不当的案件，需要采取强有力的应对措施，以防止再次发生。

105. 国际人权法还规定，隐私权受到侵犯的人可以获得补救。这一点在大数据和开放数据时代更为重要。

106. 将数据作为开放数据发布的关键挑战是，缺乏一种方法来明确地确定所谓的去识别数据集或汇总数据中是否存在个人信息。

107. 经济和政治推动因素构成了开放数据相关政策和做法的基础。在资本主义经济固有的商业模式中，如果没有相应的经济劣势来抵消所获得的利润，就会缺乏保护个人数据的动力。

108. 建立具有一致数据保护和明确跨国访问规则的国际框架，将有助于权衡隐私保护和各国在获取数据方面可能存在的利益冲突(例如在执法领域)，或跨国公司在管理内部数据流动方面可能存在的利益冲突。

109. 允许不受限制地共享数据和取消对隐私的现有法律保障的举措违反了保护隐私权的原则，必须停止。

110. 不支持作为个人数据的保障措施把(出于公共利益)对去识别数据集进行再识别的行为定为刑事罪。

111. 未经数据主体同意，不得在网上披露或公布详细的单元记录级别数据(可识别数据)。使用实物和技术方法(如安全研究环境)来限制对敏感单元记录级别数据的访问，是适当的。

112. 消费者法和数据保护法可以有效地相互补充。隐私法及其人权和社会方面为消费者法提供了支柱。单纯依靠消费者法，将使个人无法从基本人权与其补救机制之间的相互依存关系中更多受益。

113. 人工智能当前和潜在的表现形式需要不同学科领域的专家进行独立监督。这项技术的发展需要一个立足于人权的强大法律和政策框架。这一问题既紧迫、又关键。

114. 需要密切监测《通用数据保护条例》第 22 条的适用情况，这涉及该条处理因使用人工智能而产生的自动化处理问题的能力。

115. 必须解决缺乏技术能力来设计适当的系统、方法和程序的问题，并确保系统、方法和程序的稳健，以便对个人数据进行强有力的保护。这应该涉及小型科技公司和初创企业。

116. 如果会员国正在考虑制定促进开放数据的立法，⁶⁹ 建议考虑以下要素：

- (g) 所有立法必须高度符合各国的国际人权义务；
- (h) 应当对数据保护立法方面的最佳做法加以研究，以供效仿；
- (i) 基于公平正义原则的数据道德框架和问责机制对于公共和私营部门的数据做法是必要的；
- (j) 适当的隐私和数据保护监管模式需要结构独立性、充足的资源和具有独立能力的监管者；
- (k) 取消隐私法和数据保护法以实现开放数据的做法违背了全球趋势，很不明智，也违反了各国在隐私权方面的国际人权义务；
- (l) 需要在定义和概念中区分数据共享、使用、披露和发布；
- (m) 共同设计框架需要使用具有充分多样化代表性的参与模式和机制，以解决土著人的数据主权等问题。

I. 建议

117. 根据协商，特别报告员对其在 2017 年 10 月 19 日提交大会的报告(A/72/540)中提出的原始建议作了扩充，内容如下：

- (a) 在立法、政策和实践中，应把政府内部共享个人数据与作为开放数据向公众发布数据区分开来；
- (b) 除非并且直到能够明确地确定汇总数据中是否存在个人信息，或者分类数据无法重新汇总，否则开放数据不应包含单元记录级别的记录；
- (c) 为维持数据共享和国际标准化活动而制定国际隐私标准的工作必须毫不拖延地继续进行，并得到会员国的支持；
- (d) 需要对差分隐私进行研究，应将其用于汇总统计和复杂数据类型以及其他隐私保护技术，如同态加密和安全多方计算；
- (e) 作为对商定在全球层面协调一致的详细隐私规则的临时最低回应，鼓励会员国通过授权法律文书(《欧洲委员会条约汇编第 223 号》议定书)批准现代化《第 108 号公约》，并通过国内法毫不拖延地执行其中所载的原则，特别注意立即执行那些要求为监控和其他国家安全目的而收集的个人信息提供保障的规定；
- (f) 为了与最佳做法保持一致，鼓励欧洲联盟以外的会员国在审查和更新国内法以实施现代化《第 108 号公约》时，尽可能纳入《通用数据保护条例》所载、《公约》没有作出强制规定的保障措施和补救办法；

⁶⁹ 例如，见澳大利亚在“New Australian Government data sharing and release legislation: issues paper for consultation”中提出的建议，可查阅：www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation，载于 M. Paterson 提交的意见。

(g) 各国政府和公司应承认土著人民对关于他们或从他们那里收集的、涉及土著人民、知识体系、习俗或领土的数据拥有主权，始终纳入由土著人民制定的正式原则，重点关注土著人民领导权和问责机制；

(h) 会员国应审查关于人工智能的所有法律和政策框架是否足以保护言论自由和隐私权；促进统计学家、律师、社会科学家、计算机科学家、数学家和学科领域专家进行强有力的多学科合作；制定战略，防止或处理因使用算法、自动化处理、机器学习和人工智能而对享受人权产生的任何不利影响。

118. 特别报告员还重申他在上次报告中提出的建议(见 [A/72/540](#)，第 126-131 段)。
