



人权理事会

第五十四届会议

2023年9月11日至10月13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

人权理事会 2023年10月12日通过的决议

54/21. 数字时代的隐私权

人权理事会，

遵循《联合国宪章》的宗旨和原则，

重申《世界人权宣言》、《公民及政治权利国际公约》、《经济社会文化权利国际公约》和其他相关国际人权文书所载的人权和基本自由，

回顾大会和人权理事会以往关于数字时代隐私权的所有决议，以及其他相关决议，

欢迎联合国人权事务高级专员办事处就数字时代隐私权问题开展的工作，又欢迎人权理事会各特别程序任务负责人关于隐私权的工作及其对促进和保护隐私权所作的贡献，

重申人的隐私权，即任何人的私生活、家庭、住宅或通信不得受到任意或非法干涉，并有权受法律保护免遭这种干涉，并确认隐私权的行使对于实现其他人权，包括自由表达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十分重要，是民主社会的基础之一，

认识到隐私权与有效保护每个人的个人数据存在内在联系，

又认识到隐私权可以使人享有其他权利，自由发展个人的个性和身份以及个人参与政治、经济、社会和文化生活的能力，

申明人在线下享有的权利，包括隐私权，同样必须在线上得到保护，并注意到线上和线下空间的加速同步会影响到个人，包括他们的隐私权，

注意到线上的算法或自动决策过程可能会影响线下个人权利的享有，



认识到需要以国际人权法为基础，进一步讨论和分析与促进和保护数字时代隐私权、程序性保障、国内有效监督和补救、监控对享有隐私权及其他人权的影响有关的问题，还需要审查与监控做法有关的非任意性、守法性、合法性、必要性和相称性原则，并考虑潜在的歧视性影响，

注意到技术的迅猛发展使世界各地的人都能使用信息和通信技术，同时也增强了政府、工商企业和个人开展监控、拦截、黑客攻击和收集数据的能力，这些做法可能侵犯或践踏人权，尤其是隐私权，因而是一个日益令人关切的问题，

又注意到在数字时代侵犯和践踏隐私权的行为可能影响到所有人，尤其影响到妇女、儿童、残疾人和老年人，以及处境脆弱者和边缘化群体，处理个人数据，特别是处境脆弱者的数据，必须遵守人权保障措施和限制，

还注意到妇女和女童的隐私权在线上和线下都受到针对性别的侵犯和践踏，以及带有性别影响的侵犯或践踏，认识到许多数字平台的设计、商业化、维护和管理方式可能导致虚假信息、错误信息和仇恨言论，从而加剧性别成见，造成性暴力和性别暴力，破坏数据保护，影响妇女和女童实现所有权利，特别是隐私权，

指出儿童的隐私权特别容易受到践踏和侵犯，包括受到网络欺凌、网络跟踪以及性虐待和性剥削，又指出缔约国必须在数字环境方面执行《儿童权利公约》，隐私对于儿童的能动性、尊严和安全以及对于儿童行使权利至关重要，

承认在构思、设计、使用、获取、转让、出售、部署和进一步开发新技术和新兴技术，如涉及人工智能的技术时，需要开展人权尽责工作，因为如果没有适当的保障措施，这些技术可能会影响隐私权和其他人权的享有，并承认能够而且应该避免或尽量减少这些权利面临的风险，为此可采取措施确保安全、透明、可问责、有保障和高质量的数据基础设施，开展尽责管理并对已部署技术进行定期审查，以评估、预防和减轻对人权的不利影响，提供包括司法补救在内的有效补救和纠正机制，并建立人为监督，

认识到使用数字技术和人工智能系统，尽管有积极作用，但需要处理大量数据，而且往往涉及个人数据，包括个人行为、社会关系、私人喜好和身份等数据，包括元数据，因此可能对隐私权构成严重风险，特别是在用于对个人进行识别、追踪、特征分析、面部识别、行为预测或评分的时候，

注意到使用数据提取和算法将内容精准推送给在线用户，可能会损害用户能动性和在线获取信息的机会以及意见和表达自由权，还会使错误信息、虚假信息 and 仇恨言论的威胁加剧，特别是在社交媒体平台上，进而可能导致暴力，包括政治暴力，就此回顾《关于禁止构成煽动歧视、敌意或暴力的鼓吹民族、种族或宗教仇恨言论的拉巴特行动计划》，

关切地注意到数据收集做法的侵入性和影响、监控所产生的相关影响和危害，以及在人工智能系统的应用上越来越多地使用算法的现象，

又关切地注意到某些预测算法以及越来越多地使用面部识别和监控技术有可能导致歧视，特别是在算法训练使用的数据不准确、不相关、不具代表性且没有经过编码偏见审计的情况下，

注意到在没有人权保障措施的情况下使用人工智能，有可能加剧歧视，包括加剧结构性不平等，处理敏感数据时尤为如此，并认识到在设计、开发、实施和使用新的和新兴数字技术时必须防止出现种族歧视和其他类型的歧视性结果，

关切地注意到有报告显示生物数据识别技术，包括表现出种族特征偏差和对妇女带有偏见的面部识别技术，准确性较低，包括在使用了不具代表性的训练数据的情况下，注意到使用数字技术可能复制、强化甚至加剧种族和性别不平等，并认识到这方面有效补救措施的重要性，

承认虽然元数据可带来益处，但某些类型的元数据汇总后可以泄露敏感度不低于实际通信内容的个人信息，还可能暴露个人的行为举止，包括行踪、社会关系、政治活动、个人喜好和身份等，因此回顾指出，服务提供商应采取步骤，尽量减少、隐藏或删除元数据，降低用户元数据的可追踪性，以加强加密保护并保护隐私权，

认识到缺乏获取负担得起和可靠技术和服务的机会仍是许多发展中国家面临的一项严峻挑战，尤其是在弥合数字鸿沟，包括国家之间和国家内部的数字鸿沟及性别数字鸿沟方面，以及在加速推进各种形式的发展，包括实现可持续发展目标方面，就此强调指出全世界许多国家，包括发展中国家在内，都需要获得支持以弥合上述数字鸿沟，实现可持续发展目标，

又认识到需要通过开展人权影响评估等方式，确保在数据驱动技术的构思、设计、开发、部署、评价、监管和技术标准制定方面遵守国际人权法，并确保这些技术受到充分的保障和监督，

表示关切的是，随着个人数据，包括敏感数据的收集、处理、使用、储存和共享在数字时代显著增加，个人尤其是儿童，往往不会也(或)不能对自己数据的收集、处理和储存或对自己个人数据的再次使用、出售或多次转售做出自由、明确和知情的同意，如果个人敏感数据遭到泄露，可能会对个人造成格外严重的损害、伤害或困难，

特别指出对数字通信的监控必须符合国际人权义务，必须依据法律框架进行，这个框架必须公开、清晰、精确、全面且无歧视，指出对隐私权的任何干涉都必须符合合法性、必要性和相称性原则，铭记哪些是追求合法目标的合理方式，并回顾《公民及政治权利国际公约》缔约国必须采取必要步骤，通过必要的法律或其他措施，以落实《公约》中确认的权利，

深为关切地注意到，在许多国家，参与促进和维护人权和基本自由的个人及组织、记者、其他媒体工作者可能由于其从事的活动而频繁面临威胁和骚扰，安全无保障，隐私权也遭到非法或任意干涉，

又深为关切地注意到，私营或公共行为体利用私人监控行业开发的技术工具进行监控、使用恶意软件或间谍软件等方式侵入设备和系统、拦截和中断通信、收集数据，干扰个人包括那些从事促进和维护人权和基本自由的个人、记者和其他媒体工作者的职业和私人生活，侵犯或践踏他们的人权，特别是隐私权，

回顾如《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》所述，包括技术公司在内的工商企业有责任尊重人权，回顾促进和保护人权和基本自由的义务和主要责任在于国家，并欢迎高级专员办事处就这些原则在数字技术方面的应用所做的工作，

强调数字时代保障和保护数字通信机密性的技术解决方案，包括加密、假名化、匿名等措施，对于确保人们享有人权，尤其是隐私权、意见和表达自由权、和平集会和结社自由权十分重要，并认识到各国必须推广此类措施，避免使用非法或任意监控技术，其中可能包括各种形式的黑客攻击以及限制获取和使用加密技术，

强调指出，需要确保国家安全和公共卫生措施，包括利用技术监测和遏制传染病的传播，完全符合国家根据国际人权法承担的义务，符合守法性、合法性、目的正当性、必要性、相称性原则，在应对公共卫生突发事件或其他紧急情况时必须保护人权、包括隐私权以及个人数据，又强调一旦收集的数据不再符合收集目的，需要删除或匿名处理，

1. 重申《世界人权宣言》第十二条和《公民及政治权利国际公约》第十七条所述隐私权，这项权利是指任何人的私生活、家庭、住宅或通信不得受到任意或非法干涉，并有权受法律保护免遭这种干涉；

2. 回顾国家应确保对隐私权的任何干涉符合合法性、必要性、相称性原则；

3. 又回顾新技术和新兴技术，例如监控、人工智能、自动化决策和机器学习，以及特征分析、追踪和生物识别，包括面部识别等领域开发的这些技术，在没有人权保障的情况下，越来越影响到隐私权和其他人权的充分享有，承认某些应用程序可能不符合国际人权法；

4. 申明人们在线下享有的权利同样必须在线上得到保护，包括隐私权；

5. 又申明为了保护、尊重和促进隐私权，只应出于具体、明确和合法目的收集个人数据，而且必须以合法、公平和透明的方式处理这些数据；

6. 重点指出人人均应能够确定有哪些公共机关或个人或私人机构控制或可以控制其个人数据，对数据保护的任何干预必须具有合法性，符合国际人权法，包括合法性、相称性、必要性和不歧视原则；

7. 承认在构思、设计、使用、获取、转让、出售、部署和进一步发展人工智能等新的和新兴数字技术方面，可以而且应当依照适用的国际人权法义务，采用适当条例或其他适当机制，尽量减少对隐私权和其他人权造成的风险，为此应确保安全、有保障和高质量的数据基础设施，开展尽责管理以评估、预防和减轻对人权的不利影响，并建立人为监督和纠正机制；

8. 强调指出，在收集、处理、分享、储存个人数据时，国家必须遵守人权义务，包括技术公司在内的工商企业应尊重隐私权和其他人权，特别是采取数据保护政策和保障措施；

9. 又强调指出，由于侵扰性强且广泛影响到大量人口，远程生物识别监控系统，包括面部识别，在相称性方面引发了严重关切；

10. 促请所有国家：

(a) 尊重和保护隐私权，包括在数字通信以及新的和新兴数字技术方面；

(b) 采取措施制止侵犯和践踏隐私权的行为，并创造条件防止此类侵犯和践踏行为，包括确保相关国家法律符合国际人权法规定的义务，尤其是在涉及处境脆弱者或边缘化群体的情况下；

(c) 定期审查关于包括大规模监控及拦截和收集个人数据的在内的通信监控的程序、做法和立法，以及关于使用特征分析、自动化决策、机器学习和生物识别技术的程序、做法和立法，以期通过确保充分和切实履行国际人权法规定的所有义务维护隐私权；

(d) 在拦截个人数字通信和(或)收集个人数据时、在分享或以其他方式提供通过信息和情报共享协议等途径获取的数据时、在要求包括工商企业在内的第三方披露个人信息时，遵守国际人权义务，包括尊重隐私权；

(e) 确保为打击恐怖主义和助长恐怖主义的暴力极端主义而采取的任何干涉隐私权的措施都符合合法性、必要性和相称性原则，并符合国际法规定的义务；

(f) 确保生物识别和确认技术，包括公共和私人行为体的面部识别技术，不会带来任意或非法监控，包括对行使和平集会自由权的人进行监控；

(g) 确保数字或生物识别方案的设计、实施和运作具备适当的技术、监管、法律和道德保障措施，并完全符合各国根据国际人权法承担的义务；

(h) 依照国际人权法，制订或保持和执行适当的立法，其中应规定有效的处罚和补救措施，保护个人隐私权免遭侵犯和践踏，即个人数据免遭他人、政府、工商企业或私营组织未经当事人的自由、明确和知情同意而进行收集、处理、保留或使用，除非另有合法原因；

(i) 考虑通过或保持符合本国国际人权义务的、包括数字通信数据在内的数据保护立法、条例和政策，内容可包括关于保护敏感个人数据的规定，设立拥有权力和资源的独立的国家主管机构，负责监督数据隐私做法，调查违规和侵权行为，接收个人和机构来文，并提供适当的有效补救；

(j) 考虑通过或审查立法、条例或政策，以确保所有工商企业，包括社交媒体企业和其他在线平台，将隐私权和其他相关人权充分纳入包括人工智能在内的各项技术的设计、开发、部署和评估，采取适当措施加强和鼓励企业承担责任，并向权利可能遭到侵犯或践踏的个人提供有效补救，包括赔偿和保证不重犯；

(k) 在这方面进一步制订或保持针对数字时代侵犯和践踏隐私权行为的预防措施和补救措施，这些行为可能影响所有个人，包括可能特别影响到妇女、儿童、处境脆弱者或边缘化群体；

(l) 制定、审查、实施和加强有助于增强所有妇女和女童的权能、促进和保护所有个人在数字时代的隐私权、考虑到性别层面的政策和方案；

(m) 就如何尊重人权向工商企业提供有效和最新的指导，就人权尽责管理等适当方法以及如何切实考虑性别、脆弱性和(或)边缘化问题提供建议，并考虑采取适当措施，使工商企业能够就国家当局提出的获取私人用户数据和信息的请求采取适当的自愿透明度措施；

(n) 避免以不符合国际人权义务的方式使用监控技术，包括避免以不符合国际人权义务的方式对人权维护者、记者和其他媒体工作者使用，并采取具体行动保护隐私权不受侵犯，包括为此对监控技术的出售、转让、使用和出口实行监管；

(o) 促进所有人享有无障碍、包容性的优质教育和终身教育机会，通过提供在线安全培训、指导和提高认识等方式，培养有效保护自身隐私所需的数字和数据素养及技术技能，并确保相关利益攸关方能够在这一领域获得适当培训；

(p) 避免要求工商企业采取任意或非法干涉隐私权的举措，保护个人免受伤害，包括工商企业通过收集、处理、储存、共享数据和特征分析以及使用自动化程序和机器学习造成的伤害；

(q) 加强努力，打击使用人工智能系统造成的歧视，包括为此开展尽责管理，以评估、预防和减轻部署这些系统对人权造成的不利影响；

11. 鼓励所有工商企业，特别是收集、储存、使用、共享和处理数据的工商企业：

(a) 审查其商业模式，确保其设计和开发流程、业务运营、数据收集和数据处理做法符合《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》，强调必须对其产品，特别是对算法和排名系统的作用开展人权尽责管理；

(b) 以明确、适龄、便于理解，包括便于残疾人理解的方式向用户通报可能影响隐私权的用户数据收集、使用、共享和保留情况，避免在未经用户同意或缺乏法律依据的情况下采取上述做法，并制定能让用户作出自由、知情和有效同意的透明制度和政策；

(c) 将隐私权和其他相关人权纳入内部决策、产品工程、业务发展、员工培训和其他相关内部进程；

(d) 实行政治、技术和物理保障措施，以确保合法处理数据，确保就处理目的而言这种处理是必要的，确保处理目的的正当性以及处理过程的准确性、完整性和保密性，防止未经授权披露或使用数据；

(e) 确保个人能够访问自己的数据，并有可能修改、更正、更新、删除数据以及就其数据的使用撤回同意，尤其是在数据不正确或不准确，或者数据是非法获得或用于歧视目的的情况下；

(f) 确保将对隐私权和其他相关人权的尊重纳入自动化决策和机器学习技术的设计、操作、评估和监管，并对这种决策和技术造成或助长或牵涉到的践踏人权行为提供有效的补救，包括赔偿；

(g) 建立适当的保障措施，设法防止或减轻与自身业务、产品或服务直接相关的不利人权影响，包括在必要时通过合同条款进行保障，并在发现其产品和服务受到滥用时，迅速向相关的国内、区域或国际监督机构通报侵权或违规行为；

(h) 加强努力，打击使用人工智能系统造成的歧视，包括开展人权尽责管理，对人工智能系统开展全生命周期监测和评价，并监测和评价部署这种系统对人权的影响；

(i) 提高算法决策、自动化系统和人在回路系统的透明度和充分可解释性，确保用于算法训练的数据具有代表性且属于合法收集；

(j) 制定适当的保障措施，确保组织内部和组织之间的数据分发和传输和(或)数据重组，包括通过云计算、非结构化数据集、区块链技术、增强现实和物联网进行的分发、传输和重组，符合数据保护和隐私权的要求；

(k) 在人工智能系统和数字技术的整个生命周期，包括在开始设计和开发涉及个人数据处理的应用程序和软件之前，采取适当措施，以期建立一个风险监测和管理系统，确保公平合法地处理数据；

12. 鼓励工商企业，包括通信服务提供商，努力开发能够确保和保护数字通信和交易保密性的解决方案，包括加密、假名化和匿名措施，并确保实施符合人权的保障措施，吁请各国推广强加密、假名化和匿名措施和技术解决方案，不干涉此类技术解决方案的使用，这方面的任何限制都应符合国家根据国际人权法承担的义务，并颁布保护个人数字通信隐私的政策；

13. 鼓励各国并在适用情况下鼓励工商企业，在构思、设计、开发、部署或出售或获取和运作人工智能系统的整个生命周期内系统地开展人权尽责管理，包括定期进行全面的人权影响评估，并让所有相关利益攸关方参与其中；

14. 鼓励所有相关利益攸关方在构思、开发和执行数字技术及相关政策时纳入性别平等视角，并促进妇女参与，以便应对因为使用技术而发生或加剧的对所有妇女和女童的暴力和歧视，为此鼓励数字技术公司包括互联网服务提供商遵守标准，落实透明和便捷的报告机制；

15. 请联合国人权事务高级专员办事处编写一份报告，说明在隐私权领域的歧视和不平等享有方面与数据收集和处理有关的挑战和风险，包括本决议所述挑战和风险，确定并澄清相关的人权原则、保障措施和最佳做法，并将报告提交人权理事会第五十七届会议，随后举行互动对话；

16. 又请高级专员办事处在编写上述报告时，征求不同地域的利益攸关方的意见并考虑到它们已做的工作，这些利益攸关方包括国家、国际和区域组织、人权理事会特别程序、条约机构、联合国其他相关办事处、机构、基金和方案(在其各自任务范围内)、国家人权机构、民间社会、私营部门、技术界和学术机构。

2023年10月12日

第48次会议

[未经表决获得通过。]