联 合 国 A/HRC/46/37

大 会

Distr.: General
25 January 2021
Chinese
Original: English

人权理事会
第四十六届会议
2021 年 2 月 22 日至 3 月 19 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

人工智能与隐私，以及儿童隐私

隐私权特别报告员约瑟夫·坎纳塔奇的报告*, **

概要

本报告系根据人权理事会第 28/16 号和第 37/2 号决议编写。隐私权从未像现在这样重要，也从未像现在这样受到围攻。正如 2015 年所预测的那样，技术趋势对隐私权的享有提出了前所未有的挑战。在本报告——亦即首任隐私权特别报告员的最后一份报告中，他讨论了两个不同的挑战：首先是人工智能与隐私，其次是儿童隐私，特别是隐私在支持自主和积极参与社会方面的作用。本文概述了通过磋商和研究制定的指导意见和建议，以应对这些挑战。本报告与特别报告员在以往的报告中提出的其他建议共同完成了 2016 年提交人权理事会的工作计划(A/HRC/31/64)。附件概述了特别报告员自 2015 年以来根据任务授权开展的各项活动。

* 因提交方无法控制的情况，经协议，本报告迟于标准发布日期发布。

** 本报告附件不译，原文照发。

一. 针对开发和运行人工智能解决方案提出的隐私保护建议

背景和宗旨

1. 本文所列建议的宗旨是就作为应用信息和通信技术(信通技术)的一部分开发人工智能[1] 解决方案的过程中使用个人和非个人信息问题提供指导原则，并强调各国政府和公司在人的隐私权这一总体框架内处理人工智能数据的合法依据的重要性。

2. 这些建议以《世界人权宣言》为基础，反映了《宣言》的精神和理念。特别是，第七条(非歧视)和第十二条(隐私权)对于开发或运营人工智能解决方案至关重要。这些条款的主题和价值观也载于《公民及政治权利国际公约》第二和第三条(不歧视)及第十七条(隐私)，属批准该条约的各国应承担的义务。

3. 权利在信息社会中极为重要。大会和人权理事会确认，人们离线时享有的权利在线时也应该得到保护(A/75/62-E/2020/11, 第 9 段)，作为互联网保持全球性、开放性和互可操作性的条件(人权理事会第 26/13 号决议)，并作为加速推进各种形式发展、包括实现可持续发展目标的驱动力(大会第 73/179 号决议)。

4. 建议的重点是人工智能解决方案背后的所有数据的隐私。[2] 我们希望这些建议能够成为通用国际基线，用于人工智能解决方案、特别是在国内实施的人工智能解决方案的数据保护标准。特别报告员认识到人工智能解决方案的许多经济和社会效益，并希望这些建议能够成为如何在人工智能解决方案的背景下保护隐私权的基准点。

5. 执行这些建议需要各国政府、民间社会、私营部门、技术界和学术界之间的全面合作，并应坚持包容、尊重、以人为本、人权、国际法、透明度和可持续性等人类共同价值观。

6. 人工智能解决方案涉及应用旨在指导、预测或做出影响每个人生活的决定的人工智能系统。人工智能解决方案提供了诸多益处，但同时也造成了种种影响，目前社会上正就此进行辩论。这些辩论──道德、伦理和社会问题，涉及隐私、不歧视和自由参与等人权──仍将持续。要解决所有这些问题，就必须从隐私的角度予以合法处理。这一点尤为必要，因为大多数数据由利用其商业价值的私营公司持有，这些公司将不同数据集组合在一起，以期最大限度地提高分析能力。公众日益关切数据收集的侵扰性和潜在影响、被监视的风险，关切日益使用借助这些数据集的算法来自动生成影响个人生活的决定，必须对此作出回应(A/75/62-E/2020/11, 第 10 段)。

7. 鉴于人工智能部署的背景，监督专门立法的隐私和/或数据保护监管机构必须有效、独立地运作。

[1] 人工智能有若干定义。本报告中所采用的是最常见的意思，亦即《牛津参考文献》给出的定义：“能够执行通常需要人类智力完成的任务(如视觉感知、语音识别、决策和语言之间的翻译)的计算机系统的理论及其开发”。这远远不是人工智能技术应用的详尽清单。

[2] 特别报告员认为数据保护可追溯到《保护人权与基本自由公约》第八条中尊重私人生活的权利，将数据保护法视为隐私条例的一个子集中的一部分。他认识到，由于欧洲的历史发展，数据保护被明确单列为《欧洲联盟基本权利宪章》的一项条款，但他请读者查阅历史参考资料。

范围

8. 本文所列建议适用于社会所有部门(包括公共和私营部门)人工智能解决方案的数据处理。数据处理是指人工智能解决方案生命周期(包括人工智能解决方案的设计、开发、部署和停用，以及基于先前人工智能解决方案的任何迭代或重新设计)中涉及数据的每个阶段。

9. 这些建议适用于所有人工智能解决方案的管理者。这可能包括设计师、开发人员或运营者(自负责任或主要责任人)，每个人都有自己特定的功能。其目的是在一个组织内部，每个人工智能解决方案都有一个法人或自然人对该人工智能解决方案负全责。

10. 这些建议并不限制或以其他方式影响任何法律赋予数据主体更多、更广泛或更好的权利、保护和/或补救。它们也不限制或以其他方式影响任何法律在数据隐私方面为数据管理者和处理者规定更高、更广泛或更严格的义务。

11. 这些建议不适用于可能由个人在纯粹私人或家庭活动中开展的人工智能解决方案。

考虑人权和道德问题

12. 社会有责任在人权框架内以道德和负责任的方式开发人工智能解决方案。人工智能解决方案现在已经影响到日常生活的诸多方面，这种影响未来只会加剧，从而对人们的个人生活和工作产生深远影响。未来，人工智能解决方案可能会涵盖更广泛的反映人权法和道德问题的基本原则。如何使用这项技术至关重要。

13. 不歧视对于避免不平等、不公正和痛苦至关重要，因为这可能影响人们享有人权，包括经济、社会及文化权利。需要精确监测人工智能解决方案的使用，且必须纠正任何侵犯人权的歧视或其他结果的发生，以避免这种不利影响。

14. 不应鼓励在最终决策中使用人工智能解决方案，而只应将其作为某些领域决策支持的一部分，例如司法或医疗领域的决策。人权评估应始终与数据保护评估一同进行，以全面了解必要的框架条件。

15. 世界各地的委员会，例如欧洲委员会人工智能特设委员会，目前正在起草人工智能解决方案的监管框架和道德准则。应参考上述监管框架和道德准则及其他相关指导意见，如《工商企业与人权指导原则》。

人工智能与数据隐私

16. 目前的人工智能系统包括或代表基于结构化专家知识(数据仓库、商业智能)的分析系统与机器学习的结合，以及对所学知识的针对性应用。用来解决特定问题的预先编好程序的算法系统和可以学习的系统之间是有区别的。后者配备了学习算法，必须经过训练。

17. 算法决策过程通常被用作人工智能的基础。在这一过程中，往往基于信息进行评估，进而作出决定、进行预测或提出行动建议。在“监督学习”的情况下，人工智能系统有解决某一特定问题的解决标准，而在“非监督学习”的情况下，人工智能系统本身会选择或推荐相关的解决标准。

18. 因此，数据处理和根据上述处理作出的决定都对数据主体具有潜在风险。

19. 经典信息技术(其要素是“输入”—“处理”—“输出”)通过感知、理解、行动和学习能力得以延展。这些活动以前只能由人开展，现在则越来越多地由机器执行。“理解”一词是与计算机相关的新领域，必须伴随着对可追溯性的批判性审查，且须遵守人权和道德价值。

20. 机器学习是指人工神经网络中的一系列优化方法等。人工智能系统在输入层和输出层之间可能具有非常复杂的结构。通过梳理若干分级处理层，机器学习的效率可以大大提高(深度学习)。这不可避免地导致人工智能决策的可追溯性降低。由于算法的复杂性和机器执行的种种运算，较深的处理层(隐藏层)在决策标准及其权重方面不透明。

21. 披露人工智能所基于的算法是当前关于人工智能透明度的辩论的核心要求。然而，在实践中，使用公开算法对极为复杂的人工智能系统的决策逻辑进行具体验证可能很困难。无论我们处理可诠释人工智能、可解释人工智能还是其他模型，如果在过程或结果中出现疑问或失败，就必须捕获数字证据，以重建发生了什么，以及为什么建议了某一结果或为什么实际上产生了某一结果。

22. 通过对照系统的预定目标审查决策本身和道德治理，从外部监控人工智能系统的决策过程有诸多好处，包括实用性。

23. 必须查明超出预期结果或决策范围的人工智能决策，并进行干预。专门为检测意外结果和分析人工智能决策而开发的工具是先决条件。完全由机器监控机器增加了不可预见的风险或称“未知的未知”的可能性。因此，必须遵守一个原则，即人工判断必须始终主导人工智能监控过程。

24. 除了学习机制的效率外，机器学习能否成功还取决于可用数据的数量和质量。信息技术的大数据趋势和优质数据的海量可获得性正显著加速人工智能系统的发展。

25. 人类知识和决策所涉及的十分复杂的心理和情感过程很可能继续是人类掌控的领域，而不是机器掌控的领域。因此，在评估和权衡与人工智能系统及其决策相关的适用法律时，必须铭记，机器决策所基于的原则和机制(尽管基本是由人类开发的)与人类决策所应用的原则和机制不同。

26. 为了实现人工智能系统的必要安全性，必须在使用人工智能解决方案的实体所拥有的控制环境中有效实施对人工智能决策的全面道德和法律治理。此外，还需要改进数字合作，多个利益攸关方应思考，如何在不同社会环境下的人工智能应用中，设计和适用透明度和非偏见等标准和原则。

A. 使用人工智能解决方案的数据隐私原则

27. 无论对负责任的管理者适用何种法域或法律环境，在规划、开发和实施人工智能解决方案时，都必须考虑到八项主要原则。这些原则及其具体说明不会取代适用于人工智能解决方案从业者的任何其他或更严格的数据保护法规。主要原则是：

(a) 法域；

(b) 道德和法律依据；

(c) 数据基础；

(d) 责任和监督；

(e) 控制；

(f) 透明度和“可解释性”；

(g) 数据主体的权利；

(h) 保障措施。

法域

28. 为了创造法律确定性和可追溯性，理想情况下，应该有一个反映国际共识的跨国框架，其中应包含识别和监管人工智能解决方案中的责任以及管理已知风险的机制。

29. 鉴于没有这样的跨国框架，一种选择是就地制定解决方案和保障措施，并就地执法。在这种情况下，如果人工智能解决方案使用分布式决策机制，该分布式机制也应位于单一法域。

30. 其他选择是签订双边或多边协议；或在一个法域就地监管，但通过跨境安排提供便利；抑或，如果人工智能继续在市场力量的作用下实施，并有可能决定监管，则可制定消费者法律或其他形式的补救办法。

31. 除非制定用于解决信通技术中法域问题的专门特设国际法机制，特别是针对在一个法域开发、但在另一个法域使用的人工智能解决方案，如果某一人工智能解决方案必须在多个法域运作，则应该作为单一法域单个人工智能解决方案的多国联盟加以实施和运作。

道德和法律依据

32. 由于处理人们的个人数据总是侵犯数据主体的权利，因此人工智能解决方案背后的数据处理必须有良好的道德和法律依据。如果处理过程本身旨在促成或做出影响数据主体的地位或权利的决定，那么这一点就变得更加重要。无论法域或管理者的个人法律环境如何，以下一种或多种情况可能会为人工智能系统的数据处理提供充分的法律依据：

(a) 如果一部法律是按照民主原则和人权起草的，且能够解决管理者和数据主体之间的利益冲突，并为保护数据主体的权利提供适当保障，那么它就可以提供具体的法律依据；

(b) 如果使用人工智能解决方案是履行与数据主体的某一合同所必需的，得到了他们的明确同意，且合同没有对数据主体造成重大不利影响或侵犯数据主体或其他人的人权；

(c) 如果数据主体对人工智能的目的、使用人工智能的后果和收回同意的程序表示了自由知情同意。同意必须通过具体行动作出，负责任的管理者必须制定同意管理系统，允许随时收回同意，并包括足够的文件；

(d) 基于管理人的合法、普遍利益和/或重大社会利益，如果数据主体在数据处理开始之前得到了充分的信息，并有机会反对数据处理，或至少有权在合理的时间内查阅现有机制或程序，或补救他们的情况；

(e) 每个人工智能解决方案都受到其最初设计、实施和正确记录的目的的约束和限制。虽然这并不妨碍其他或补充用途(如进一步处理)或由另一管理者使用，但需要重新评估进一步使用的法律依据和保障措施，包括看似兼容的目的；

(f) 设立了特殊条件，以保护属于特殊、敏感或脆弱类别的数据主体，如儿童、囚犯或其他群体，并为将人工智能解决方案应用于这些数据主体提供法律依据。

数据基础

33. 数据质量包括准确性(如及时性和非歧视)以及数据最小化和目的限制。应该解决数据保护要求以及处理特定数据(如与健康有关的数据或儿童数据)的任何额外要求。

责任和监督

34. 在一个组织内部，每个人工智能解决方案都需要一个法人或自然人对数据处理及其结果负全责。这涵盖了过程和技术管理的方方面面，包括数据处理的合法性、记录、改编、结果、算法数据集的可信可验证性、处理、洞察力考虑和协作以及履行数据主体的权利。如果人工智能解决方案分布到该组织以外，则需要确定、记录和商定后续各方的责任。

35. 这些责任，包括人工智能解决方案的最终处理者，必须是透明的，数据主体以及公共监督当局和监管机构必须能够充分查阅。

36. 要进行适当的治理，特别是在较大的法人实体中，可以设立数据隐私官一职，其职责和职能包括就遵守数据隐私要求提供建议，并监测人工智能解决方案的实施。必须为数据隐私官一职提供足够的资源，并为其赋予足够的权力，以履行上述职能。担任这一职位的人应接受全面、适当的培训，或具备有效、独立履行职责和任务的资格(无论是通过认证，还是基于经验)。强烈鼓励在这一职位与相关监督或监管机构之间建立有效的沟通渠道。在较小的国家和初创企业，也需要对人工智能治理进行投资，无论治理是否包括设立这样一个职位。

37. 有关这些问责安排的信息应公之于众。

38. 需要一个独立、称职的监管机构进行监督，也需要对违反相关法律的行为提供司法补救。

控制

39. 人工智能解决方案，包括从第三方采购的解决方案，必须在相关管理者的完全控制下。从最初的设计构想到最终的关闭和停用，必须清楚人工智能解决方案处理了哪些数据，哪些参数和数据质量指标为决策提供了依据，以及它们将如何相互平衡和加权。必须持续监测结果，并在必要时进行纠正。在自动化决策解决方案领域，任何决策都不能基于有意识或无意识的偏见。在系统推出之前及其整个生命周期内，必须定期检查和纠正可能存在的偏差和歧视性影响。

40. 如果将人工智能用于决策支持系统，则决策者需要一组类似的控制机制。

41. 管理者(必要时可与处理者一道)必须能够随时停止或更改数据处理。错误结果必须记录在案，采取的纠正措施也必须记录下来，以减轻对数据主体造成的任何风险。一旦为查明、纠正或取证目的完成对错误结果的使用，必须立即予以删除。

42. 应对此类控制的运作情况进行内部和外部审查，并且必须能够处理有关人工智能解决方案或其结果的任何重大发现。

透明度和“可解释性”

43. 人工智能解决方案必须对公众和数据主体透明。这些信息必须是有意义的、可理解的，并涵盖与评估解决方案和数据主体可能的权利有关的所有方面。这包括目的的“可解释性”、总体功能、辅助流程、使用的数据来源和预期结果的范围。这些方面可能包括：

(a) 用于导入和训练人工智能解决方案的数据源和数据，以及人工智能解决方案产生的数据；

(b) 数据处理的目的和法律依据；

(c) 构筑人工智能决策基础的参数及其权重；

(d) 澄清人工智能解决方案旨在为人作出最终决策做准备(决策支持)，还是人工智能解决方案自己作出最终决策(自动化决策)；

(e) 数据管理者和处理者(如果不是同一人)之间的职责如何分配，以及联系方式和可能的沟通渠道；

(f) 纳入第三方(例如，其他数据管理者或处理者)、转移到其他国家(如有)以及纳入和转移的原因。还需要一份声明，声明第三方与管理者遵守同样的要求，如数据保护要求，并具有类似的角色和责任，无论他们身在何处；

(g) 必须至少在涵盖该人工智能解决方案的数据隐私政策中发布必要信息，并且必须是可访问、可理解和与数据主体相关的。

数据主体的权利

44. 如果一些个人或群体(数据主体)的个人信息或可识别的个人信息由人工智能解决方案处理，则他们应有权：

(a) 理解和查询，以便以明晰的形式确定个人数据是否存储在自动数据文件中；如果是存储在自动数据文件中，其目的是什么；哪些公共当局或个人或私人机构控制或可能控制其文件；

(b) 如果曾表示同意，且同意被用作数据处理的法律依据，应可以在处理过程中随时撤回同意而不产生负面后果；

(c) 如果数据处理是基于合法利益，则应可以随时以正当理由反对数据处理；

(d) 获取关于满足本节列出的所有数据隐私要求的信息；

(e) 成比例地获取他们的数据，包括有关其个人数据、如何使用和处理其个人数据、结果以及结果可能如何影响其地位和个人权利的全面书面信息；

(f) 如果他们有正当理由怀疑人工智能解决方案提出或做出的决定不准确或不正确，则可请求某个人做出决定；

(g) 如果数据不准确，应予以更正；

(h) 提出申诉，如申诉成立，应可获得补救；

(i) 如果人工智能解决方案的原有目的不再存在，或者如果数据不再需要用于另一合法目的，应有权删除和清除数据。

45. 这些权利不凌驾于其他权利和/或超越数据主体在特定法域根据适用法律享有的权利。

保障措施

46. 人工智能解决方案应以稳健的方式运作，并应通过适当的风险防范措施来确保其安全，使用的方法应有助于促进相关各方(包括数据主体和公众)的信任和理解。在部署之前，所有人工智能解决方案，即使只是测试性的，也必须至少开展一次初步人权和数据保护风险评估，以确定与预期解决方案相关的具体风险和关键度。取决于初步评估的结果，可能需要进一步评估权利和风险。

47. 必须使用“通过设计保护隐私”方法，逐个单独评估旨在减轻已查明风险的技术和组织保障措施。这应该包括匿名或假名、加密、客户端分离、访问管理(限制)、删除政策以及日志和活动监控等措施。

48. 在风险评估期间，必须审查技术、架构和/或结构方面的发展动态(如分布式计算)带来的新风险和挑战。

49. 可使用国际标准缓解风险，如国际标准化组织和国际电工委员会在 ISO/IEC 27000 系列(信息安全管理系统)中联合发布的标准。具体而言，ISO/IEC 27701 载有数据隐私扩展，至少为以下目的规定了相关措施：

(a) 防范：制定控制措施，防范已评估风险的影响；

(b) 发现：制定应对措施，尽快发现异常情况；

(c) 应对：制定控制措施，遏制和消除异常事件的风险，并确保在找到整体解决方案和情况恢复正常之前核心业务流程仍可正常运行。

B. 人工智能解决方案的关键度评估

50. 要采取的措施必须以人为本，并与侵犯人权(特别是歧视)和侵犯数据保护的风险以及数据处理解决方案的复杂性或关键度相称。以下列出了一些适当的方法。

在规划阶段开展人权评估

51. 所有人工智能解决方案都必须尊重法治、人权、民主价值观和多样性。因此，每一个规划中的人工智能解决方案，包括算法，都应该接受及时的人权评估，包括道德和平等性评估。规划中的人工智能解决方案不得非法侵犯享有平等待遇的权利。例如，人工智能解决方案使用反映出无意识偏见的信息，将导致可能会对社会中某些个人或群体造成歧视的结果。此外，即使向人工智能解决方案提供的信息是“正确的”，也可能会导致“错误的”结果，因为从收集到的信息衍生出的人工智能解决方案的学习可能会造成人工智能解决方案的错误假设。

52. 要实现通过设计保护隐私以及默认保护隐私，就必须在规划阶段评估人工智能解决方案的实施可能会给任何人权(包括隐私权)带来何种影响。

测试和矫正阶段——监测

53. 在规划阶段和初步人权评估之后，必须在进一步发展阶段考虑已确定的框架条件。在实施阶段和上线之前，人工智能解决方案必须经过密集测试阶段，应将测试数据另行置入自成一体的环境中，以评估是否不仅考虑了基本的一般假设，而且还满足了这些假设。只有在负责任的管理者能够确信人工智能解决方案正常运行的情况下，方可启动该解决方案的线上运作。

54. 在人工智能解决方案的整个运行时间内，直至最终关闭，必须对照规划阶段界定的基本要求，监测人工智能解决方案产生的结果。

55. 由于难以控制算法操作的所有方面，且人工智能解决方案运行期间算法不断变化，因此必须以另一种可行的方式不断对照解决方案的初始预期目的对结果进行检查，以提供一个比较基点。如果怀疑存在偏差或观察到偏差，则必须相应地调整人工智能解决方案的数据传输，否则必须停用解决方案。

56. 为从新的创造性方法中获益，并拓宽开发人员和管理者的视野，需要将隐私工作从业者、跨部门、跨行业、民间社会和用户社区的输入和反馈纳入人工智能解决方案的开发、测试和监测。必须为准备好运作的人工智能解决方案建立测试设施，例如，通过在互联网上安装所谓的黑匣子，将单独的、自成一体的解决方案向第三方开放，它们可以输入数据，以确定人工智能解决方案将产生的结果类型，或者由监管机构在参与制定人工智能解决方案的组织内实施沙箱。

基于不同类型数据的用途进行关键度评估

57. 除了妥善规划、测试和实施外，数据的关键度和预期目的也与适当处理数据所需的措施有关。

58. 这适用于一般数据，如一般个人信息或电信服务或健康方面的数据。相较于不那么敏感的个人信息，处理与健康有关的数据和其他一些信息(例如电子通信的内容)时，必须更加严格。这意味着，相对于其他情况，必须加强相关的技术和组织措施，例如，严格限定目的和数据最小化、加密、假名、限制访问和及早删除或匿名。

59. 数据的预期用途在确定所需的保护级别方面发挥着关键作用。如果处理个人信息纯粹是为了存储目的，则其关键度就低于画像用途。必须非常仔细地评估目的的正当性和保障措施。

60. 在所有风险评估期间，必须采取上述行动并将其记录在案。

对人工智能系统进行定期评估和记录，并向外部审计和监管机构提供记录

61. 评估范围涵括系统的以下方面：

(a) 预期或非预期的结果；

(b) 对个人和群体的公平性、偏见和歧视；

(c) 利弊及如何减轻弊端。

C. 其他考虑因素

外部审计和认证

62. 审计和认证计划应能够查阅所有相关的内部文件，如评估日志，以监测人工智能系统遵守使用多方利益攸关方和多边办法制定的工程和道德标准的情况。

63. 应考虑对在数据隐私方面获得核可、同时也被正式认可为具有人工智能专业知识的审计师进行外部认证。这可能有助于缓解公众和数据主体的担忧。它可能特别适用于可能导致重大不良后果和导致公众和/或监管界对其失去信任的人工智能解决方案。

法律法规的改变

64. 世界范围内正在考虑修改法律法规，这将影响大多数人工智能解决方案。是否合规在很大程度上将取决于：

(a) 是否能够达到现有和新兴的国内和国际标准；

(b) 是否能够由根据国内或国际协议运作的适当认证机构加以认证。

参与讨论

65. 人工智能战略和/或运作人工智能解决方案的负责人，以及监测其使用的人，应该参与有关人工智能和新出现的道德和技术问题的讨论。

教育和宣传

66. 人工智能是一个复杂的主题，要在人工智能系统中部署和使用数据，就必须向用户和数据提供者以及参与人工智能解决方案及其运营决策的高管、经理和其他人做出明确、全面的解释。仅公布算法是不够的。

二. 关于儿童隐私权的原则和建议

67. 儿童和所有人一样有权享有人权和自由。国际和区域法律文书阐明了隐私权和儿童隐私权。[3]

68. 载有儿童权利的主要文书是《世界人权宣言》和《儿童权利公约》，它们已获得 193 个缔约方的批准，因此几乎得到普遍接受。

69. 《公约》第 16 条规定：

(1) 儿童的隐私、家庭、住宅或通信不受任意或非法干涉，其荣誉和名誉不受非法攻击。

(2) 儿童有权享受法律保护，以免受这类干涉或攻击。

[3] 它们包括区域文书，如《非洲儿童权利和福利宪章》(1990 年)和《欧洲行使儿童权利公约》(1996 年)，以及区域体系，如美洲人权体系。

70. 该条款必须作宽泛解释，以充分考虑到儿童的隐私体验。[4]

71. 儿童的权利具有普遍、不可分割、相互依存和相互关联性。[5] 隐私权使他们能够获得对培养个性和人格至关重要的其他权利，如表达和结社自由权以及健康权等。[6] [7] 儿童的隐私关系到他们的身心完整、作决定方面的自主权、个人身份、信息隐私和物理/空间隐私。

72. 未来的智力生活、情感生活和性生活的基础是在童年和青春期发展起来的，并受到私人生活条件的影响。[8] 在世界各地，童年经历和隐私权不尽相同。[9] 种族等交叉因素影响着童年的构建。[10]

73. 一般来说，有助于儿童个性形成的领域是家庭和家庭生活、学校和社会网络。与儿童权利一样，这些领域是相互关联的，反映了背后的结构性因素。

74. 无家可归的儿童，如无人陪伴的儿童、街头儿童、“非家庭环境”照料中的儿童、冲突地区和其他脆弱处境中的儿童，在获得人权方面面临着更多的挑战。[11]

75. 虽然隐私权对不同的人有着不同的意义，但特别报告员强调隐私权的积极和促进性的方面，它涉及到人与生俱来的尊严，并促进其他人权的享有。[12]

76. “自决”的意思是个人有能力决定是否以及在多大程度上公开其个人生活的各个方面。[13] 自主性是指在思想、感觉和行动上自我指导的能力。“儿童”一词是指不满 18 周岁的个人。

确定问题

矛盾的利益

77. 考虑儿童的隐私权和人格权如何引发自主性，就是审查这些权利所处的种种矛盾和不同视角。

[4] John Tobin and Sarah M. Field, “Article 16: The right to protection of privacy, family, home, correspondence, honour, and reputation”, in *The UN Convention on the Rights of the Child: a commentary*, John Tobin, ed. (Oxford, Oxford University Press, 2019).

[5] 儿童权利委员会，第 16 号一般性意见(2013 年)，第 12 段。

[6] 联合国人权事务高级专员办事处(人权高专办)中东和北非区域办事处提交的材料(未获准发布材料)。

[7] 国际图书馆协会联合会提交的材料，第 2 页。在获得授权的情况下，为回应特别报告员的磋商而提交的材料将公布在以下网址：www.ohchr.org/EN/Issues/Privacy/SR/Pages/CFI_Privacy_and_Children.aspx。

[8] 比利时残疾论坛提交的材料，第 2 页。

[9] InternetLab 和 Alana 研究所；澳大利亚维多利亚州信息专员办公室提交的材料。

[10] Rebecca Epstein, Jamila Blake and Thalia González, “Girlhood interrupted: the erasure of black girls’ childhood”, Georgetown Law Center on Poverty and Inequality, 2017.

[11] 马特和平、发展和人权基金会提交的材料，第 7 页。

[12] 见大会第 68/167 号决议，人权理事会第 20/8 号决议和 A/HRC/13/37。

[13] Abstract of the German Federal Constitutional Court’s judgment of 15 December 1983, 1 BvR 209, 269, 362, 420, 440, 484/83 [CODICES].

78. 《儿童权利公约》规定缔约国和父母有能力和义务在必要时根据儿童不断发展的能力来判定其享有第 16 条所载权利的情况(第 5 条)，以确保儿童的最大利益(第 3 条)。[14]

79. 传统上，儿童的隐私权一直被认为是一个由成年人决定的问题。然而，儿童的隐私需求不同于成人的隐私需求，而且可能与成人的隐私需求相冲突。[15] 例如，“晒娃”可能会使父母的表达自由权与孩子的隐私权发生冲突。[16]

80. 成年人对儿童隐私需求的解读会阻碍儿童的自主性和独立性的健康发展，以保护的名义限制儿童的隐私。[17] 成年人依靠监视来保护儿童就是一个很好的例子。它限制了儿童的隐私权和自主权，但儿童越来越多地受到政府、私营部门、父母、家庭和同龄人的技术监视。[18] 父母的监视随着孩子年龄的增加——也就是当年轻人变得(或应该)变得更加独立的时候——而增加，而不是减少。[19] 照顾有额外需求的儿童的父母和照料者倾向于采取甚至更具保护性的立场，包括高默认隐私设置，并希望能够决定他们孩子的在线隐私。[20]

81. 父母的行为可能会与父母公开表示的担忧相矛盾。据报道，在 13-17 岁青少年的父母中，57%的人担心孩子接收或发送露骨图片，[21] 85%的人担心孩子的数字隐私。然而，只有不到三分之一的父母在孩子的设备上使用家长设置，81%的父母在知情的情况下允许孩子使用针对普通观众的 YouTube，而不加以监督。[22]

82. 最近的一项研究表明，没有经历过网络伤害(如暴力威胁或网上喷子)的成年人更有可能希望限制信息获取和在线匿名，这说明需要开展以证据为基础、以儿童为中心的风险评估、决策和监管。[23]

[14] Tobin and Field,“Article 16”.

[15] 家长权利基金会提交的材料；加拿大促进性健康和权利行动组织提交的材料，第 4 页；国家信息技术与自由委员会提交的材料，第 11 页。

[16] 南澳大利亚州儿童和青年事务专员提交的材料(其中“晒娃”一词被解释为父母和准父母越来越倾向于使用互联网在网上发布孩子的信息，这在孩子有能力表示同意或开始创建自己的数字足迹之前很久就形成了孩子的在线身份)，第 3 页。

[17] 国际儿童权利中心和民辩组织提交的材料。

[18] 同上；Jane Bailey and Valerie Steeves, *Defamation Law in the Age of the Internet: young people's perspectives* (Law Commission of Ontario, Canada, 2017)；爱丽尔国际基金会提交的材料。

[19] 南澳大利亚州儿童和青年事务专员提交的材料。

[20] 见 www.ofcom.org.uk/__data/assets/pdf_file/0023/190616/children-media-use-attitudes-2019-report.pdf.

[21] Monica Anderson “A majority of teens have experienced some form of cyberbullying”, Pew Research Center, 27 September 2018.

[22] ACT/应用程序协会提交的材料。

[23] BT/DEMOS, “Online harms: a snapshot of public opinion” (2020).可查阅 https://demos.co.uk/wp-content/uploads/2020/10/Online-Harms-A-Snapshot-of-Public-Opinion-1.pdf。

83. 随着孩子的成熟，他们渴望并需要隐私，不仅包括免于学校、企业和政府的侵扰，也包括免于父母的侵扰。[24] 这种需要随着孩子的成长而增长。5 岁到 7 岁的儿童一般不认为父母监控他们的网络活动是侵犯隐私的行为，但 15 岁到 17 岁的青少年通常担心家长和学校的监控。[25] 青少年认为，免于评判和监视的隐私和私人空间使他们能够探索想法和创造性表达，并形成独立的见解。[26] 家长的控制需要与儿童不断发展的能力和观点相称。[27]

个人身份

84. 如今的儿童是出生在数字时代的第一代人，[28] 而他们的父母则是养育出“数字儿童”的第一代人。[29]

85. 父母和家人越来越多地在网络上分享宫内影像，因此孩子的身份在出生前就开始了。许多此类影像都嵌入了个人信息。

86. 儿童数字身份基本是通过家人的行动形成的，贯穿整个童年时期，生活在西方发达国家的儿童之中，80%在两岁之前就有了数字足迹。[30] 儿童影像也在未经同意的情况下被用于慈善筹款。[31]

87. 现在，儿童参与网络活动的方式多种多样，而且起始年龄也比以前更小。[32] 他们使用社交媒体的比例在 9 到 10 岁和 11 到 12 岁之间会经历阶段性的变化，从 34%倍增至 69%。[33] 在七年级到十一年级之间，儿童的在线联系人数量翻了一番。[34] 许多 13 岁以下的儿童拥有社交媒体账户(根据欧洲的调查，9-12 岁的儿童中，38%拥有社交媒体账户)，[35] 其中大多数人拥有 2-5 个平台的账户。[36] 冠状病毒病(COVID-19)大流行加剧了这一趋势，2020 年 3 月到 9 月，Facebook 儿童版 Messenger 的日活跃账户增长了 350%。[37]

---

[24] 未来隐私论坛；爱丽尔国际基金会提交的材料。

[25] 全球隐私大会数字教育工作组提交的材料，第 25 页。

[26] 澳大利亚维多利亚州信息专员办公室提交的材料。

[27] 国家信息技术与自由委员会提交的材料，第 11 页。

[28] 加拿大人权委员会提交的材料，第 2 页。

[29] Danah Boyd, “Social network sites as networked publics: affordances, dynamics, and implications”, in *A Networked Self: Identity, Community, and Culture on Social Network Sites*, Zizi Papacharissi ed. (Routledge, 2011).

[30] 匈牙利国家数据保护和信息自由管理局提交的材料，第 42 页。

[31] 国际儿童权利中心和民辩组织提交的材料；克罗地亚儿童事务监察员提交的材料，第 3 页。

[32] 联合王国信息专员办公室；国家信息技术与自由委员会；阿尔巴尼亚信息和数据保护专员提交的材料。

[33] 拉丁美洲和加勒比经济委员会(拉加经委会)提交的材料。

[34] 匈牙利国家数据保护和信息自由管理局提交的材料，第 29 页。

[35] 同上，第 53 页。

[36] 阿尔巴尼亚信息和数据保护专员提交的材料，第 14 页。

[37] Facebook 提交的材料。

88. 形成个性和身份所必需的自尊和自我概念越来越以数字化的形式被构建。[38] 儿童使用互联网对他们的生活进行持续报道，社交媒体上的红心和点赞成为他们思想的附属品，[39] 但他们担心失去对其线上信息的控制。[40]

89. 数字生活中，暴力、性虐待和网络欺凌屡见不鲜，尤其是对于年轻的 LGBTQI 人群而言(见 A/HRC/43/52)。在 13 到 17 岁的青少年中，约 25%的人报告说，他们曾在未经同意的情况下收到过露骨图片。[41] 约 29%的女孩和 20%的男孩报告说，有人在未征求他们意见的情况下主动向其发送露骨图片。未经同意向儿童发送和发布图片，即使这些图片客观上不会造成伤害、冒犯或尴尬，也会损害儿童的自尊心、自主权、人际关系和社会心理发展。[42]

90. 儿童性虐待，无论是线下还是线上，都是对身体完整性和做决定方面的自主权的侵犯。它对个性和能力有长期的影响，而儿童性虐待资料在网上的持续存在加剧了这些后果。虐待的形式和后果根植于社会对儿童及其身体的看法。[43] 打击此类虐待行为需要基于人权的战略。[44] 年轻人浸润在不断扩展的数字技术中，产生了持续不断的数据流，这些数据通过人工智能、机器学习应用程序以及面部和语音识别技术得以收集和增强。儿童和他们的数据推动了数字世界的业务。[45] 到 2021 年，面向儿童的在线广告市场价值可达 17 亿美元，在线广告公司在儿童 13 岁之前为每个儿童收集的数据超过 7,200 万条。[46]

91. 营销人员接触、影响年轻人，并与之建立持续的关系。年幼的儿童特别容易受到定向营销的影响，因为他们不区分广告和内容，不区分虚构和现实，也不理解广告的诱导性质。[47] 纳入了行为技巧(诱导设计/暗箱操作)的技术可以最大限度地提高参与度，触发冲动行为，影响决定的作出，造成被排除在外的担忧，并压倒隐私方面的关切。[48]

[38] Anna Bunn 提交的材料，第 11 页；澳大利亚维多利亚州信息专员办公室提交的材料，第 2 页。

[39] 爱丽尔国际基金会提交的材料。

[40] C. Mahieu；澳大利亚维多利亚州信息专员办公室；国家信息技术与自由委员会提交的材料。

[41] Monica Anderson,“A majority of teens have experienced some form of cyberbullying”.

[42] Bunn；Mahieu 提交的材料。

[43] InternetLab 和 Alana 研究所提交的材料。

[44] 消除对妇女歧视委员会，第 38 号一般性建议(2020 年)；马特和平、发展和人权基金会提交的材料，第 7 页。

[45] Shoshana Zuboff, *The Age of Surveillance Capitalism* (Profile Books, 2019)；InternetLab 和 Alana 研究所提交的材料。

[46] 国家信息技术与自由委员会提交的材料，第 3 页。

[47] 无广告童年运动和数字民主中心；InternetLab 和 Alana 研究所；国家信息技术与自由委员会提交的材料。

[48] 联合王国信息专员办公室；澳大利亚维多利亚州信息专员办公室；Mahieu；美国大学 Jonathan Crock 等人；国家信息技术与自由委员会；拉加经委会提交的材料。

92. 对儿童进行画像限制了他们在童年、青春期甚至可能成年后的潜在自我发展，因为行为预测和助推技巧可以预先决定选项和选择。需要对照儿童权利和最大利益对技术产品进行评估，[49] 因为儿童个人数据的处理可能：

(a) 侵犯隐私和数据保护，包括丧失自主性和个人声誉受损；

(b) 损害儿童的精神和心理健康及身体健康；

(c) 造成经济损害或商业剥削。[50]

93. 儿童和青年寻求能够尽量减少企业获取和使用其数据的对策；[51] 商业活动的分区；以及处理他们最大利益的机制，包括删除发布材料的能力。[52] 儿童认为他们应能行使其权利，向任何公司索要其个人数据副本，约 40%的儿童认为他们应能在任何年龄提出查阅或删除请求，21%的人表示 13 岁或 13 岁以下即可提出上述请求。只有 13.5%的人认为须年满 18 岁才能提出查阅或删除请求。[53]

94. 数字时代有利于儿童的发展。然而，儿童必须能够享有不受阻碍地发展个性的权利，而不受商业行为的侵害。

95. 据报，在南美洲，使用生物特征监控和跟踪技术发现和监测被怀疑有不当行为的儿童；且在司法程序中未能保护儿童隐私。[54] 识别执法当局关注的儿童或被监禁父母的子女或与恐怖主义有关联的父母的子女有违隐私权，导致成见和歧视，并损害个性的发展。[55] 尽管共享数据可能会造成问题，特别是与安保人员共享数据，[56] 但是不向有关支持部门查明这些儿童，也同样有可能限制他们的发展。[57]

性、性别、身体完整性和身体自主权

96. 儿童在身体、智力、社交和情感能力方面有极大的差异。这种差异在青春期尤为明显，青春期的特点是身体、认知和社交能力急剧变化，包括性和生殖系统的成熟。[58]

---

[49] 加拿大人权委员会提交的材料，第 2 页；澳大利亚维多利亚州信息专员办公室；无广告童年运动和数字民主中心提交的材料。

[50] 联合王国信息专员办公室提交的材料。

[51] Valerie Steeves, “Young Canadians in a wired world, phase III: trends and recommendations”, MediaSmarts, 2014.

[52] eQuality 提交的材料。

[53] 全球隐私大会提交的材料，第 24 页。

[54] InternetLab 和 Alana 研究所提交的材料。

[55] 儿童权利委员会，第 24 号一般性意见(2019 年)。

[56] 欧洲囚犯子女协会；“外面的家人”组织；国际被监禁父母子女联盟；贵格会联合国办事处提交的材料。

[57] 联合国毒品和犯罪问题办公室(禁毒办)，“关于被恐怖和暴力极端团体招募和剥削的儿童的手册：司法系统的作用”(维也纳，2017 年)，第 138-139 页；联合国，反恐怖主义办公室，“受外国战士现象影响的儿童：确保基于儿童权利的方法”(2019 年)，第 103 页。

[58] 儿童权利委员会，第 4 号一般性意见(2003 年)。

97. 性表达、身体完整性和身体自主权是儿童隐私相互交织的肌理的一部分，也是他们表达自由的一部分。[59] 青少年需要能够就其健康和身体做出决定，并随着他们的成熟安全而私密地探索性取向，[60] 无论是线下还是线上。[61]

98. 然而，儿童的身体完整性和自主权受到政府、商业实体、医疗和其他专业人员、父母和同龄人的行为的侵犯。发现的侵权行为包括：[62]

(a) 女童遭受女性生殖器切割；强迫婚姻；强迫性行为；强迫怀孕和生育；强制孕检；强制绝育；被剥夺生殖性信息和服务；获得处方避孕药具和堕胎必须通知父母和/或征得其同意；“矫正”疗法；对同龄人之间双方同意的性行为施以刑事处罚，包括发送性短讯；线上和线下的性虐待；“名誉”杀人；“荡妇羞辱”；

(b) 男童遭受割礼；强迫婚姻；强迫性行为；强制绝育；被剥夺生殖性信息和服务；“矫正”疗法；对同龄人之间双方同意的性行为施以刑事处罚，包括发送性短讯；线上和线下的性虐待；骚扰；体罚；

(c) 性别认同、性取向和性表达各异、性征不同的儿童遭受暴力侵害；歧视和骚扰；对其性别认同或身体的病理化；不必要的医治；公布生殖器官的详细资料；污名化；“指示”强奸；“矫正”疗法；不给予特定保健服务，包括跨性别者医疗保健服务及生殖性信息和服务；不准查阅医疗档案；对同龄人之间双方同意的性行为施以刑事处罚，包括发送性短讯；线上和线下的性虐待；性别不受法律承认。

99. 侵犯身体隐私会影响其他权利，如《儿童权利公约》第 3、第 6、第 8、第 12、第 16、第 19 和第 29 条第 1 款规定的权利。例如：[63]

(a) 强制孕检侵犯了女孩的尊严、平等和自主权；

(b) 查明生理性别/社会性别多样学生的调查侵犯了不受歧视的权利，如被用来开除学生，则侵犯了他们的受教育权；

(c) 通常由父母强制进行的“自愿”贞洁检测侵犯了女孩的尊严、平等和自主权；

(d) 高度医疗化的程序意味着，需要进行手术，性别方可获得法律承认，这影响到健康权；[64]

(e) 获得性健康或生殖健康服务必须征得父母同意或通知父母，影响到健康权、身份权、生命权、免受伤害的权利和儿童的最大利益。

[59] Matimba；欧洲委员会；澳大利亚人权委员会提交的材料。

[60] 国际人权中心提交的材料。

[61] ParentsTogether 提交的材料。

[62] Crock 等人；人权观察；国际男女同性恋协会欧洲分会、跨性别者欧洲协会和国际男女同性恋、双性恋、跨性别者、性别奇异者和间性者青年和学生组织；荷兰性别多样性组织；“选择：青年与性”组织；公开行动国际；澳大利亚人权委员会；国际人权中心；欧洲委员会提交的材料。

[63] 国际间性者组织欧洲区提交的材料。

[64] Matimba；A. McCarthy 提交的材料。

100. 儿童需要并有权获得关于健康的性关系、同意和安全做法方面的指导。[65] 全面的性教育可以帮助儿童保护和提高他们的隐私、独立性和自主性，[66] 并促进他们的福祉，特别是对 LGBTQI 青少年来说。[67] 据报道，在世界各地，包括巴西、多米尼加共和国、加纳、肯尼亚和波兰，都出现了反弹，反对向儿童和青少年提供全面的性教育。[68]

身份的承认

101. 所有人都有权利，正是因为他们作为人具有与生俱来的平等身份。[69] 档案和档案保管系统确立官方身份，[70] 但很少就儿童的档案给予其能动性。

102. 官方身份始于出生登记。然而，世界各地的许多儿童没有登记，特别是在原住民和土著社区中。[71] 法律不予承认影响了获得自主性所必需的许多权利，例如受教育权。

103. 对于跨性别和间性儿童、通过国际代孕安排出生的儿童、失踪儿童、无人陪伴的难民儿童和非家庭环境照料中的儿童来说，出生证可能对获得尊严、身份、隐私和发展构成挑战。[72]

教育和入学

104. 教育的目的是最大限度地发展儿童的个性、才华和身心能力。[73] 教育是一项人权，是儿童过上有尊严生活的基本手段。教育通过保护儿童免受剥削，赋予他们作为个人和集体以权能。受教育权要求各国通过消除性别禁令和暴力等教育障碍，尊重、保护和实现这一权利。[74]

105. 学校在儿童的日常隐私体验中发挥着重要作用。宣布新冠病毒病大流行之后，截至 2020 年 4 月 1 日，193 个国家关闭了学校，影响到全球大约 90%的学生人口。[75]

---

[65] 儿童权利委员会，第 15 号一般性意见(2013 年)；经济、社会及文化权利委员会，第 22 号一般性意见(2016 年)；澳大利亚人权委员会提交的材料；Mahieu 提交的材料；生殖权利中心提交的材料，第 1 页。

[66] 加拿大性健康和性权利行动；国际男女同性恋协会欧洲分会、跨性别者欧洲协会和国际男女同性恋、双性恋、跨性别者、性别奇异者和间性者青年和学生组织提交的材料。

[67] McCarthy 提交的材料。

[68] 人权观察提交的材料，第 18 段。

[69] Dinah Shelton, “On identity”, *The George Washington International Law Review*, vol. 39 (1999).

[70] “在档案设计中纳入权利”项目、莫纳什大学和联邦大学提交的材料；D.Z.诉荷兰(CCPR/C/130/D/2918/2016)。

[71] 澳大利亚人权委员会提交的材料。

[72] 澳大利亚人权委员会提交的材料；“在档案设计中纳入权利”项目、莫纳什大学和联邦大学提交的材料；Kathryn Allan and David Lacey, “Identity management in disaster response environments: a child exploitation mitigation perspective”, *Australian Journal of Emergency Management*, vol. 33, No. 3 (July 2018)。

[73] 《儿童权利公约》，第 29 条第 1 款(a)项。

[74] 大会第 75/166 号决议。

[75] ParentsTogether 提交的材料。

106. 与 2019 年末每周平均下载量相比，目前在线教育应用的下载量增长了 90%。[76] 向在线教育的转变加剧了教育技术公司与儿童之间以及政府与儿童和家长之间现有的权力失衡，几个国家的政府豁免了现有的儿童数据隐私法。例如，在威尔士，政府豁免了要求家长和学生同意的规定。[77] 在其他地方，公立学校中，对孩子的隐私权没有保护。[78] 然而，非国家行为体通常控制着儿童的数字教育记录。[79]

107. 儿童学习数据的数字化和存储包括思维特征、学习轨迹、参与度分数、反应时间、阅读页数和观看的视频。[80] 大多数儿童和家长没有能力挑战教育技术公司的隐私安排，也没有能力拒绝提供数据，因为教育是义务的。[81]

108. 学校对应用程序和网上学习工具的选择侧重于课程和财务方面的考虑，而不是隐私。[82] 2020 年 9 月，对 22 个国家的 496 个教育技术应用程序进行了分析，发现许多应用程序正在收集设备标识符，27 个应用程序正在获取位置数据，123 个手动测试的应用程序中有 79 个正在与第三方(如广告合作伙伴)共享用户数据。[83] 数据安全令人担忧。例如，微软报告称，2020 年 8 月 24 日至 9 月 24 日期间，发生了 570 万起恶意软件事件，影响了其教育软件的用户。[84]

109. 学校本身拥有儿童的大量信息，并通过监控学生的在线活动和监控摄像头越来越多地跟踪儿童。[85] 与教育技术应用一样，使用这种技术需要问责、真正意义的同意、目的限制、数据最小化、透明度和安全保障。[86]

110. 无论在哪里或以何种方式进行教育，教育进程不需要、也不应该破坏隐私权和其他权利的享有，[87] 同时也不应该加剧现有的不平等。[88]

---

[76] 人权观察提交的材料，第 44 段。

[77] 同上，第 48 段。

[78] 南澳大利亚州儿童和青年事务专员提交的材料。

[79] 见 https://rm.coe.int/educational-settings/16809f3ba3。

[80] 全球隐私大会提交的材料，第 4 页。

[81] DefendDigitalMe；欧洲委员会提交的材料。

[82] 澳大利亚维多利亚州信息专员办公室提交的材料。

[83] Alfred Ng, “Education apps are sending your location data and personal info to advertisers”, CNET, 1 September 2020.

[84] 人权观察提交的材料，第 49 段。

[85] 南澳大利亚州儿童和青年事务专员提交的材料。

[86] InternetLab 和 Alana 研究所；巴西福塔莱萨大学技术、信息和社会研究组；布宜诺斯艾利斯自治市监察员；欧洲委员会提交的材料。

[87] 儿童权利委员会，第 1 号一般性意见(2001 年)；大会第 75/166 号决议；DefendDigitalMe；布宜诺斯艾利斯自治市监察员；巴西福塔莱萨大学技术、信息和社会研究组提交的材料；匈牙利国家数据保护和信息自由管理局，案号 NAIH/2020/7127/。

[88] 大会第 75/166 号决议；布宜诺斯艾利斯自治市监察员；拉加经委会；欧洲委员会提交的材料。

适龄性和不断发展的能力

111. “适龄”一词被普遍认为是年龄与行为之间的一致性，也是年龄与儿童可获得的服务(如在线内容)的一致性。监管意义上的适龄性是衡量在线提供商提供的服务是否适合儿童年龄的一项标准。大不列颠及北爱尔兰联合王国的《适龄设计规范》就是最近的一个例子。[89] 在美利坚合众国，1998 年的《儿童在线隐私保护法》对针对 13 岁以下儿童的网站运营商和在线服务以及知道自身在收集 13 岁以下儿童个人信息的其他网站运营商和在线服务提出了要求。

112. 然而，适龄机制不是万能药，因为：

(a) 资料可能是适龄的，但仍然对儿童及其权利有害。从个人的角度来看，这种机制可能会保护儿童并为其赋权，但考虑到同龄儿童在智力和情感发展方面存在相当大的差异，这种机制可能无法满足一群儿童的需要；[90]

(b) 作为一个通用的门槛，适龄性对不同能力的儿童造成不公平，是对他们不断发展的能力的粗略衡量，潜在地限制了他们个性的发展和自主行使权利，而且可能具有歧视性；

(c) 当年龄成为获得服务的标准时，需要可核实的身份证件，这引起了人们对安全、指令性做法以及缺乏年龄保障标准、工具和行业认证计划的关切。[91] 另有人表示，年龄验证程序可以通过符合隐私的方式实现。[92]

113. 将年龄作为评估儿童能力的唯一准绳一直备受诟病。[93] 一些国家承认能力并不取决于年龄。[94] 2020 年初，加拿大安大略省当局出台了一项立法，允许年轻人明确根据能力、而不是年龄获取他们的个人信息，并请求予以修改。如发生冲突，应优先考虑儿童的权利，而不是父母或监护人的决定。[95]

114. 儿童是否准备好作决定并自我承担责任，最好不是由年龄决定，而是由情境决定，包括风险和可获得的支持、个人经验、受影响的权利以及理解其行动(或不采取行动)产生的影响的能力。例如，在决定儿童何时有能力就处理其个人数据表示同意时，必须考虑他们对数据处理的实际了解、他们的最大利益、权利和观点。[96]

---

[89] 见 https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2020/01/ico-publishes-code-of-practice-to-protect-children-s-privacy-online/。

[90] 儿童权利委员会，第 7 号一般性意见(2005 年)。

[91] 国家信息技术与自由委员会提交的材料，第 10 页；Facebook 提交的材料。

[92] Yoti 提交的材料。

[93] 见 www.dataprotection.ie/sites/default/files/uploads/2019-09/Whose%20Rights%20Are%20They%20Anyway_Trends%20and%20Hightlights%20from%20Stream%201.pdf。

[94] 全球隐私大会提交的材料，第 20 页。

[95] 同上，第 25 页。

[96] 欧洲委员会提交的材料。

115. 从本质上讲，适龄性概念与不断发展的能力的原则之间存在某种矛盾。需要更多地探索如何根据儿童不断发展的能力调整服务。

备选解决方案

116. 最大限度地保护儿童的隐私是为他们的最大利益行事的重要手段。[97] 遵循最大利益的方法要求成年人积极征求并认真对待儿童的意见。这一点并不总是体现在国家、公司、父母和其他方面的行动中，[98] 但根据国际法，儿童被承认为人，而不仅仅是儿童，因此根据国际法，儿童有权享有人权。[99]

117. 所有各方——政府、公司、社区、个人和父母——都需要承认儿童是权利承担者。例如，要全面有效地打击信通技术所便利的虐待儿童行为，就需要采取基于人权的多方利益攸关方办法，让儿童、家庭、社区、政府、民间社会和私营部门积极参与进来。[100]

118. 虽然儿童的依赖性(亦即脆弱性)可能会导致风险，但风险并不等同于伤害，驾驭一些风险对于儿童培养韧性和应对技能是必要的。[101] 只根据儿童的脆弱性来定义儿童，而不考虑他们的能力或潜力，很可能会造成过度保护，因而可能有损儿童的个性。

保护儿童数据

119. 虽然隐私是一个更广泛、更复杂的概念，但数据保护与此密切相关。要培养人的个性自由发展，就必须防止个人数据被无限制地收集、存储、使用和共享。

120. 许多人认为同意是一个基础。然而，同意既不一定表达儿童的自主性，也不保护儿童的自主性，特别是在权力失衡的情况下。此外，父母的同意可能并不总是符合孩子的最大利益，也不一定与孩子的观点一致。[102]

121. 《欧洲通用数据保护条例》可以更好地保护儿童的个人数据，[103] 它要求为未成年人量身定做有关数据处理的信息，从而向未成年人提供特殊保护(第 12 条)；对儿童画像尤其保持警惕(叙述性部分第 71 条)；加强了被遗忘的权利(叙述性

[97] 禁毒办提交的材料。

[98] Promsex 提交的材料。

[99] John Tobin, “Understanding children’s rights: a vision beyond vulnerability”, *Nordic Journal of International Law*, vol. 84, No. 2 (June 2015).

[100] 禁毒办；Facebook 提交的材料。

[101] 南澳大利亚州儿童和青年事务专员提交的材料。

[102] 克罗地亚儿童事务监察员提交的材料，第 4 页。

[103] Simone van der Hof and Eva Lievens, “The importance of privacy by design and data protection impact assessments in strengthening protection of children’s personal data under the GDPR”, *Communications Law*, vol. 23, No. 1 (2018).

部分第 65 条)，第 8 条引入了 13 至 16 岁儿童对数据处理表示同意的能力。[104] 此外，通过设计进行数据保护的一般要素、默认保护隐私、不受自动化个人决策影响的权利(第 22 条)和数据保护影响评估值得加以更广泛地适用，以保护儿童个人数据。[105]

122. 《公约 108+》[106] 还规定不得单纯根据自动化数据处理作出决定(第 1 条(a)项)，欧洲委员会最近通过的“教育环境中儿童数据保护准则”扩大了个人数据处理的定义，以涵盖对具有共同特征的群体或个人的预测，并扩大了生物特征数据处理的定义，以涵盖这些类型的处理。[107]

隐私工程与数字素养

123. 技术设计有助于打击“诱导设计”和“暗箱操作”，[108] 推动实现法律法规的目标。[109]

124. 除了数字技术隐私工程，儿童和青少年还需要操作技能以及认知和社交能力，以便以经过深思熟虑、道德和安全的方式使用技术。数字素养教育可以从源头上防止有害网络行为。[110] 人们(包括儿童)广泛认同，数字素养可以打造他们的网络安全并培养其自主性，[111] 特别是考虑到儿童上网的年龄越来越小，父母难以提供有效支持。[112]

125. 然而，如果各国不采取严格和持续的行动来解决结构性不平等问题并确保儿童隐私、数据保护和安全，仅有技术解决方案和数字素养是不够的。[113] 各国有相当大的空间进行投资，以改善与民间社会、业界、学术界和儿童的伙伴关系，从而共同构建解决方案的原型。

---

104 在该年龄以下，数据处理需要征得父母或监护人的同意。

105 Van der Hof and Lievens,“The importance of privacy”.

106 《关于个人数据自动化处理的个人保护公约》，后经欧洲委员会条约汇编订正议定书第 223 号现代化。可查阅 https://rm.coe.int/convention-108-convention-for-the-protection-of-individuals-with-regar/16808b36f1。

107 欧洲委员会提交的材料。

108 无广告童年运动和数字民主中心；国家信息技术与自由委员会提交的材料。

109 ACT/应用程序协会提交的材料。

110 Jane Bailey and Valerie Steeves, *eGirls, eCitizens: Putting Technology, Theory and Policy into Dialogue with Girls' and Young Women's Voices* (University of Ottawa Press, 2015); Jane Bailey and Jacquelyn Burkell, “Legal remedies for online attacks: young people's perspectives”, *The Annual Review of Interdisciplinary Justice Research*, vol. 9 (2020).

111 国际图书馆协会联合会；澳大利亚维多利亚州信息专员办公室；隐私未来论坛；欧洲委员会；澳大利亚人权委员会；Crock 等人提交的材料，第 5 页。

112 阿尔巴尼亚信息和数据保护专员；InternetLab 和 Alana 研究所提交的材料。

113 大会第 75/166 号决议。

三. 结论

126. 促进儿童的隐私和培养他们的自主性需要：

(a) 制定符合以下条件的政策、法律和法规：

(一) 将儿童视为人权的承担者，他们的隐私权、自主权和平等权是不可剥夺的；[114]

(二) 纳入广泛的隐私保护范围，而不仅仅是数据保护，以使儿童的潜力得到充分发挥；[115]

(三) 将儿童观点、儿童隐私战略、以儿童为侧重点的研究的结论和/或儿童隐私影响评估纳入公共政策环境；[116]

(四) 提供独立手段，对个别或系统侵犯儿童人权行为进行调解、仲裁和补救，[117] 并确保在发生侵权行为时采取执法措施；[118]

(b) 解决将儿童定位为脆弱和没有主观能动性的结构性情况；

(c) 鼓励技术创新，在保护儿童隐私的同时改善信息通信服务。[119]

四. 建议

127. 特别报告员建议各国：

(a) 确保政府立法、政策、决定、档案系统和服务以《儿童权利公约》关于隐私、个性和自主性的权利和价值为基础；

(b) 支持对儿童获取在线服务和其他服务的自主决定能力进行全面分析，确保基于证据制定专门针对儿童的隐私法律、政策和法规；

(c) 只有在没有更好的办法时，才以最谨慎的态度采用适龄标准作为监管工具；

(d) 针对面向儿童的产品和服务，促进并要求落实通过设计保证安全、通过设计保护隐私和默认保护隐私指导原则，确保儿童在隐私受到侵犯时能够获得有效补救；

(e) 鼓励与民间社会和业界缔结伙伴关系，共同创造符合儿童和青年最大利益的技术产品；

[114] Bailey and Steeves, *eGirls, eCitizens*.

[115] 南澳大利亚州儿童和青年事务专员；国际儿童权利中心和民辩组织；匈牙利国家数据保护和信息自由管理局提交的材料，第 58 页。

[116] 南澳大利亚州儿童和青年事务专员提交的材料；Bailey and Steeves, *eGirls, eCitizens*。

[117] 加拿大人权委员会提交的材料。

[118] 5Rights 基金会提交的材料。

[119] ACT/应用程序协会提交的材料。

(f) 通过特别报告员关于防止基于性别的侵犯隐私行为的建议(A/HRC/43/52，第 33-34 段)；

(g) 根据《儿童权利公约》第 29 条第 1 款和欧洲委员会“教育环境中儿童数据保护准则”，[120] 制定全面的在线教育行动计划；

(h) 确保为在线教育建立并维持适当的法律框架；

(i) 为非商业性的教育和社会空间创建公共基础设施；

(j) 弥补所有法律漏洞和程序例外，确保所有触犯司法系统的儿童在全部诉讼程序中始终保持隐私，终身不得公布任何刑事司法记录；

(k) 审查法律框架，使公司能够自愿采取行动，合法和相称地侦查在线儿童性虐待资料；

(l) 确保对与恐怖团体或暴力极端团体有关联的儿童的个人数据予以保密，且仅在为协调个人康复和重返社会之目的而严格必要的情况下进行共享；

(m) 在将民事和刑事身份数据库相链接之前开展人权影响评估，以评估对儿童及其隐私的影响，并开展协商，以评估生物特征监控的必要性、相称性和合法性；

(n) 制定惯例和法律，确保向媒体提供的信息不侵犯儿童隐私权；如儿童的父母触犯法律，确保媒体和其他机构的报道保护这些孩子的隐私；

(o) 如父母被监禁，确保在与其进行的所有接触中维护孩子的隐私，包括书面、电子和电话通信以及探监；

(p) 确保仅在合法、必要、相称和完全符合儿童权利的情况下才收集儿童的生物特征数据，且只能作为特例；

(q) 确保在有正当法律依据的前提下，使用能够代表最佳做法的数据保护框架，如《通用数据保护条例》和《公约 108+》，为特定目的公平、准确、安全地处理儿童的个人数据；

(r) 确保个人数据的处理者，包括父母或照料者和教育工作者，意识到儿童有权享有隐私和数据保护；

(s) 确保儿童可在数据保护当局的网站上获得有关如何行使权利的信息，并确保专门为儿童提供包括针对网络欺凌在内有关问题的咨询、投诉机制和补救措施；

(t) 确保在法律或实践中不禁止匿名、假名或儿童使用加密技术；

(u) 确保各种背景的儿童和青年都有机会参与针对他们的框架、政策和方案的决策和设计；

(v) 禁止为了作出有关儿童的决策，或分析或预测个人偏好、行为和态度，自动处理对儿童进行画像的个人数据；仅在特殊情况下，出于儿童的最大利益或压倒一切的公共利益，在拥有适当法律保障机制的情况下，方可予以豁免；

[120] 见 www.coe.int/en/web/data-protection/-/protect-children-s-personal-data-in-education-setting。

(w) 确保企业政策、管理决定和服务以《儿童权利公约》关于隐私、个性和自主性的权利和价值为基础；

(x) 落实《工商企业与人权指导原则：“保护、尊重和补救”框架》及其性别问题指导(A/HRC/41/43, 附件)；[121]

(y) 建立补救和申诉机制，同时确保这些机制不妨碍人们利用基于国家的机制；

(z) 就报告关切事项(包括投诉)、补救和申诉机制提供可理解的信息；

(aa) 采取合理、相称、及时和有效的措施，确保其网络和在线服务不被滥用于危害儿童的犯罪目的或其他非法目的；

(bb) 与执法部门合作，支持对犯下侵害儿童罪行的人进行法律识别和起诉。

今后的工作

128. 今后有关隐私与儿童工作的紧急优先事项包括：

(a) 在国际上开展工作，制定设计指导框架，以保护在线活动中儿童的隐私；

(b) 在国家访问期间和专题报告中吸收儿童参与儿童隐私问题；

(c) 研究父母监控规范及其对儿童成长的影响。

[121] 另见 www.ohchr.org/Documents/Issues/Business/Gender_Booklet_Final.pdf。

Annex I

Overview of activities

The key achievements of the mandate since 2015 include:

A. Detailed thematic reports and recommendations on:

Big data and open data, A/72/540 (2017) and A/73/438 (2018)

Health-related data, A/74/277 (2019)

Privacy and gender, A/HRC/40/63 (2019)

Artificial intelligence and privacy, and children's privacy, A/HRC/46/37 (2021)

B. Security and surveillance

The establishment of the International Intelligence Oversight Forum, which met in Bucharest (2016), Brussels (2017), Valletta (2018) and London (2019).

The draft legal instrument on government-led surveillance, while not progressed, has increasingly been demonstrated as needed and a useful reference for future work.

Networks have been established through the use of working parties, consultations and involvement of regional human rights bodies/entities, particularly in Europe.

Discussions with and specific recommendations to intelligence agencies, police forces and/or Governments of Member States concerning reinforcement of safeguards and remedies, including legislation regarding surveillance, encryption and independent oversight authorities.

Intensive work on complaints of infringement of privacy by Julian Assange and President Lenin Moreno, including preparation of interim reports.

The Special Rapporteur presented a report to the Human Rights Council on governmental surveillance activities from a national and international perspective, A/HRC/34/60 (2017).

The Special Rapporteur presented a report to the General Assembly on the implications of the COVID-19 pandemic for the right to privacy, A/75/147 (2020).

Communications to Member States

Since 2015, 101 communications have been issued to Member States concerning practices that appeared inconsistent with the right to privacy. Thirty were issued in 2020 (see annex II).

Visits and events

The COVID-19 pandemic prevented any official country visits during 2020.

Country visits were undertaken in: the United States of America in 2017 (A/HRC/46/37/Add.4); France in 2018 (A/HRC/46/37/Add.2); the United Kingdom of Great Britain and Northern Ireland in 2018 (A/HRC/46/37/Add.1); Germany in 2018 (A/HRC/46/37/Add.3); Argentina in 2019 (A/HRC/46/37/Add.5) and the Republic of Korea in 2019 (A/HRC/46/37/Add.6).

During 2020, the Special Rapporteur continued to promote privacy via online events, including the forty-second International Conference of Data Protection and Privacy Commissioners and multiple civil society organization and non-governmental organization events.

Taskforces

Security and surveillance

The annual International Intelligence Oversight Forum 2020 was postponed due to the COVID-19 pandemic. However, collaborative networks were maintained. The Special Rapporteur continued to work with various countries and their intelligence agencies on the upgrading of laws regulating surveillance and encryption. More detailed laws are needed to protect encryption and thereby, the privacy of communications.

Taskforce on corporations' use of personal data

The Special Rapporteur held five taskforce meetings attended by civil society organizations and leading corporations. The dialogue was highly productive, addressing issues including identity verification, European Court judgments concerning cross border movement of data, artificial intelligence, and privacy and children.

The taskforce's recommendation on artificial intelligence is provided in the main text of the present report. The draft was provided for international consultation, to which 28 submissions were received.

Taskforce on privacy and personality: children

The Special Rapporteur worked independently yet collaboratively with the Committee on the Rights of the Child on new guidelines to protect children's privacy. He also provided feedback to the Committee on its draft general comment No. 25.

The Special Rapporteur released a call for contributions on how privacy affects the development of personality, particularly the evolving capacity of the child and the growth of autonomy. Contributions were sought from interested parties on research, consultations with children and good practice mechanisms. Nearly 60 submissions were received. The principles and recommendations are included in the main body of the present report.

Annex II

Communications on the right to privacy

Communications (joint and from the Special Rapporteur on the right to privacy alone) on the right to privacy sent, and replies received, between 1 June 2015 and 1 January 2021

TIME PERIOD: Sent and Responses Received	*TYPE of COMMUNICATION*						
	Joint Urgent Appeals	*Joint Allegation Letters*	*Joint Other Letters*	*SRP Urgent Appeals*	*SRP Allegation Letters*	*SRP Other Letters*	*Total*[a]
2015–2020 Sent	6	60	19	0	5	11	101
2015–2020 Responses	4[b]	51[c]	10[d]	0	7[d]	5	77[a]
2020 Sent	1	22	5	0	0	2	30
2020 Responses	0	16[e]	4[f]	0	0	2	22[a]

Source: OHCHR communication database, https://spcommreports.ohchr.org/TmSearch/Results.

Abbreviation: SRP, Special Rapporteur on privacy.

[a] The number of replies received is not equal to the number of matters raised, as some replies included more than one response.

[b] Two Joint Urgent Appeals received two responses each.

[c] 44 responses to Joint Allegation Letters included six matters which received two responses, and one matter received a total of three responses, making a total of 51 responses from Member States.

[d] Two replies consisted of two responses.

[e] One reply included three responses.

[f] One reply consisted of two responses.