联 合 国 A/HRC/51/17

大 会

Distr.: General
4 August 2022
Chinese
Original: English

人权理事会
第五十一届会议
2022 年 9 月 12 日至 10 月 7 日
议程项目 2 和 3
联合国人权事务高级专员的年度报告以及
高级专员办事处的报告和秘书长的报告

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

# 数字时代的隐私权

## 联合国人权事务高级专员办事处的报告*

概要

本报告是根据人权理事会第 48/4 号决议提交的，讨论了隐私权方面的最新趋势和挑战。报告特别侧重于：(a) 侵入性黑客工具的滥用；(b) 加密对确保享有隐私权和其他权利的关键作用；(c) 广泛监控公共场所。报告强调部署无处不在的监控系统的危险，可能破坏充满活力和尊重权利社会的发展。

* 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。

# 一. 导言

1. 本报告是根据人权理事会第 48/4 号决议提交的，理事会在该决议中请联合国人权事务高级专员办事处(人权高专办)编写一份报告，说明隐私权方面的最新趋势和挑战，提出和澄清相关的人权原则、保障措施和最佳做法，将该报告提交理事会第五十一届会议。报告应反映人权高专办发出征求资料请求后收到的答复。[1]

2. 世界各地人民都看到了惊人的技术进步，以及改善人们生活和促进经济发展的创新成果。然而，他们也经历着数字工具如何掉转矛头，对他们进行新形式的监控、划线和控制的情况。确保尊重和保护《世界人权宣言》第十二条、《公民权利和政治权利国际公约》第十七条以及许多其他国际和区域人权文书所承认的隐私权，[2] 可以在管理人权面临的新数字威胁中发挥中心作用，这些威胁与驱动数字化社会引擎的个人数据密切相关。

3. 本报告在以前提交人权理事会的应对隐私权的各种挑战报告的基础上，[3] 着重论述国家保障和促进隐私权作用的三个显著趋势：(a) 侵入性黑客工具的广泛滥用；(b) 强加密对确保享有隐私权和其他权利的关键作用；(c) 对公共场所的广泛监控。本报告强调部署无处不在的监控系统的非常真实和蚕食性风险，最终可能扼杀充满活力、繁荣和尊重权利的社会的发展。报告最后提出避免这种后果的一系列建议。

# 二. 监控个人设备和通信

## A. 黑客攻击

4. 2021 年 7 月，在大赦国际支持下，新闻调查联盟“禁忌故事”(Forbidden Stories)披露了“飞马”(Pegasus）间谍软件的使用内幕，引起国际社会对多年来不断加剧的人权危机的关注，即定向秘密监控数字设备的黑客工具在全球扩散。这款本来为打击恐怖主义和犯罪而部署的间谍软件开始经常用于非法目的，包括镇压持有或表达批评或不同意见者，比如记者、反对派政治人物和人权维护者。

5. “飞马”间谍软件的使用范围和受害者数量是惊人的。根据一份包括 5 万多个潜在和实际监控目标的电话号码的泄露清单以及对大量受感染电话的犯罪学分析，2021 年的报告显示，至少有 189 名记者、85 名人权维护者和 600 多名政治家及政府官员，包括内阁部长和外交官成为目标并受到影响。[4] 调查还揭露了窥

[1] 见 https://www.ohchr.org/en/calls-for-input/2022/call-inputs-report-right-privacy-digital-age-2022.

[2] 见《儿童权利公约》第十六条；《保护所有移徙工人及其家庭成员权利国际公约》第 14 条；《残疾人权利公约》第二十二条；《非洲儿童权利与福利宪章》第 10 条；《美洲人权公约》第 11 条；《保护人权与基本自由公约》第 8 条。

[3] 见 A/HRC/27/37、A/HRC/39/29、A/HRC/44/24 和 A/HRC/48/31。

[4] 见 https://www.washingtonpost.com/investigations/2021/07/24/whatsapp-pegasus-spyware/.

探法官、律师、医生、工会领袖和学者的情况。[5] 制造和销售“飞马”的NSO集团承认，其目标是每年招揽 1.2 万至 1.3 万个人客户。[6]

6. “飞马”间谍软件是全球公司向各国政府推销的间谍软件中最突出的例子。[7] 据研究人员称，至少有 65 个国家政府购买了商业间谍软件监控工具。[8] NSO 报告称，其客户包括 45 个国家的 60 个政府机构。就在“飞马”事件曝光几天前，公民实验室和微软发布报告详细介绍另一款软件 Candiru 如何被政府用来监视人权维护者、持不同政见者、记者、活动人士和政治家。[9] 2021 年 11 月，社交网络公司 Meta 宣布，它取缔了 7 个通过互联网在 100 多个国家进行监控的实体帐号。该公司还提醒说大约有 5 万人可能是此类活动的目标。[10] 据报道，有 500 多家公司在开发、营销和向政府出售这种监控工具。[11]

7. 全球市场上出售的间谍软件工具和服务的能力令人生畏。例如，“飞马”一旦安装，就可以完全不受限制地访问受感染设备上的所有传感器和信息，有效地将大多数智能手机变成 24 小时监控设备，可以利用摄像头和麦克风、地理位置数据、电子邮件、消息、照片和视频以及所有应用程序。入侵者能够了解受害者详细生活情况以及思想、偏好、职业活动、政治思考、健康、财务状况、社会和私人生活。虽然许多黑客工具需要受害者采取一些行动，如点击链接或打开邮件附件，但“飞马”是通过所谓的“零点击攻击”秘密安装的。[12] 一旦受害者成为目标，该软件使他们几乎不可能避免感染。

8. 黑客行动可以采取多种形式，具有不同的侵入程度。获得对手机或电脑的完全控制有助于描绘出被攻击对象的详细生活画面，而各种其他黑客技术侵入性可能稍逊，尽管也很严重，比如只是进入电子邮件账户。黑客入侵还可以访问其他联网设备，如可穿戴技术设备或车辆，进而获取额外信息，包括健康和位置数据。配备摄像头或麦克风的设备，如智能扬声器或电视机，可以变成视听监控工

[5] 见 https://forbiddenstories.org/about-the-pegasus-project/; https://citizenlab.ca/2016/08/million-dollar-dissident-iphone-zero-day-nso-group-uae/; https://citizenlab.ca/2018/09/hide-and-seek-tracking-nso-groups-pegasus-spyware-to-operations-in-45-countries/.

[6] 2022 年 6 月 21 日，调查“飞马”和同等间谍监控软件使用情况的调查委员会在欧洲议会作证，详情可查阅：https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA.

[7] 见 https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf, 第 29 页。

[8] 见 https://carnegieendowment.org/2021/07/21/governments-are-using-spyware-on-citizens.-can-they-be-stopped-pub-85019.

[9] 见 https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/.

[10] 见 https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/. 其他例子见 https://citizenlab.ca/2020/06/dark-basin-uncovering-a-massive-hack-for-hire-operation/; https://www.eff.org/press/releases/saudi-human-rights-activist-represented-eff-sues-spyware-maker-darkmatter-violating; 和 https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

[11] A/HRC/41/35, 第 6 段；商业间谍软件全球清单可查阅：https://data.mendeley.com/datasets/csvhpkt8tm/2.

[12] 应该指出，Pegasus 软件并不是具有这些功能的唯一工具，这种工具的数量在增加。

具。攻击服务提供商的基础设施可以获得成千上万客户的大量信息，包括他们的通信、浏览数据和位置。[13] 以下段落主要讨论入侵个人通信设备问题。

9. 黑客攻击个人通信设备严重干涉隐私权，并可能侵犯一系列其他权利。入侵数字通信设备可以查阅草稿以及搜索和浏览记录，并有可能深入了解受黑客攻击者的个人思维过程以及政治和宗教观点与信仰，从而干涉其意见和思想自由。[14] 黑客行动可能造成严重伤害，影响受害者及其家人的心理健康。据报道，黑客行动导致人权维护者和政治家遭受逮捕和拘留，其中一些人受到酷刑。[15] 黑客定点攻击也与法外处决有关。[16]

10. 此外，针对记者和媒体使用黑客工具严重损害媒体自由，尤其因为信息来源可能害怕被发现和受到影响。黑客软件存在本身就可能对言论自由、媒体工作以及公共辩论和参与产生寒蝉效应，并可能侵蚀民主治理。用印度最高法院最近关于“飞马”软件使用案裁决中的话来说，监视的寒蝉效应将是“对媒体至关重要的公众监督作用的攻击”。[17]

11. 黑客行动也可能对正当程序权和公平审判权产生不利影响。[18] 侵入一台设备后，入侵者不仅可以观察到该设备内的内容和与其他设备的交互，还可以操纵该设备，包括更改、删除或添加文件。[19] 因此，伪造证据以指控或勒索目标个人是可能的。[20]

12. 此外，间谍软件不仅可以影响黑客攻击的目标，还可以影响与这些人通信的每个人。如果设备的摄像头、麦克风或地理定位功能被激活，还会影响同一物理位置的任何人。[21]

13. 最后，黑客依赖并利用计算机系统中存在的安全缺陷。通过让这些漏洞保持开放，甚至创造此种漏洞，那些诉诸黑客手段的人可能对数百万用户和更广泛的数字信息生态系统造成安全和隐私威胁。[22]

---

[13] 法国和荷兰警方的 EncroChat 调查成功侵入一个加密通信网络的服务器基础设施，收集了 121 个国家超过 3.2 万部电话的信息；见德国联邦法院，2022 年 3 月 2 日的裁决，5 StR 457/21，第 18 段。

[14] A/HRC/29/32，第 20 段；关于思想自由的全面分析，见 A/76/380。

[15] 见 https://theintercept.com/2016/12/08/phone-cracking-cellebrite-software-used-to-prosecute-tortured-dissident/.

[16] A/HRC/41/35，第 1 段；另见法外处决、即审即决或任意处决问题特别报告员的会议室文件，题为“特别报告员关于 Jamal Khashoggi 先生非法死亡调查报告的附件”，可查阅：https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/.

[17] 印度最高法院，Manohar Lal Sharma 诉印度联邦案，2021 年 10 月 27 日的判令，第 39 段。

[18] A/HRC/23/40，第 62 段。

[19] A/HRC/39/29，第 19 段。

[20] 这类指控的例子见 https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/.

[21] 见 https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf，第 8 页。

[22] A/HRC/39/29，第 19 段。

14. 人权机构和专家多年来一直就间谍软件发出警告。大会和人权理事会一再声明，会员国应避免使用非法或任意监控，包括黑客攻击。[23] 几位特别报告员对黑客行动表示强烈批评，这些行动远远超出了追求合法目标(如打击恐怖主义和犯罪)所必需的范围。[24] 人权事务委员会也表示关切国家支持的黑客行动，特别是在没有适当监督或保障情况下使用黑客行动。[25] 在区域一级，美洲人权委员会前言论自由问题特别报告员谴责为不允许的目的进行黑客攻击，并呼吁严惩犯罪者，包括出于政治原因对记者和独立媒体实施监控。[26]

15. “飞马”软件的使用被披露后，各区域和国家机构，包括欧洲委员会、美洲人权委员会、欧洲议会和印度最高法院，都对间谍软件的扩散表示关切，并启动了听证和调查。[27] 刑事调查[28] 和民事诉讼[29] 也在进行中。

16. 政府使用间谍软件的最低要求和必要保障的指南可以借鉴现有大量与监控相关的人权分析成果。[30] 由于黑客行动的深远不利影响，需要严格按照国际人权法要求，对其使用采取特别审慎做法，将其限制在最特殊情况。

17. 然而，许多司法制度还没有设置必要的法律护栏，也没有明确、准确、公开的法律来管理黑客行动。一些国家颁布了符合国际人权法的法律框架，而另一些国家则依赖现代技术出现之前颁布的过于宽泛或过时的法律。

18. 正如对“飞马”软件的披露和相关报告所显示的，各种国家行为者的黑客行动似乎常常追求有悖国际人权法的目标。虽然在某些情况下，为了保护国家安全或公共秩序，允许根据《公民权利和政治权利国际公约》第十七条和第十九条，

[23] 大会第 75/176 号决议和人权理事会第 48/4 号和第 45/18 号决议。

[24] A/HRC/17/27； A/HRC/20/17； A/HRC/23/40，第 62 段； A/HRC/41/35； A/HRC/41/41； A/73/438；另见 https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

[25] 见 CCPR/C/DEU/CO/7；CCPR/C/NLD/CO/5；CCPR/C/ITA/CO/6。

[26] 见 https://www.oas.org/en/iachr/expression/showarticle.asp?artID=998&lID=1.

[27] 见 https://www.oas.org/en/iachr/expression/showarticle.asp?artID=1207&lID=1; https://www.oas.org/en/IACHR/jsForm/?File=/en/iachr/media_center/PReleases/2022/022.asp; https://www.theguardian.com/world/2022/mar/17/pegasus-spyware-ban-el-salvador-iachr-hearing; https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; https://tvn24.pl/tvn24-news-in-english/polands-senate-lunches-special-committee-to-examine-use-of-pegasus-software-5557023; 印度最高法院，Manohar Lal Sharma 诉印度联邦案，2021 年 10 月 27 日的判令。

[28] 见 https://www.euronews.com/next/2021/07/20/paris-prosecutor-to-investigate-alleged-pegasus-hacking-after-complaint-by-french-journali; https://www.aljazeera.com/news/2021/7/22/hungary-prosecutors-open-investigation-into-pegasus-spying-claims.

[29] https://www.glanlaw.org/nso-spyware-hacking; https://privacyinternational.org/examples/2605/lawsuits-target-nso-group-selling-spyware-governments-targeting-activists-and; https://www.washingtonpost.com/technology/2021/11/23/apple-pegasus-lawsuit-spyware-nso/; and https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf. 所采取的法律行动概述见 https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

[30] 见 A/HRC/27/37；A/HRC/39/29；A/HRC/23/40 和 A/HRC/23/40/Corr.1；CCPR/C/UKR/CO/8；CCPR/C/DEU/CO/7；CCPR/C/ARM/CO/3；CCPR/C/BWA/CO/2；CCPR/C/FIN/CO/7。

采取侵入性的监视措施，但出于政治或商业目的的黑客行动永远是不正当的，当人权维护者或记者成为目标时，情况往往如此。

19. 即使是追求合法的目标，如国家安全或保护他人权利，评估间谍软件使用的必要性和相称性后发现，必须严格限制这类软件可允许使用的范围。[31] 有力论据表明，“飞马”等工具能够不受约束地侵入人们的生活，甚至进入人们的内心世界，可能影响隐私权的本质，[32] 干涉思想和意见自由这些绝对权利。鉴于使用间谍软件的巨大负面影响及其影响范围远远超出任何预定目标，其使用应限于有助于防止或调查对国家安全构成严重威胁的具体严重犯罪案件或行为。应严格规定只可使用这类软件调查涉嫌实施或已实施这种行为的人。还应该是最后手段，换句话说，所有侵扰性较低的措施都已用尽或被证明无效，而且严格限制范围和持续时间。只应访问和收集相关数据。[33] 还应对这些措施进行严格独立监督；必须事先得到司法机构批准。[34] 此外，明确考虑人权风险的严厉透明的出口管制手段可以成为防止侵权和滥用的有力工具。[35] 人权高专办重申其最近的呼吁以及人权专家和团体的呼吁，即在建立基于人权的保障制度之前，暂停销售、转让和使用黑客工具。[36]

## B. 对加密进行限制

20. 近年来，各国政府采取了各种行动，这些行动可能有意或无意地破坏加密通信的安全性和保密性，对享有隐私权和其他人权将产生令人担忧的影响。

21. 加密是保护网上隐私和安全的关键手段，对保障各项权利，包括见解和言论自由权、结社和和平集会自由权、安全权、健康权和不受歧视权至关重要。加密可以确保人们自由分享信息，而不必担心被他人——国家当局或网络罪犯知道。如果人们希望安全地与其他人自由交流各种信息，包括经历、思想和身份以及敏感的健康或财务信息、性别认同和性取向的知识、艺术表达和少数群体地位信息，加密是必不可少的。在审查盛行的环境中，加密可以使个人保有一方持有、表达和与他人交换意见的空间。具体而言，如果没有强有力的加密保护，记者和人权维护者便无法开展工作，因为加密可以保护他们的消息来源，使其免受被调查的强权人物的骚扰。加密也为遭到在线监控、骚扰和暴力等特殊威胁的妇女提

[31] 见德国联邦宪法法院，2008 年 2 月 27 日的判决(1 BvR 370, 595/07)，第 247(aa)段。

[32] 欧洲数据保护主管机构，见 https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf，第 8 页。

[33] 见 https://privacyinternational.org/sites/default/files/2018-08/2018.01.17%20Government%20Hacking%20and%20Surveillance.pdf.

[34] 实施秘密监控措施的最低保障，见 A/HRC/39/29。

[35] A/HRC/39/29，第 25 段；A/HRC/44/24，第 40 段；A/HRC/48/31，第 46 段；A/HRC/41/35，第 34 和 66 段。欧洲联盟最近通过了新的出口管制条例，朝着更多考虑人权方向迈出一步。

[36] 见 https://www.ohchr.org/en/statements/2021/09/committee-legal-affairs-and-human-rights-parliamentary-assembly-council-europe; https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening; https://www.amnesty.org/en/documents/doc10/4516/2021/en/; https://cyberpeaceinstitute.org/news/renewed-call-moratorium-spyware/.

供重要保护，防止信息被非自愿披露。[37] 在武装冲突中，加密信息是确保平民之间安全通信的必要手段。值得一提的是，在 2022 年 2 月 24 日乌克兰武装冲突开始后的两个月里，加密信息应用软件 Signal 在乌克兰的下载量比前几个月增加了 1,000%以上。[38]

22. 加密作为隐私和人权保护手段的重要作用已得到广泛承认，包括得到各国、联合国机构、联合国人权事务高级专员和人权专家的认可。[39] 大会和人权理事会在几项决议中强调了加密对保障人权的重要性，呼吁各国不要干预加密技术，[40] 鼓励工商企业努力促成保障和保护数字通信和交易的保密性的解决方案，包括加密、假名化和匿名措施。[41] 特别报告员和区域专家表示支持强加密，认为是一种权利保障手段，建议推广和保护强加密，并告诫不要采取任意或非法限制使用这一关键技术的措施。[42] 儿童权利委员会强调，必须根据合法性、必要性和相称性原则，严格限制检查加密通信中儿童性剥削和性虐待材料的任何措施。[43] 人权理事会、联合国和区域人权专家强调，加密对于新闻工作和保护消息来源至关重要。[44] 联合国教育、科学及文化组织发布的互联网普及指标强调了加密对网上信任和安全的重要性。[45]

23. 尽管加密有诸多好处，但政府时常限制加密的使用，例如为了保护国家安全和打击犯罪，特别是为了检查儿童性虐待材料。限制措施包括禁止加密通信，将提供或使用加密工具刑罪化[46] 或对加密工具实施强制注册和许可[47]。有时还要求加密提供商确保执法机构或其他政府机构能够应请求访问所有通信。这样做实际上相当于对加密的全面限制，由此可能需要或至少鼓励创建某种后门(绕过加密的内置路径，允许秘密访问明文数据)。[48] 另一种干扰加密的方式是要求创建和

[37] A/HRC/35/9，第 18 段。

[38] 见 https://sensortower.com/blog/signal-telegram-ukraine-russia-2022.

[39] 见 https://www.ohchr.org/en/press-releases/2016/03/apple-fbi-case-could-have-serious-global-ramifications-human-rights-zeid.

[40] 大会第 75/176 号决议以及人权理事会第 39/6 号、第 44/12 号、第 45/18 号和第 48/4 号决议。

[41] 大会第 75/176 号决议和人权理事会第 48/4 号决议。

[42] 见 A/HRC/29/32; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf; A/HRC/41/41; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf; https://www.osce.org/representative-on-freedom-of-media/379351; https://www.oas.org/en/iachr/expression/reports/ENGIA2020.pdf.

[43] 儿童权利委员会，关于与数字环境有关的儿童权利的第 25 号一般性意见(2021 年)，第 70 段。

[44] 人权理事会第 45/18 号决议；A/HRC/29/32；https://www.osce.org/representative-on-freedom-of-media/379351.

[45] 见 https://en.unesco.org/internet-universality-indicators，指标 D.5。

[46] 见 PSE 2/2017 和 LBY 3/2022。本报告中提到的所有通信，可查阅 https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[47] 见 https://hrsly.com/wp-content/uploads/2022/06/OL-LBY-3.2022-DownLoadPublicCommunicationFile.pdf (LBY 3/2022).

[48] 见 GBR 4/2015、MYS 2/2018、AUS 5/2018 和 AUS 6/2018。

维护密钥托管系统，并将解密数据需要的所有私钥交给政府或指定第三方。[49] 实施可追溯性要求，即提供者需要能够追溯到任何信息的所谓始发者，也可能削弱加密标准。[50] 最近，一些国家开始对数字通信提供商，包括加密通信服务提供商，实施或考虑实施一般性监测义务。[51] 这种义务可能迫使提供商放弃端到端的强加密，或者寻找很成问题的变通办法(见下文第 27 至 28 段)。

24. 广泛使用的加密能力，即公众应对大规模监控和网络犯罪所需要的能力，无疑给政府寻求保护民众特别是最脆弱社会成员免受严重犯罪和安全威胁造成两难困境。然而，如促进和保护意见和表达自由权特别报告员指出的，对加密进行监管可能损害人权。[52] 寻求限制加密的政府往往未能证明所实施的限制是满足特定合法利益所必需的，因为有各种其他工具和手段可以提供具体执法或其他合法目的所需要的信息。[53] 这些替代措施包括经过改进并拥有充足资源的传统警务、卧底行动、元数据分析和加强国际警务合作。

25. 此外，大多数加密限制措施对隐私权和相关权利的冲击极大，往往不仅影响目标个人，而且影响普通大众。政府的彻底禁止，尤其是将加密刑罪化，是没有道理的，因为其管辖范围内的所有用户将无法以安全方式进行通信。密钥托管系统有很大弱点，因为依赖于存储设施的完整性，而且存储的密钥容易遭受网络攻击。此外，加密工具中的强制后门产生的责任远远超出监视犯罪嫌疑人或安全威胁等特定用户的有用性。它们危及所有用户的隐私和安全，使他们遭受非法干预，不仅是国家的非法干预，也包括犯罪网络在内的非国家行为者的非法干预。[54] 许可和注册要求具有类似的严重后果，因为需要加密软件包含可利用的弱点。[55] 这种不利后果不一定局限于施加限制的管辖地区；一旦在一国管辖范围内建立后门，这一后门很可能成为世界其他地方使用的软件的一部分。

26. 最近有人提出一个概念，即为避免上述许多问题，可通过所谓的客户端扫描来检查某些形式不良内容。客户端扫描将检查内容的步骤从发送通信经由的服务器前移到个人设备本身。由此在加密传输之前便对可疑内容进行检查。2021 年 8 月，苹果宣布计划为其 iMessage 和 iCloud 服务引入这一系统，但在受到信息技术安全专家、密码专家和人权组织的广泛强烈批评后，暂停了拟议的改革。[56] 然而，各种立法尝试[57] 至少可以间接地迫使互联网通信服务实施这种系统，从

[49] 见 RUS 7/2016 和 RUS 7/2018。

[50] 见 IND 31/2018、IND 3/2019、BRA 6/2020 和 BRA 7/2020。

[51] 例如，美利坚合众国 2020 年通过的“EARN IT”法案(见 USA 4/2020)；英国的在线安全法案草案(见 GBR 5/2022)；欧洲联盟委员会关于欧洲议会和欧洲理事会制定预防和打击性虐待儿童规则条例的提案，2022 年 5 月 11 日(COM(2022) 209)；以及印度政府 2021 年信息技术(媒介指南和数字媒体道德规范)规则(见 IND 8/2021)。

[52] 见 A/HRC/29/32。

[53] 同上，第 39 段。

[54] A/HRC/39/29, 第 20 段。

[55] A/HRC/29/32, 第 41 段。

[56] 见 https://cdt.org/wp-content/uploads/2021/08/CDT-Coalition-ltr-to-Apple-19-August-2021.pdf.

[57] 欧洲联盟委员会，欧洲议会和理事会关于制定预防和打击性虐待儿童规则条例的提案，2022 年 5 月 11 日(COM(2022) 209)；另见大不列颠及北爱尔兰联合王国在线安全法案草案，可查阅 https://www.gov.uk/government/publications/draft-online-safety-bill.

而有义务对所有通信包括加密通信进行广泛监控。由于信息内容一旦加密，除了发送者和接收者之外，任何人都不能访问，所以任何一般性监视义务将迫使服务提供商放弃传输加密信息或者在信息加密之前设法获取信息。

27. 强制实行一般客户端扫描将构成一种范式转变，引起一系列严重问题，可能对享有隐私权和其他权利造成不良后果。与其他干预措施不同，强制性一般客户端扫描势必影响到使用现代通信工具的每个人，而不仅仅限于涉嫌犯罪和严重安全威胁的人。强制客户端扫描将改变人们完全控制与其生活密不可分的通信设备的能力，并限制这些设备可分享何种信息的能力。[58] 此外，在一般通信扫描中，即使准确率很高，也无法避免出现频繁误报，从而牵连许多无辜个人。[59] 鉴于这些影响的可能性，不加区别进行监控可能对言论和结社自由产生重大寒蝉效应，人们会限制与他人交流和互动的方式，并进行自我审查。[60]

28. 客户端扫描也带来新的安全挑战，使安全违规更有可能。[61] 扫描过程也可以被操纵，人为创建假肯定或假否定特征。[62] 即使在目前用途中严格确定客户端扫描对象，但一旦开放设备供政府授权的扫描，未来便有人试图扩大扫描目标的内容范围。[63] 特别是在法治薄弱和人权受到威胁的地方，客户端扫描的影响可能大得多。例如，可能用来压制政治辩论或攻击反对派人物、记者和人权维护者。[64] 由于授权的一般客户端扫描给人权保护带来广泛重大风险，在没有实质性考虑其潜在的人权影响和采取措施减轻这些危害的情况下，不应实施此类措施。如果没有深入的调查和分析，这类限制即使为了追求合法目的按照国际人权法似乎不太可能被认为是相称的，因为其后果极为严重。[65]

## 三. 对公众进行监控

29. 高级专员多次表示关切大规模监控，特别是大规模拦截通信问题。[66] 虽然一些国家改进了监控的保障措施，但监控大部分甚至全体人口的网上活动这一令

[58] 全球加密联盟指导委员会和隐私国际提交的材料。

[59] 见 https://doi.org/10.48550/arXiv.2110.07450.

[60] 关于监控的寒蝉效应的更多信息，见下文第 47 段。

[61] 与攻击企业服务器相比，攻击个人设备可能由更多参与者在不太安全的基础设施上执行。对手可以利用访问设备时机逆向操作扫描机制，https://doi.org/10.48550/arXiv.2110.07450.

[62] https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; https://openreview.net/forum?id=CQbqeGAM_Ki.

[63] https://www.washingtonpost.com/opinions/2021/08/19/apple-csam-abuse-encryption-security-privacy-dangerous/; https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; https://doi.org/10.48550/arXiv.2110.07450.

[64] 同上。

[65] A/HRC/39/29, 第 20 段；A/HRC/29/32, 第 43 段。欧洲联盟法院的观点支持这一结论。该法院最近裁定，对交通和位置数据进行普遍和不加区分的自动分析，仅限于应对严重、真实、当前或可预见的国家安全威胁的绝对必要情况。法院驳回了任何其他理由。见 La Quadrature du Net 和他人诉总理和他人案，2020 年 10 月 6 日的判决(合并案件 C-511/18、C-512/18 和 C-520/18)，第 177 段。此外，其判例法表明对扫描内容数据持有更强烈怀疑态度，欧洲联盟法院，Maximillan Schrems 诉数据保护专员案，2015 年 10 月 6 日的判决(C-362/14)，第 94 段。

[66] 见 A/HRC/27/37；A/HRC/39/29；https://www.ohchr.org/en/press-releases/2013/07/mass-surveillance-pillay-urges-respect-right-privacy-and-protection.

人不安的做法并没有停止。以前的报告主要论述私人通信监控，对监控公共场所的隐私影响着墨不多，以下将进行讨论。

## A. 对公共场所的监控

30. 安装摄像头监控公共街道、停车场、交通枢纽和其他公共场所在许多国家已经司空见惯。预计 2021 年全球使用的监控摄像头数量已超过 10 亿。[67] 在世界上视频监控密度最高的 10 个城市中，每 1,000 名居民拥有约 39 至 115 台监控摄像头。[68]

31. 除了国家运行的监控系统，一些公司还安装了供私人使用的监控工具，配备向当局报告事件甚至允许其直接访问数据流的专用功能。[69] 这样做极大地扩展监控的公共空间，同时削弱了透明度、监督和问责制。

32. 近年来，添加复杂的视频分析功能后，监控摄像头的功能大幅度增强。据估计，2010 年销售的网络摄像头中只有不到 2%装有嵌入式视频分析功能，2016 年这一比例已增至 40%以上，并有可能继续增长。[70] 分析功能越来越依赖人工智能。增加面部识别和识别可疑行为的能力，已成为先进的视频监控系统最具争议的特点。[71] 此外，在许多国家，使用无人机进行监视也已成为常态，无人机被用于监视抗议和其他集会。[72]

33. 在“智能城市”的总称下，越来越多的数据驱动型举措正在重塑城市空间。智能城市项目主要借助日益多能的传感器技术收集和处理数据，为城市设施的管理提供信息。虽然收集和处理的数据大多不属于个人数据领域，只与交通流量、污染或噪音等问题有关，但收集的其他数据如车牌和智能电表数据，也很容易与个人相联系。此外，看似匿名的数据通常可以去匿名化，[73] 基础设施(如为监控交通数据流而安装的摄像头)可以重新用于跟踪个人。[74]

34. 这些情况常常发生在建立新的身份系统和扩展生物特征数据库的背景下。在许多国家，身份系统与存储个人数据包括指纹、面部几何特征、虹膜扫描和 DNA 等生物特征信息的庞大中央数据库相联接。此外，数据库之间往往又相互连接，可供其他机构搜索。因此，无论人在何处，都越来越容易被找到。

[67] 见 https://venturebeat.com/2022/06/18/how-ml-powered-video-surveillance-could-improve-security/.

[68] 见 https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; https://surfshark.com/surveillance-cities.

[69] 见 https://www.accessnow.org/amazon-ring-privacy-review/.

[70] 见 https://cdn.ihs.com/www/pdf/IHS-Markit-Technology-Video-surveillance.pdf.

[71] 见 Derechos Digitales 和公民自由组织国际网络提交的材料。

[72] 见大赦国际和世界公民参与联盟提交的材料。

[73] 见 https://www.cs.princeton.edu/~arvindn/publications/de-anonymization-retrospective.pdf.

[74] 关于智能城市的人权影响的更多信息，见 https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/; https://carrcenter.hks.harvard.edu/files/cchr/files/CCDP_006.pdf.

## B. 在线监视

35. 与此同时，监视公众在线话语已变得十分普遍。在全球范围内，许多当局在收集和分析社交媒体帖子以及公众开放通信平台上的私人和专业网络。这类社交媒体情报包罗万象，包括对特定用户的调查到拉网式收集、存储和分析大量数据。获取的数据可能包括：姓名、年龄、照片和相关数字模板、地址、帖子和对别人帖子的反应、社会和专业联系及相关网络、位置数据、兴趣、性取向、性别鉴定、政治派别和活动、宗教信仰和健康信息。

36. 通常，各种预测分析构成社交媒体情报活动的一部分，包括试图发现可能的犯罪热点。然而，也可利用这类分析评估个人过去、现在和未来的行为，并根据他们成为罪犯或安全威胁的可能性给予风险评分。[75] 社交媒体情报也可被用来预测社会动荡的可能性。[76]

37. 这些活动可以服务于多种正当和不正当目的，从犯罪调查和预防到审查社会福利申请人、监视抗议活动、衡量公众情绪和描绘人们社会行为。[77]

## C. 人权影响

38. 现代的数据驱动技术正在显著改变监控实施机构与被监控者之间的权力平衡。在大规模自动监控和数据分析工具出现之前，即使在公共场合为个人提供一定程度保护的监视也存在实际限制。[78] 先进的数字工具使过去的“自然”保护变得毫无意义。如今，一名官员可以查看几十人的社交媒体账户；在高级软件和大数据分析的帮助下，小型团队可以观察和分析数千账户的情况。[79]

39. 类似的发展提高了对公共场所的其他监控措施的效率和范围。例如，面部识别技术以及其他生物识别技术的兴起从根本上改变了传统的视听监控做法，因为已有更大能力在公共场所包括集会参与者中识别个人。现场面部识别技术可以实时识别个人身份，并对其进行定点监视和跟踪。对个人的回溯识别可能扩大各种数据的来源，如果部署时没有最大限度的克制，将导致同样侵入性影响。[80]

40. 公共监控对人权的影响进一步加剧，因为各种数据源日益融合，例如面部识别的视频监控资料与社交媒体数据[81] 和政府数据库相连接。政府数据库中包含社会保障、移民、恐怖主义嫌犯、逮捕或甚至因政治原因被列入清单人员等信息。

41. 此外，各国还依赖各种私人公司收集的大量数据。在以前的报告中，高级专员和特别报告员着重指出了政府往往在强制性数据保留法律背景下要求查阅电信

[75] 见 https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/, 第 152 页。

[76] 见 https://dx.doi.org/10.2139/ssrn.2702426, 第 1 页。

[77] 见 https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.

[78] A/HRC/44/24，第 34 段。

[79] 见 https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.

[80] 见大赦国际提交的材料。

[81] 见公民自由组织国际网络提交的材料。

和互联网服务提供商收集的数据的问题。[82] 收到此类请求的公司数量不断增加。一些国家强迫公司允许它们直接访问经由其网络的数据流。这种直接获取方式令人严重关切，因为特别容易被滥用，而且常常绕过关键的程序保障。[83]

42. 此外，各国越来越依赖商业企业提供的监控服务，例如从数据经纪人和其他收集与出售个人数据的公司获得数据。[84] 这种做法可以绕过重要的程序限制和保障，使国家能够间接利用若自己部署将违反人权义务的工具。譬如，数千个执法机构使用 Clearview AI 公司开发的面部识别工具，而事实上这一工具是从互联网上收集数十亿人照片构建的，是对隐私权的大规模侵犯。[85]

43. 在公共场所对人员进行在线和离线系统监视，特别是结合其他方法如分析和连接其他数据来源已有信息，构成对隐私权的干预，可能严重损害享有其他人权。[86] 这样做可能威胁言论和和平集会自由、参与和民主，因此应极其谨慎地对待，必须严格遵守人权要求。即使被监控的活动在公共场合或公开社交媒体平台上进行，情况也是如此。因为个人需要有一个不受系统观察和侵扰特别是不受政府实体观察和侵扰的空间。正如高级专员先前指出的，隐私权的保护延伸到公共空间和公开信息。[87] 人权事务委员会拒绝接受在公共场所收集的数据必然属于公共领域并可以自由获取的观点。[88] 欧洲人权法院认为，公开可得或可察觉的信息很可能属于隐私权范畴，特别是个人数据被系统或永久记录时。[89]

44. 公共监控尤其令人关切的一个问题是摄影图像的记录。人的影像体现个性的关键属性，揭示区别于其他人的独特特征。未经个人同意记录、分析和保留其面部图像是干预隐私权行为。在公共场所部署面部识别技术，需要收集和处理摄像头捕捉到的所有人的面部图像，这种干预在大规模和不加区分地发生。[90]

---

[82] A/HRC/27/37，第 26 段；A/HRC/39/29，第 18 段；A/HRC/23/40 和 A/HRC/23/40/Corr.1，第 65-67 段；A/69/397，第 53-55 段。

[83] A/HRC/39/29，第 19 段。

[84] 参见 https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances; https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf, 第 25 页。

[85] 各数据保护机构认定 Clearview AI 违反了数据保护法，处以高额罚款和/或下令删除所获取的个人数据，见 https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/; 另见 https://www.oaic.gov.au/updates/news-and-media/clearview-ai-breached-australians-privacy; https://edpb.europa.eu/news/national-news/2022/facial-recognition-italian-sa-fines-clearview-ai-eur-20-million_en; https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. 数据保护机构认为，警察使用该工具违反了数据保护法，见 https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en; https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

[86] 见 CCPR/C/NGA/CO/2，人权事务委员会对监控社交媒体表示关切，第 40 段。

[87] A/HRC/39/29，第 6 段。

[88] CCPR/C/COL/CO/7，第 32 段。

[89] 见欧洲人权法院，Rotaru 诉罗马尼亚案，2000 年 5 月 4 日的判决，第 43 段；Peck 诉联合王国案，2003 年 1 月 28 日的判决，第 59 段；Perry 诉联合王国案，2003 年 7 月 17 日的判决，第 38 段；Vukota-Bojić 诉瑞士案，2017 年 1 月 18 日的判决，第 55 段。

[90] A/HRC/44/24，第 33 段。

45. 此外，公共监控行动可能导致或常常作为依据采取直接影响个人和社区的措施，包括强制措施。这些措施包括加强对某些居住区、群体或个人的监测和监管，有时会对个人进行审讯、逮捕和拘留。一些团体和个人也可能被列为潜在威胁或风险，例如可能的恐怖分子或罪犯，而往往没有确凿的事实依据。一些政府利用各种公共监控措施的结果来发现批评他们的人或不符合社会期望的人，可能对他们进行骚扰、拘留或剥夺基本服务。[91]

46. 监控行动往往更多地针对少数族群和边缘化群体。[92] 使用人工智能，[93] 包括使用面部识别技术进行种族和族裔定性，[94] 有可能使这种歧视模式长期延续下去。警务和司法的预测系统已证明对少数群体产生了严重影响。[95]

47. 此外，监控对人们如何行使权利，特别是言论和和平集会自由权利，具有相当大的寒蝉效应。[96] 各种研究证明了这种影响的程度。2015 年的一项调查显示，知道爱德华·斯诺登事件的回复者中有 25%改变了他们使用各种技术平台的方式。[97] 另一项研究发现，34%至 61%的作者(取决于所涉国家)由于害怕政府监视而回避或至少考虑回避其作品中的某些主题。[98] 在挪威技术委员会进行的一项调查中，39%的受访者表示，他们会避免使用受到警方监控的词语。[99] 正如高级专员先前指出的，这种寒蝉效应延伸到集会，包括和平抗议。[100]

---

91 见 https://privacyinternational.org/explainer/55/social-media-intelligence.

92 见 CERD/C/CHN/CO/14-17；https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media.

93 见高级专员“关于促进和保护非洲人和非洲人后裔人权与基本自由以使其不受执法人员过度使用武力和其他侵犯人权行为侵害”的会议室文件，第 93 和 94 段。可查阅 https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session47/list-reports.

94 A/HRC/41/35，第 12 段；A/HRC/44/57，第 39 段。

95 消除种族歧视委员会，关于防止和打击执法人员的种族定性行为的第 36 号一般性建议(2020 年)，第 33-34 段；A/HRC/44/57, 第 43 段；高级专员“关于促进和保护非洲人和非洲人后裔人权与基本自由以使其不受执法人员过度使用武力和其他侵犯人权行为侵害”的会议室文件；第 93 段；A/HRC/48/31, 第 24 段；https://www.nyulawreview.org/online-features/dirty-data-bad-predictions-how-civil-rights-violations-impact-police-data-predictive-policing-systems-and-justice/; https://www.fairtrials.org/app/uploads/2021/11/Automating_Injustice.pdf; https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

96 A/HRC/27/37, 第 20 段；关于抗议活动，见 A/HRC/44/24, 第 29、35 和 52 段；欧洲人权法院，Big Brother Watch 和他人诉联合王国案，2021 年 5 月 25 日的判决(58170/13、62322/14 和 24960/15)，第 495 段；http://dx.doi.org/10.15779/Z38SS13; https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; https://pen.org/research-resources/global-chilling/.

97 见 https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf.

98 见 https://pen.org/research-resources/global-chilling/.

99 见 https://teknologiradet.no/wp-content/uploads/sites/105/2018/05/Online-with-the-public.pdf.

100 A/HRC/44/24，第 35 和 53 段。

## D. 人权要求

48. 公共监控无疑带来巨大的人权风险，可能严重损害隐私权。因此，诉诸公共监控的国家必须评估其行动的潜在人权影响，严格遵守国际人权法。国际人权法要求任何此类干预或限制必须以法律为依据，是实现正当目标所必需的，而且是相称的。目前的公共监控措施往往达不到这些要求。

49. 合法性：尽管各种形式的公共监控产生了深远影响，但大多数国家没有可行的适用法律框架。数据保护法往往缺失、不充分，或者为执法和情报部门留出大量例外。[101] 此外，一般性数据隐私法通常不提供详细的指导或确保对特定监控工具的使用规定足够限制。在这方面，需要有专门的法律文书，特别是用以规范执法和国家安全背景下的监视。[102] 法律法规需要对访问和合并政府数据库实施明确和严格限制。可惜几乎没有迹象表明各国在努力规范社交媒体情报手段、技术和工具的使用。尽管地方、国家和区域层面的监管者和立法者在加大努力来监管面部识别和其他生物特征监控工具，[103] 但由于这种活动无法律可依，大多数机构仍在继续使用生物识别监视系统。

50. 正当目标：毫无疑问，公共监控可以服务于广泛的正当目标，例如保护人们的生命或身体完整以及重要基础设施的安全。但令人遗憾，仍在为了国际人权法不允许的目的进行日常公开监控。公共监控尤其不适当地用于识别和追踪政治异见者，进行种族和族裔定性，针对男女同性恋、双性恋、跨性别者和间性人群体，以及评估人们是否符合社会规范。

51. 必要性和相称性：虽然公共监控可能是允许的，但国家必须证明有关措施的必要和相称性。然而，监控措施的有效性常常令人怀疑，其必要性或相称性也存在严重问题。视频监控对安全和犯罪预防的效果已证明好坏参半。大多数研究表明，在监控摄像头监控的区域，某些类型的犯罪(如与车辆和财产相关的犯罪)最多只略有减少，一般而言暴力犯罪似乎不会受到监控摄像头存在的影响。[104] 此外，对不同国家众多城市的比较发现，公共监控摄像头的数量与整个城市的犯罪或安全之间几乎没有关联。[105] 关于自动威胁检测，警察部队广泛使用这一系统来检测枪声，以确定可能的犯罪现场。事实上在 89%的案件中将一般声音错误地

[101] A/HRC/39/29，第 34 段。

[102] 高级专员以前曾简要介绍过关于监控法律的最低要求，见 A/HRC/27/37 和 A/HRC/39/29。

[103] 见拟议的欧洲联盟人工智能法案；欧洲数据保护委员会关于在执法领域使用面部识别技术的指南，05/2022，1.0 版，可查阅 https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en; 另见美国华盛顿州关于使用面部识别的法律，可查阅 https://www.securityindustry.org/report/washington-facial-recognition-law-faq/; 以及地方和区域立法机构通过的禁令和暂停令。

[104] 见 https://academicworks.cuny.edu/jj_pubs/256/; https://doi.org/10.1080/01924036.2021.1879885.

[105] 见 https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/.

识别为枪声。[106] 最后，许多签署预测警务服务合同的警察部门已终止这些合作，称其用处有限。[107]

52. 对公共场所人员的普遍监控几乎总是过分的。公共场所的监控措施应有针对性，并为了实现具体的正当目标，如阻止足以抵消其负面人权影响的重大公共安全或安保威胁。这类监控措施需要加以限制，聚焦特定的地点和时间，例如有证据表明可能发生犯罪或可能出现公共安全威胁时。没有更少侵犯隐私的选择。必须对所捕获数据的存储期限以及此类数据的相关用途施加严格限制。远程生物识别监控系统的相称性尤其令人严重关切，因为其高度侵入性和对大量人口的广泛影响。[108] 在这种背景下，高级专员欢迎最近努力限制或禁止使用远程生物识别技术，并呼吁至少在关键保障措施到位之前，暂停在公共场所使用这种技术。[109] 如果要使用，只能用于应对严重犯罪和严重公共安全威胁等情况，而且还需要排除歧视性影响，接受充分和有效监督，包括独立授权和定期独立人权审计。

## 四. 结论和建议

53. 本报告简要介绍了目前对数字领域隐私权造成威胁的几个关键方面。数字技术的迅速应用带来一系列其他挑战，这些挑战在本报告没有涉及，却值得进一步关注。例如，高级专员在以前报告[110] 中讨论的大规模秘密监控仍是严重问题。同样，数字身份系统和生物识别技术的各种应用已在全球推广，但对如何影响人权还知之甚少。广告商、金融机构和数据经纪人等无数公司对互联网用户的全面跟踪，需要在国际人权论坛上给予更多关注。冠状病毒病(COVID-19)和令人眼花缭乱的数字反应阵列可以成为一份报告的主题。必须更深入探讨和了解侵犯和践踏隐私权对边缘化群体和弱势群体的影响。也应密切关注新的动态，如积极推动广泛采用区块链、扩展和虚拟现实技术以及日益强大的神经技术。

54. 尽管本报告仅关注少数几个关键动态，却呈现了一幅令人不安的画面，显示隐私权在数字时代正日益受到损害。这一分析结果不应该被理解为否认数字技术给社会带来的巨大好处——相反，各个社会应该充分拥抱技术进步。技术变革赋权人民，改善生活，加强正义和提高生产力。然而，无处不在的监控在以多种方式威胁人权和法治，并可能侵蚀充满活力的多元民主，着实令人深感震惊。现代网络数字技术因其自身特点可能成为控制和压迫人民的强大工具：数字空间中的每一个行动都会留下数据痕迹；云计算技术促进了不同数据源的融合和分析；自动化提高了监控的可能范围和效率；数字监控很难为受监控者观察到。此外，数字监控必然普遍地与缺乏透明度相关联。公众通常对交织在各方面生活的各种监

[106] 见 https://www.macarthurjustice.org/blog/shotspotter-is-a-failure-whats-next/; https://igchicago.org/2021/08/24/oig-finds-that-shotspotter-alerts-rarely-lead-to-evidence-of-a-gun-related-crime-and-that-presence-of-the-technology-changes-police-behavior/.

[107] 见 https://themarkup.org/prediction-bias/2021/12/02/crime-prediction-software-promised-to-be-free-of-biases-new-data-shows-it-perpetuates-them.

[108] A/HRC/48/31，第 26-27 段；A/HRC/44/24，第 33-38 段。

[109] A/HRC/48/31，第 27 和 59(d)段。

[110] 见 A/HRC/27/37 和 A/HRC/39/29。

控行为知之甚少。政府往往不发布它们使用何种监控系统以及为何种目的使用的可靠信息，也常常忽视这些系统有效性的证据。

55. 不符合国际人权法的监控措施已经很普遍。即使监控的目的正当，底层基础设施也很容易改变用途，经常服务于有悖最初设计的目的(所谓的“功能蠕变”)或追随政治格局的变化。决策者在考虑增强收集和分析个人数据能力的新项目时，应牢记这一点。迫切需要就监控的界限展开公开辩论。没有积极的公众讨论，社会可能梦游般进入监控系统的陷阱，让当权者对日常生活施加前所未有的控制。

56. 有鉴于此，人权高专办建议各国：

(a) 确保对隐私权的任何干涉，包括窃取数据、限制获得和使用加密技术以及对公众进行监视，都符合国际人权法，包括合法性、正当目的、必要性和相称性以及不歧视的原则，并且不损害这项权利的实质；

(b) 在设计、开发、购买、部署和运行监控系统时，系统地开展人权尽职调查，包括定期进行全面人权影响评估；

(c) 在进行人权尽职调查和评估新监控系统及力量的必要性和相称性时，考虑到这些系统或力量所处或将要处于的整个法律和技术环境；各国还应考虑滥用、功能蠕变和改变用途的风险，包括未来政治变革带来的风险；

(d) 通过独立、公正和资源充足的机构，颁布和有效执行符合国际人权法的公共和私营部门数据隐私法律，包括有效保护隐私权的保障制度、监督办法和补救措施；

(e) 立即采取措施，有效提高监控技术使用的透明度，包括适当告知公众和受影响的个人和社区，并定期提供相关数据，供公众评估其功效和对人权的影响；

(f) 促进关于使用监控技术的公开辩论，并确保所有利益攸关方有意义地参与关于获取、转让、销售、开发、部署和使用监控技术的决策，包括公共政策的制定及其实施；

(g) 暂停在国内和跨国销售和使用监控系统，如可用于在公共场所识别或区分个人的黑客工具和生物识别系统，直到出台足够的人权保障措施；这种保障措施应包括国内和出口管制措施，符合本报告和提交人权理事会前几份报告中提出的建议；[111]

(h) 确保与使用监控系统相关的侵犯人权和虐待行为的受害者能够获得有效补救。

[111] 见 A/HRC/27/37、A/HRC/39/29、A/HRC/44/24 和 A/HRC/48/31。

57. 关于本报告提出的具体问题，人权高专办建议各国：

黑客攻击

(a) 确保当局将入侵个人设备作为最后手段，仅用于防止或调查对国家安全构成严重威胁的具体行为或具体的严重犯罪，并严格针对涉嫌实施这些行为的人；这类措施应接受严格的独立监督，并应事先得到司法机构的批准；

加密

(b) 促进和保护强加密，避免对加密的使用施加任何直接或间接、普遍和不加区分的限制，如禁止、定罪、实施弱加密标准或强制要求客户端扫描；只有得到独立司法机构授权，并在个案基础上，才能对个人的私人通信加密进行干预。只在调查严重犯罪或预防严重犯罪或对公共安全或国家安全的严重威胁的绝对必要情况下，才可针对个人进行此种干预；

公共场所的监控和监控技术的出口管制

(c) 采用适当的法律框架来管理社交媒体情报的收集、分析和分享，明确界定允许的理由、先决条件、授权程序和适当的监督机制；

(d) 避免对公共场所进行侵犯隐私的一般性监控，并确保所有公共监控措施对实现重要的正当目标是绝对必要和相称的，包括严格限制这些措施的位置和时间，以及数据存储的期限、数据使用的目的和获取数据的途径；生物识别系统只能在公共空间使用，为防止或调查严重犯罪或严重公共安全威胁，而且必须符合国际人权法关于公共空间的所有要求；[112]

(e) 建立对监控技术的强有力和量身定制的出口管制制度，因为监控技术的使用对享受人权带来很大风险；各国应要求进行透明的人权影响评估，评估应考虑到相关技术的能力以及接受国的情况，包括尊重人权、遵守法治、是否存在和有效执行管理监控活动的适当法律以及是否存在独立的监督机制；

(f) 确保在提供和使用监控技术时，公私伙伴关系坚持并明确纳入人权标准，不放弃对政府的人权问责。

[112] 包括 A/HRC/44/24 号文件第 53(j) (i–v)段和 A/HRC/48/31 号文件第 59(d)段提出的要求。