联合国 A/HRC/41/41

大会

Distr.: General
17 May 2019
Chinese
Original: English

人权理事会
第四十一届会议
2019年6月24日至7月12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

和平集会自由权和结社自由权

和平集会自由权和结社自由权特别报告员的报告*

概要

和平集会自由权和结社自由权特别报告员克莱芒·尼亚雷索西·武莱在这份报告中重点讨论数字时代和平集会自由权和结社自由权面临的机遇和挑战。特别报告员试图为如何更好地保持和最大限度地利用这些机遇并应对风险提供指导意见。

特别报告员得出结论认为，国际法保护和平集会自由权和结社自由权，无论是自行行使、通过当今的技术行使还是通过未来将会发明出来的技术行使。现行国际人权规范和原则不仅应规范国家行为，而且应当成为指导数字技术公司设计、控制和管理数字技术的框架。

* 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。

GE.19-08114 (C) 240519 070619
1908114

一. 导言

1. 和平集会自由和结社自由权特别报告员根据人权理事会第 15/21 号和第 32/32 号决议向人权理事会第四十一届会议提交本报告。特别报告员在第二节叙述他自 2018 年 6 月 18 日向人权理事会介绍其报告之后开展的一些活动，在第三和第四节讨论数字时代行使和平集会自由和结社自由权的问题，第五节详述他的结论和建议。

2. 数字时代为享有和平集会和结社自由权开辟了新的空间。全球有许多例子表明，当希望团结起来推进民主、和平与发展的人们手中拥有数字技术时会产生怎样的力量。但是，数字革命也给这些基本权利带来了一系列新的风险和威胁。

3. 特别报告员注意到，在过去十年中各国是如何利用技术来压制、监视和骚扰异见人士、政治反对派、人权维护者、活动家和抗议者并操纵舆论的。政府更为频繁地下令关闭互联网，并在选举和抗议等重大民主事件之前封锁网站和平台。世界许多国家旨在打击网络犯罪的立法和政策激增，也为惩罚和监督活动人士和抗议者打开了大门。虽然技术在宣传恐怖主义、煽动暴力和操纵选举方面可能发挥的作用确实是一个严重的全球问题，但这种威胁经常被用作压制新的数字民间社会的借口。

4. 与此同时，脸书、推特和油管等占主导地位的在线平台已经成为人们享有和平集会权和结社权能力的守护者，对个人和民间社会行为者能否进入和参与民主空间掌握巨大的权力。

5. 随着新兴技术——包括物联网和人工智能——的发展和日益普遍，数字技术对于行使集会和结社自由产生的机遇和威胁将会增加。特别报告员以其他相关特别程序任务负责人编写的报告[1] 为基础，在本报告中寻求为如何在应对风险的同时最好地保护并最大限度地利用这些技术带来的机会提供指导。本报告无意做到面面俱到，只希望对最紧迫的挑战初步做个全面介绍，在今后的报告和通报中将作进一步阐述。

6. 特别报告员在起草本报告期间通过征求意见和磋商的公共进程受益良多。2018 年 11 月，他呼吁各界为报告提供投入。截至报告发表之日，已收到民间社会组织提交的 10 份材料、数字技术公司提交的 2 份材料和政府提交的 2 份材料。特别报告员于 2018 年 10 月 11 日至 12 日在日内瓦召开了一次专家会议。他还分别在曼谷(2018 年 12 月 21 日)、贝鲁特(2019 年 1 月 18 日)、墨西哥城(2019 年 1 月 24 日至 25 日)、美利坚合众国加利福尼亚州硅谷(2019 年 1 月 27 日至 30 日)和内罗毕(2019 年 2 月 21 日至 22 日)与民间社会组织举行了区域磋商。他在哥本哈根与专家举行了会议(2019 年 3 月 6 日)，并在日内瓦与各国政府举行了磋商(2019 年 3 月 20 日)。此外，2018 年 12 月 18 日和 19 日他在曼谷与促进和保护意见和表达自由权特别报告员大卫·凯伊举行了联合磋商。

[1] 例见 A/HRC/17/27、A/71/373、A/HRC/23/40 和 A/HRC/38/47。

二. 特别报告员的活动

A. 国别访问

7. 特别报告员于 2018 年 9 月 17 日至 28 日访问了突尼斯(见 A/HRC/41/41/Add.3)，并于 2018 年 11 月 7 日至 16 日访问了亚美尼亚(见 A/HRC/41/41/Add.4)。他感谢两国政府在访问之前和访问期间给予的合作。

B. 通信

8. 2018 年 4 月 1 日至 2019 年 4 月 25 日，特别报告员总共向 60 个国家发送了 130 份信函。他对向各国发送的信函的意见和收到的答复载于本报告增编(A/HRC/41/41/Add.1)。

C. 参加各种活动

9. 特别报告员参加了包括以下在内的许多活动：

(a) 2018 年 7 月 16 日至 20 日对巴西的学术访问；

(b) 2018 年 9 月 13 日至 14 日在伯尔尼举行的关于公民空间萎缩问题和为民间社会创造有利环境的瑞士发展合作会议；

(c) 2018 年 10 月 24 日至 26 日在班珠尔举行的非洲人权和民族权利委员会第六十三届会议和 2019 年 4 月 24 日在埃及沙姆沙伊赫举行的该委员会第六十四届会议；

(d) 2018 年 10 月 30 日在巴黎举行的题为“让我们的空间再次变大：应对不断缩小的空间、限制性法律和资金限制——现实情况和未来 20 年的主要问题”的全球人权维护者峰会上的会议；

(e) 2018 年 11 月 21 日在荷兰乌得勒支大学全球挑战中心举行的“受攻击的公民空间”会议；

(f) 2018 年 11 月 26 日至 28 日在日内瓦举行的工商业与人权论坛；

(g) 2018 年 12 月 10 日法语国家国际组织在纽约举行的纪念《世界人权宣言》70 周年活动；

(h) 亚洲人权与发展论坛于 2018 年 12 月 20 日和 21 日在曼谷组织的与亚太区域民间社会和政府关于限制公民空间以及意见、表达和集会自由对选举的影响问题区域对话会；

(i) 2019 年 2 月 14 日在奥斯陆举行的挪威非政府组织协会年会，主题是“非政府组织能否拯救民主？”；

(j) 2019 年 3 月 4 日至 5 日在哥本哈根举行的“共同主张公民空间国际会议”；

(k) 2019 年 5 月 6 日至 10 日在金斯敦举行的美洲人权委员会第 172 届会议。

三. 数字时代的和平集会自由权和结社自由权：国际法律框架

A. 国家义务

10. 《世界人权宣言》第二十条和《公民权利和政治权利国际公约》第二十一和第二十二条保护和平集会自由和结社自由的权利。人权理事会强调，国家有义务在网上和网下尊重和充分保护这些权利[2]。大会还呼吁所有国家“根据人权法，确保个人在线下享有的权利，包括表达自由权、和平集会自由权和结社自由权，同样在线上也得到充分保护”。[3]

11. 在前几份报告中，任务负责人承认数字技术是行使和平集会权和结社权不可或缺的组成部分[4]。技术既是促进离线行使集会和结社权利的手段，也是使权利得到积极行使的虚拟空间[5]。事实上，对于努力以迅速和有效的方式并以低廉的成本动员一大群人的组织者来说，这种技术是重要的工具，也为那些在实体空间运作受限的社会边缘化群体提供了在线空间[6]。任务负责人呼吁各国确保每个人都能访问和使用互联网以行使这些权利，并根据国际人权标准为在线联合[7] 和集会[8] 提供便利。人权理事会认识到，虽然集会通常被理解为人们的实际集会，但人权保护，包括集会自由，也可适用于在线进行的类似互动。[9]

12. 虽然这些权利不是绝对的，但为行使和平集会和结社权利而获取和使用数字技术的自由应被视为常例，而限制应被视为例外。一般准则应该是允许开放和免费使用互联网和其他数字工具[10]。人权理事会第 15/21 号决议明确指出，允许的限制应由“法律所规定，是民主社会为了国家安全或公共安全、公共秩序、保护公众健康或道德或者保护他人的权利和自由所必需的”[11]。在作出这种限制时，“缔约国必须说明其必要性，而且所采取的措施必须符合合法的目的，以便确保不断和有效地保护《公约》权利。在任何情况下都不能以可能损害《公约》权利实质的方式实行限制。”[12]

13. 各国不仅有不过度干涉和平集会和结社权利的消极义务，而且有根据国际人权标准促进和保护这些权利的积极义务[13]。这意味着确保人人享有和平集会和结

[2] 见人权理事会第 38/7 号决议。

[3] 见大会第 73/173 号决议。

[4] 见 A/HRC/20/27 和 A/HRC/38/34。

[5] A/HRC/29/25/Add.1, 第 53 段。

[6] 见 A/HRC/35/28。

[7] A/HRC/20/27, 第 52 段。

[8] A/HRC/29/25/Add.1, 第 34 段。

[9] 见人权理事会第 38/11 号决议。

[10] A/HRC/23/39, 第 76 段。

[11] 见人权理事会第 15/21 号决议。

[12] 人权事务委员会关于《公约》缔约国的一般法律义务的性质的第 31 号一般性意见(2004 年)，第 6 段。

[13] A/HRC/17/27, 第 66 段；A/HRC/29/25/Add.1。

社自由的权利，不因种族、肤色、性别、语言、宗教、政治或其他见解、民族或社会出身、财产、出生或其他身份而受到歧视(《公民权利和政治权利国际公约》第二条第 1 款)。[14]

14. 在数字时代，促进行使和平集会和结社自由权的积极义务包括努力“弥合数字鸿沟，包括性别数字鸿沟，并加强对信息和通信技术的剖用，以促进所有人充分享有人权”[15]。保护的义务要求采取积极措施，防止包括企业在内的非国家行为者采取可能不适当地干涉和平集会和结社自由权的行动。[16]

15. 在和平集会和结社权利受到不当限制的情况下，受害者应当能够行使其获得有效补救和取得赔偿的权利。人权理事会呼吁各国“确保按照本国的国际义务，就侵犯人权行为，包括与互联网有关的侵犯人权行为提供切实补救”。[17]

16. 侵犯和平集会和结社权利也会干扰离线和在线享有其他人权。这些权利包括隐私权以及意见和表达自由权，它们与享有和平集会和结社权利密切相关。其他权利也可能受到影响，特别是经济、社会和文化权利。

B. 企业的角色和责任

17. 在数字时代，和平集会和结社权利的行使在很大程度上取决于工商企业，它们的法律义务、政策、技术标准、财务模式和算法会影响这些自由。特别是在线平台和社交媒体公司对和平集会自由权和结社自由权如何得到享受和行使拥有重大权力，特别是在和平集会和结社自由权的“离线”行使受到严重限制的国家。然而，这些平台也成为针对和监督民间社会行为者的新的工具。

18. 《工商业与人权指导原则》提供了评估数字技术公司尊重人权责任的全球框架[18]。指导原则 11-24 承认，企业“应尊重人权”，避免侵犯他人的人权，并解决自身所涉及的不利人权影响。为了履行这一义务，工商企业应制定人权政策和程序──包括履行尊重人权责任的政策承诺；一个人权尽职调查程序，以确定、预防、减轻和说明如何应对其人权影响；以及能够补救[19] 它们造成或促成的任何不利人权影响的程序。

19. 在这方面，任务负责人赞同促进和保护意见和表达自由权特别报告员的观点，后者指出，“人权法为公司提供了阐明和制定尊重民主规范和反对专制要求

[14] 又见《公约》第二十六条。

[15] 人权理事会第 38/7 号决议，第 5 段。这也反映在 2030 年《可持续发展议程》中，其中承诺“大幅提升信息和通信技术的普及度，力争到 2020 年在最不发达国家以低廉的价格普遍提供因特网服务”(具体目标 9.C)，并“加强技术特别是信息和通信技术的应用，以增强妇女权能”(具体目标 5.B)。又见 A/HRC/35/9。

[16] 见《公约》第二条第 2 款；人权事务委员会第 31 号一般性意见。

[17] 见人权理事会第 38/7 号决议。

[18] A/HRC/17/31。

[19] A/72/162, 第 86(c)段。

的政策和程序的工具”[20] 同样，人权理事会认识到，“国际人权法应指导私营部门行为体的行动，并成为其政策的基础”[21]。

20. 就国家而言，它们有义务保护人权，防止与企业等第三方的作为或不作为有关的侵权行为。指导原则 1 申明，“国家必须保护在其领土和/或管辖范围内人权不受第三方，包括工商企业侵犯。这就要求采取适当步骤，通过有效政策、法律、条例和裁定，防止、调查、惩治和补救此类侵犯行为。”[22]

四. 数字时代和平集会和结社权利的行使：机遇与挑战

A. 数字机遇

21. 数字技术为享有和平集会和结社自由的权利带来了巨大的机会。数字技术既可以作为“离线”行使这些权利的工具，也可以作为个人积极组建在线集会和协会的空间[23]，极大地扩展了个人和民间社会团体组织和动员、推进人权和为社会变革而创新的能力。

22. 社交媒体在动员人们上街游行方面的作用是众所周知的。例如，在 2018 年访问亚美尼亚期间，特别报告员听到了几个故事，讲述了社交媒体平台、直播工具和通信应用如何在导致总理辞职的 2018 年“天鹅绒”革命中发挥了关键作用。主题标签#MyStep 和#MerzhirSerzhin 被用来分享信息，发动民众并争取他们的支持，同时绕过政府控制的媒体。争取种族平等的#BlackLivesMatter 运动始于在美国和世界其他地方利用一个主题标签来动员社区进行大规模抗议，反对针对非洲人后裔的警察暴力和系统性种族主义。世界各地的许多青年运动都得到了社交媒体的支持，孟加拉国的#RoadSafetyMovement 运动、南非的#FeesMustFall 运动、#FridaysForFuture 运动和#ClimateStrikes 全球活动都证明了这一点。

23. 个人现在可以使用在线空间参与一个虚拟的互联公民社会。例如，女性活动人士利用互联网建立联系和交流战略，包括跨境交流，并将其作为组织的空间[24]。#MeToo 运动也许是最近最显著的例子。2017 年，性暴力幸存者利用社交媒体平台讲述遭受性骚扰和性虐待的个人故事，并在主题标签#MeToo 下呼吁工作场所的性别平等。据报道，一年之内，幸存者和该事业的支持者使用这一主题标签的次数超过 1900 万次[25]。虽然这场运动始于美国，但法国(#BalanceTonPorc)、阿拉伯世界(#AnaKaman)、印度(#MeTooIndia)、乌克兰(#IAmNotAfraidToSayIt)和墨西哥(#MeTooMexico)的妇女也加入了进来。

[20] 见 A/HRC/38/35。

[21] 见人权理事会第 38/7 号决议。

[22] 见 A/HRC/17/31。

[23] 见 A/HRC/29/25/Add.1。

[24] A/HRC/35/9, 第 23-24 段。

[25] Pew Research Center, “How social media users have discussed sexual harassment since #MeToo went viral”,11 October 2018.

24. 加密技术、假名和其他安全特性使属于少数群体的个人能够找到彼此并创建社区。人权理事会强调，“确保和保护数字通信保密性的技术解决方案，包括加密和匿名措施，会对确保享有人权，特别是隐私权、表达自由权以及和平集会和结社自由权十分重要”[26]。特别报告员认为，协会的组织和行为也是如此。这些工具为个人和民间社会行为者提供了安全的在线空间，以便在没有第三方和政府不当干预的情况下，与其团体的其他成员聚集和联系，并组织和协调活动[27]。

25. 通过使用社交媒体、电子请愿书和众筹平台，民间社会组织能够接触新的受众、传播信息、吸引成员并找到资金，而在以前这是不可能或极其昂贵的。例如，2018 年墨西哥地震后，一群公民通过#Verificado19S[28] 在线动员起来，提供可靠的信息，并向受害者提供所需的资源。在土耳其，Oy ve tesi 等组织利用社交媒体工具招募了 60 000 多名志愿者，在 2015 年 11 月大选期间监督 130 000 多个投票箱。在美国，美国公民自由联盟在一个周末筹集了数百万美元的在线捐款，支持其捍卫移民权利的工作。同样，在俄罗斯联邦严格限制民间社会获取外国资源的能力后，人权组织 OVD－Info 利用众筹来争取支持和筹集小额私人国内捐款[29]。同样，数字技术对于工会履行其核心职能变得越来越重要，包括组织抗议、与成员保持联系以及提供讨论和决策的空间。[30]

26. 许多民间社会团体利用技术来为社会问题寻找创新解决办法。例如，“地标”项目[31] 提供关于世界各地土著人民和地方社区集体拥有和使用的土地的公开地图和其他重要数据，以确保对他们的保护。“目击者”项目开发了技术，以提高民间社会行为者和个人描述和记录侵犯人权行为的能力[32]。开源软件和免费共享空间的发展在很大程度上是由民间社会组织推动的，如 Mozilla 基金会和维基媒体。通过开发“Signal”和“Crabgrass”等平台，以增强民间社会团体数字通信的安全性。难民住区或土著社区的社区网络是民间社会以创新方式解决社会问题的另一个例子。

27. 政府当局应把数字技术视为“在和平集会之前和期间与众多不同受众互动的绝佳机会，以提高当局对自身作用和职能的认识，并最终建立或加强民众对自身的信任”。[33] 同样，各国应认识到技术对促进人民的公众参与权的价值。特别报告员欢迎许多国家政府努力建立在线平台，通过这些平台，感兴趣的人可以提交和收集对于政府政策和立法行动的请愿书签名。

[26] 见人权理事会第 38/7 号决议。

[27] 见 A/HRC/29/32 和 A/HRC/38/35/Add.5。

[28] #Verified19S.

[29] A/HRC/35/28, 第 62 段。

[30] Jeffrey M. Hirsch,“Worker collective action in the digital age”， *West Virginia Law Review*, vol. 117 (2015)，pp. 921–959；and Klaus Schoemann,“Digital technology to support the trade union movement”， *Open Journal of Social Sciences*, vol. 6, No. 1 (2018)，pp. 67–82.

[31] 见 www.landmarkmap.org.

[32] 见 www.eyewitnessproject.org.

[33] A/HRC/23/39, 第 74 段。

28. 这些例子显示了数字技术在享有和平集会和结社权利方面的广泛应用，以及离线和在线领域之间的相互作用。特别报告员注意到，和平集会和结社自由权利的行使经常在网上和网下无缝衔接。例如，许多协会都有办公室，人们面对面交流。与此同时，他们利用数字技术开展日常活动，并作为召开在线讨论和集会的空间。同样，主要基于在线的协会也可以举行面对面的讨论和集会。在线和离线活动的范围取决于协会的成员组成、策略和目标。简而言之，国际法保护和平集会和结社自由的权利，无论是亲自行使，还是通过今天的技术亦或通过未来将会发明的技术行使。[34]

B. 国家限制的趋势

29. 特别报告员感到关切的是，各国使用各种措施和策略来控制和阻碍人们获取和使用数字技术以行使集会和结社自由权。将在线内容定为犯罪的法律持续激增，对宣传和动员产生了显著的寒蝉效应。许多司法管辖区在选举和公众示威期间关闭通信网络和服务，并封锁属于包括人权组织在内的民间社会团体的网站。一些国家——以及恶意的第三方行为者——高度熟练地掌握了新兴技术工具，增加了对民间社会行为者、人权维护者、反对派政治领导人以及计划举行和平公共集会者的数字监控和在线骚扰。所有这些都大大减少了人们捍卫和促进共同利益的空间。值得注意的是，人权理事会表示关切“在重大政治关头出现散布虚假信息和施加不当限制、阻止互联网用户获取或传播信息的新趋势，从而影响人们组织和举行集会的能力”。[35]

30. 本节审查这些国家行动，以确定它们是否符合《公约》第二十一和第二十二条以及这些条款规定的相关分析检测标准。

1. 合法性

31. 如前所述，对和平集会自由权和结社自由权的任何限制都必须有法律依据(分别为“按照法律”或“法律所规定”)[36]，作出限制的当局的任务和权力也必须如此。法律本身必须足够精确，以使个人能够评估自身行为是否违反法律，并预见任何此类违反行为的可能后果。[37]

32. 很多国家越来越多地通过将获取和使用数字工具定为犯罪的法律。这些法律通常以模糊和不明确的术语确立刑事责任，从而可以任意或酌情适用，导致法律不确定性。这样一来，它们就不符合《公约》第二十一和第二十二条确定的允许的限制的法律标准。这方面的例子包括网络犯罪法、反恐法、监控法和反抗议法。

---

[34] Douglas Rutzen and Jacob Zenn,“Assembly and association in the digital age”，*International Journal of Not-for-Profit Law*, vol. 13, issue 4 (December 2011)，p. 67.

[35] 见人权理事会第 38/11 号决议。

[36] 《公约》第二十一条规定，对和平集会权利的行使不得加以限制，除去按照法律而加的限制。第二十二条第 2 款规定，“对此项权利的行使不得加以限制，除去法律所规定的限制”。

[37] A/HRC/20/27, 第 16 段；A/HRC/31/66, 第 30 段。

网络犯罪法

33. 例如，孟加拉国 2018 年《数字安全法》禁止使用电子设备“破坏社区和谐，或制造不稳定或混乱，或扰乱或即将扰乱法律和秩序的状态”[38]，这赋予官员以过度的酌处权，可确定什么构成非法行为，并可基于任意和主观理由对个人提起刑事诉讼。当局可能会将社交媒体上的和平集会呼吁与制造不稳定或破坏社区和谐混为一谈。其他网络犯罪法律赋予政府广泛的权力，可根据广泛宽泛的国家安全概念，封锁被视为批评当局的网站，如属于人权维护者的网站[39]。

反恐怖主义法

34. 任务负责人多次对反恐立法中经常使用过于宽泛的语言表示关切[40]。虽然特别报告员意识到，各国需要保护国家安全和公共安全，这是限制结社和集会自由的合法理由，但这些法律的起草方式往往会给滥用制造机会。例如，许多法律在恐怖主义的定义中包含了宽泛和主观的概念，如“通过政治极端主义广泛传播恐怖”、“严重社会动乱”[41]、“扰乱公共服务”、“煽动示威游行中的暴力”和“在公众中制造恐惧以破坏一个国家的团结”[42]。由于这些概念非常模糊，因而很难比较确定地判定什么样的(在线和离线)行为会被视为“恐怖主义”。被视为宣传或传播大多数人不认同或对当局不利的的观点或信仰的组织和个人尤其容易受到伤害。这会在他们之中产生显著的寒蝉效应，并进一步将它们排除在数字空间之外。

监控法

35. 任务负责人强调，过于宽泛和模糊的监控法往往无法基于合理的怀疑将特定个人作为目标[43]。例如，大不列颠及北爱尔兰联合王国 2016 年的《调查权力法》包含模糊的语言，使得当局可以针对某一群体或某一类人，而不要求对每个监控目标进行单独识别[44]。其他形式的监督法为各国监督公民在线活动大开方便之门，例如澳大利亚的《电信和其他立法修正案》，其中有些条款赋予当局不受约束的权力，可强制公司为安全机构获取加密用户数据提供便利，并削弱加密技术[45]。鉴于许多关于监控的现行法律法规跟不上监控技术及其潜在用途的快速变化，滥用的风险增加了。

---

[38] 见 BGD 4/2018, 可通过以下网址查阅：https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[39] 例见 EGY 13/2017。

[40] A/HRC/26/29, 第 59 段。

[41] 见 BRA 8/2015。

[42] Asian Forum for Human Rights and Development (Forum-Asia)， *Instruments of Repression: A Regional Report on the Status of Freedoms of Expression, Peaceful Assembly, and Association in Asia*, pp. 84 and 89.

[43] 见 A/HRC/35/28/Add.1.

[44] 同上。

[45] 见 AUS 5/2018。

媒体与反“假新闻”法

36. 在与民间社会的协商中，有人对柬埔寨 2018 年 5 月 28 日第 170 号部际法令使用的宽泛语言表示关切，该法令禁止“旨在制造社会动乱”的在线活动。这项规定赋予当局过度的酌处权，可禁止各种在线活动──包括上传警方虐待抗议者的照片和视频，传播呼吁和平示威的信息，还有政治竞选活动。这些规则还规定了严厉的处罚，民间社会组织面临因传播被禁止的内容而被关闭的风险，这与结社自由权不符合也不匹配。此外，这些限制是通过政府法令实施的，从而增加了合法性方面的关切。[46]

示威法

37. 例如，在俄罗斯联邦，“亚罗瓦娅法”对《刑法》提出了过于宽泛的修正案，禁止“诱导、招募或以其他方式让他人参与”组织“大规模动乱”。[47] 在互联网上发表声明被认为是一个加重处罚的因素。与此类似，在哈萨克斯坦，《刑法》禁止向“非法”集会提供“援助”，包括通过“通信手段”[48]。这些条款的宽泛措辞不适当地限制了和平集会、结社和言论自由的权利，有可能使宣传、讨论、寻求或链接有关抗议活动的信息成为犯罪行为。

2. 合法目的

38. 对和平集会和结社自由权的限制必须追求合法目的。《公约》只承认下列目的是合法的：“国家安全或公共安全、公共秩序、保护公众健康或道德或保护他人的权利和自由”。各国不能援引可允许的理由来掩盖非法目的。

在线活动的刑罪化

39. 在世界许多国家，将个人和组织的在线活动定为犯罪成为一个日益增长的趋势[49]。个人经常被指控犯有反恐法、网络犯罪法和反抗议法中定义不清的罪行。例如，越南逮捕并指控一名在互联网上发表批评政府言论的人权维护者[50]。委内瑞拉玻利瓦尔共和国判定一名在社交媒体上呼吁进行反政府抗议的政治反对派领导人犯有煽动暴力罪[51]。阿拉伯联合酋长国逮捕和起诉了人权维护者，指控他们“在互联网上传播虚假和误导性信息，以传播仇恨和宗派主义”[52]，以及利用社交媒体从事《网络犯罪法》规定的“危害国家安全和侮辱统治者”的活动[53]。作为对社交媒体上所发表的评论的报复，埃及逮捕和起诉了一些活动人士，理由是

[46] Inter-American Commission on Human Rights,“Second report on the situation of human rights defenders in the Americas”(OEA/Ser.L/V/II. Doc. 66)，para. 165.

[47] 见 RUS 7/2016。

[48] A/HRC/29/25/Add.2, 第 57 段。

[49] A/71/373, 第 29-35 段。

[50] 见 VNM 1/2017。

[51] 见任意拘留问题工作组第 26/2014 号意见。

[52] 见 ARE 1/2018。

[53] 见 ARE 5/2013。

他们“加入一个违反《宪法》而设立的组织”和“危害国家机构”[54]。在沙特阿拉伯，据报道，沙特公民权利和政治权利协会的一名创始成员被判处 8 年监禁和 8 年旅行禁令，理由是他“煽动公众舆论反对该国统治者，并签署呼吁人们示威的在线声明”，以及“坚持不遵守撤销沙特公民权利和政治权利协会的司法决定”，因此“违反了反网络犯罪法第 6 条”[55]。反对驾驶禁令的沙特妇女人权维护者在与恐怖主义相关的案件中受到起诉，罪名包括“煽动抗议”、“试图煽动公众舆论”和“拍摄抗议并发表到社交媒体上”。[56]

40. 虽然各国在提出这些指控时经常援引国家安全和公共秩序关切，但实际上刑事起诉往往是被用来压制异议和管控在线空间，而这并不是一个合法的政府目标，直接违反了《公约》第二十一和第二十二条。任何人都不应因组织、倡导或参与和平抗议[57] 或为合法目的建立或经营协会而被追究刑事、民事或行政责任。异议是行使和平集会和结社权利的合法组成部分，应当受到保护，包括线上和线下。[58]

任意封锁网上内容

41. 在世界许多地方，包括中东和北非地区的国家，封锁人权组织和政治反对党的整个网站越来越普遍。例如，在阿拉伯联合酋长国和沙特阿拉伯，当局经常封锁包含在线批评的网站。属于民间社会组织和人权团体的网站尤其成为攻击目标，例如 2013 年被封锁的沙特#Women2Drive 运动。同样，埃及当局封锁了几个人权组织的网站[59]。中国使用的防火墙系统地阻止人们访问包含“民主”和“人权”等关键术语的几千个中国境外网站和在线内容。[60]

42. 个人或协会的网站为个人或协会开展下述活动提供了一个重要的手段：倡导一项事业；提出公众关注的问题并促进公众辩论；举报侵犯人权行为；发表研究成果；寻求、接受和传播各种信息和思想；与包括国外组织在内的其他组织建立联盟和网络；进行筹款；招募成员和志愿者；与国际和区域人权机构互动。总体而言，封锁整个网站是一种极端和过分的措施，严重限制了开展这些活动的能力，因此损害了集会和结社自由的行使。在许多情况下，这些措施似乎被不适当地用来针对不同意见，因此，不能以追求合法目标作为其理由。特别报告员认为，“仅以批评政府或政府支持的政治社会制度为由”[61] 禁止个人或协会在网上发布材料不符合和平集会、结社和表达自由的权利。

---

[54] 见 EGY 4/2017。

[55] 见 SAU 4/2016。

[56] 见 SAU 11/2018 以及 SAU/1/2017。

[57] A/HRC/31/66, 第 27 段。

[58] A/HRC/20/27, 第 84 段。

[59] 见 EGY 13/2017。

[60] Freedom House, Freedom on the Net 2018, available from https://freedomhouse.org/report/freedom-net/freedom-net-2018. See also Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012), pp. 31–47.

[61] A/66/290, 第 39 段。

政府资助的喷子和网络攻击

43. 一些国家利用技术来监视和阻碍人权维护者和民间社会行为者的工作。这方面的策略有很多。许多涉及黑客攻击电话和计算机、发布死亡和强奸威胁、传播篡改的图像、暂时中止目标的账户、劫持主题标签、传播阴谋论、指控叛国和宣扬恶毒的歧视情绪。虽然特别报告员意识到国家不是这些行为的唯一肇事者，但政府对这些行为的责任包括委托和鼓励第三方进行这种行为。

44. 这些攻击直接侵犯了个人的和平集会和结社自由权，因为它们不能被视为在民主社会中追求合法目标的行为。他们的目的恰恰相反：恐吓民间社会行为者，摧毁他们的信誉和合法性，并剥夺他们在数字空间进行动员所需的关注。这些攻击削弱了民间社会组织和活动人士分享或接收信息以及与其他人交流的能力。这些攻击促使人们进行自我审查，同时威胁个人的人身安全和完整性。

45. 例如，喷子们被指示开展宣传，孤立或淹没批评观点，抑制反政府运动，同时放大政府官员的信息，增加追随者数量[62]。例如，在阿曼，当局“有系统地侵入在线账户，劫持它们，并向推特等社交媒体无休止地推送大量主题标签，从而扰乱了对特定话题的讨论”。[63]

46. 这一趋势的另一个例子是利用商业间谍软件，如“Finfisher”监控技术和“Pegasus”间谍软件套件，对民间社会行为者发动网络攻击。有记录完整的报告称，“Pegasus”间谍软件套件与针对巴林、哈萨克斯坦、墨西哥、摩洛哥、沙特阿拉伯和阿拉伯联合酋长国等国的活动人士和人权维护者的间谍软件攻击有联系[64]。这些攻击允许黑客侵入并实时监视他们的通信、位置和活动[65]，并可影响一国境内或域外的目标[66]。

47. 另一种使用的技术是对社交媒体团体或论坛进行渗透，通过与活动人士“结交”来跟踪民间社会的在线活动。开源情报还可以通过逮捕那些在网上通报和计划活动的组织者来预先阻止和平抗议。

48. 妇女和女同性恋、男同性恋、双性恋、变性者和双性人尤其容易遭受这些袭击。例如，据报道，埃及政府通过渗透和监督男女同性恋、双性恋、变性者和双性人活动人士在社交媒体平台 Grindr 上的活动，确定并逮捕了他们[67]。巴西当局先利用“Tinder”建立联系，然后对参与抗议的女性活动人士进行监视[68]。在泰国，女性人权维护者在博客和社交媒体上遭到广泛的诽谤、骚扰和死亡威胁[69]。

---

[62] Institute for the Future,“State-sponsored trolling: how governments are deploying disinformation as part of broader digital harassment campaigns”(2018).

[63] A/HRC/29/25/Add.1, 第 34 段。

[64] 例见 the Citizen Lab,“Hide and Seek: tracking NSO Group’s Pegasus spyware to operations in 45 countries”。

[65] 见 LBN 2/2018.

[66] Brief of amici curiae submitted in *John Doe a.k.a. Kidane v. Federal Democratic Republic of Ethiopia* before the United States Court of Appeals for the District of Columbia Circuit.

[67] Article 19,“Apps, arrests and abuse in Egypt, Lebanon and Iran”， February 2018.

[68] Privacy International,“State of privacy Brazil”.

[69] 例见 THA 6/2017。

这些攻击有特定的形式，包括传播篡改的通常是性化和性别化的照片；传播旨在败坏名声的信息，往往充满有害和负面的性别陈规定型观念；社交网络上发表暴力仇恨信息和威胁性信息，包括呼吁进行轮奸和谋杀；侵犯隐私，包括侵入家庭成员的电脑和电话，暴露电话号码、家庭地址以及个人和家庭照片。任务负责人赞同暴力侵害妇女及其原因和后果问题特别报告员的调查结论，即对妇女的网上虐待是对妇女影响力和充分参与公共生活的直接攻击，应予以应有的调查和惩罚[70]。

3. 保护合法目标所必需和适度的

49. 《公约》第二十一条和第二十二条第 2 款规定，对和平集会和结社自由的限制应当是在民主社会中为维护国家安全或公共安全、公共秩序，保护公共卫生或道德或他人的权利和自由所必需和适度的限制。有人指出，在本特别程序任务下，“必需|”一词意味着必须有“进行干预”的迫切的社会需要。当出现这种紧迫的社会需要时，各国就必须确保任何限制性措施都在民主社会所能接受的限度之内，而民主社会“只有在多元化、宽容和思想开放的情况下才存在”[71]。确定存在正当理由的责任始终在于国家。

50. 国家往往通过就所援引的具体威胁而言既不必要也不相称的限制来阻碍在线行使集会和结社自由。这方面的一些例子包括中断网络、国家强制封锁在线内容、社交媒体税和使用数字技术的监控。

中断网络

51. 数据表明[72]，2018 年至少有 40 起网络中断与公众示威及和平抗议有关，2017 年有 37 起，2016 年有 27 起。受影响最大的地区是亚洲和非洲，印度[73]、伊朗伊斯兰共和国[74]、乍得[75]、喀麦隆[76] 和多哥[77] 均有互联网关闭或社交媒体被禁的案例报告。2016 年至 2018 年，仅印度就发生了 64 起与公众示威有关的网络中断事件。据报道，世界其他地区也发生了针对和平集会的网络中断事件，这表明这已成为一种危险的全球趋势。自 2016 年以来，选举期间网络中断和社交媒体禁令的数量也在增加，严重影响了反对党和社会运动的影响力和在关键时刻动员支持的能力。这些措施影响人权维护者开展工作和记录侵犯人权行为的能力。[78]

---

[70] 见 A/HRC/38/47。

[71] A/HRC/20/27, 第 17 段。

[72] Access Now, #KeepitOn campaign，and Shutdown Tracker Optimization Project (STOP).

[73] 见 IND 5/2016, IND 3/2017 和 IND 7/2017。

[74] 见 IRN 1/2018。

[75] 见 TCD 3/2016。

[76] 见 CMR 1/2018。

[77] 见 TGO 1/2017。

[78] A/68/299, 第 28 段。

52. 特别报告员认为，关闭网络明显违反国际法，在任何情况下都没有正当理由。关闭不符合《公约》第二十一条规定的限制和平集会权和第二十二条第 2 款规定的限制结社自由权的既定标准。在大多数情况下，网络关闭命令缺乏法律依据。即使有法律依据，关网的命令往往伴随着宽泛而模糊的规定，缺乏适当的独立监督[79]。尽管这些措施通常以国家安全和公共秩序为理由，但对于实现这些合法目标来说，它们是过分而且通常是无效的手段。

53. 这些极端措施对人权、经济活动、公共安全和应急服务造成了各种各样的损害，超过了声称的好处。网络中断经常适得其反，导致混乱和动荡。在抗议和选举时期，当紧张局势达到顶点时，实际上正需要这些工具来防止虚假信息和驱散谣言，并保护自由和人身完整的权利，因为它们可使人们获得紧急帮助并与家人和朋友联系[80]。人权理事会明确表示关切“违反国际人权法、旨在或有意阻止或干扰在网上获取或传播信息的措施”[81]。

社交媒体税

54. 特别报告员感到关切的是，一些国家最近对使用社交媒体征税，这可能过多地影响弱势群体行使结社和集会自由的能力，而且这些“社交媒体税”可能引起必要性或相称性方面的关切。例如，乌干达的社交媒体税“过度和负面地影响到用户获得负担得起的互联网接入的能力，从而不适当地限制了他们的言论自由权以及和平集会和结社的权利——特别是对低收入公民而言，他们每月购买 1 GB 的数据将花费他们平均月收入的近 40%”[82]。虽然这些税收可能有合法的经济理由，但各国应采取措施，确保税收不会过度妨碍个人与社会其他成员交流的能力，也不会扩大数字鸿沟。

使用数字工具进行监控

55. 过去十年来，全球范围内不必要和过度的监控措施有所增加。必要性要求意味着需要证明监视将如何实现既定目的，而监视行为本身往往会损害这一目的。例如，澳大利亚和联合王国等国声称，国家安全或公共秩序可作为削弱加密工具的正当理由[83]。正如促进和保护意见和表达自由权特别报告员所指出的，“信息安全专家普遍认为，这种削弱给整体数字安全带来了巨大的成本，因为它们可能会被未经授权的第三方利用，即使它们本意只是供政府使用”。[84]

56. 相称性原则要求证明所使用的措施是侵入性最小的选择。对所有通信元数据的大规模监控或大规模收集和分析[85] ——明确针对个人之间的联系——本质上是

[79] 见 A/HRC/29/25/Add.2.

[80] Jan Rydzak, Global Network Initiative, “Disconnected: a human rights-based approach to network disruptions”.

[81] 见人权理事会第 38/7 号决议。

[82] 见 UGA 3/2018.

[83] 见 A/HRC/35/28/Add.1.

[84] 见 A/HRC/38/35/Add.5。

[85] 元数据是指与一次通信有关的信息，如地理位置、通信时长和通信各方。

不相称的[86]。同样，不加区别地一律要求通信服务提供商在本地存储个人和敏感数据和登记 SIM 卡的法律要求使当局可以获取与任何严重犯罪或具体威胁无关和并不重要的信息[87]。强制性 SIM 卡登记法尤其“事实上要求大多数人口向有关国家透露个人身份信息”[88]。大型文化活动、大型体育赛事、音乐节和政治集会中使用的人脸识别技术也引发了相称性问题。同样，国际移动用户身份捕捉设备(IMSI 捕捉器) [89] 使各国在特定地区或政治示威等公共活动中从数千部移动电话中收集数据。这种做法被用来识别和监视所有参加特定活动或出现在特定公共场所的个人[90]。这些形式的身份识别和数据收集侵犯了个人在公共场所的匿名性，并对参与公共集会的决定产生显著的“寒蝉效应”。[91]

57. 应当禁止在实体和数字空间使用监视技术对行使和平集会和结社权利的人进行不加区别和不分目标的监视。对行使和平集会和结社权利的个人的监视只能有针对性地进行，即有合理的理由怀疑他们正在从事或计划从事严重的刑事犯罪的情况下，并且根据非常严格的规则，依照必要性和相称性原则进行，并规定严密的司法监督。

C. 数字技术公司：重大关切

58. 由于控制了在线平台和工具，这些公司很可能收到来自国家的获取用户数据的要求。有时，这种要求可能以非正式要求或压力的形式出现。如果国内法违反国际人权标准和规范，公司就会面临相互矛盾的法律义务，威胁到它们对人权的遵守以及它们在某些司法管辖区开展业务的能力。这可能导致用户和平集会和结社的权利受到侵犯，并引起透明度和问责制方面的问题。世界各地的公司经常不能充分披露关于数据收集和政府要求的信息。[92] 来自美国和欧洲的主要全球数字技术公司发布的透明度报告是积极的例子，应当扩大和改进。

59. 在线平台根据自己的社区标准对内容进行审核的方式也引发人权关切，包括和平集会和结社权利方面的关切。特别是，社交媒体公司的内容政策反映了对什么是可接受的表达和行为的不同解释，而这些解释可能不符合国际人权标准和规范。此外，通过内容审核来执行这些内容政策的方式也可能不符合人权标准，并引发任意干涉的问题，尽管存在一些改进的尝试。内容政策的实施似乎也更多地影响了那些具有公众影响的人。事实上，通过依靠用户举报违反社区标准的行为(即社区警务)和执行内容政策，使活动人士和呼吁群众发动起来的人们面临内容

[86] 见人权理事会第 34/7 号决议。

[87] A/HRC/29/32, 第 51 段；A/HRC/35/22, 第 20 段。

[88] 同上。

[89] 见 A/HRC/35/28/Add.1。

[90] The Human Rights, Big Data and Technology Project,“The Universal Declaration of Human Rights at 70: putting human rights at the heart of the design, development and deployment of artificial intelligence”， 20 December 2018, p. 31.

[91] Daragh Murray and Pete Fussey,“Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data”， *Israel Law Review*, vol. 52, issue 1.

[92] Ranking Digital Rights, The Ranking Digital Rights 2018 Corporate Accountability Index, chap. 3,“Inadequate disclosure”.

遭到任意删除和账户被暂停或停用风险。那些有公共影响力的用户不仅比知名度低的用户更有可能被举报(鉴于他们的影响力)，而且经常面临针对自身、旨在删除内容和封锁账户的一些运动。使用人工智能进行内容审核使这一问题更加复杂，因为平台越来越多地使用自动化过程来标记需删除的内容。

60. 算法系统也被用来影响材料的可发现性、可见性和可访问性——也就是说人们看到了什么内容，他们与谁联系，他们找到了什么群体。这意味着内容的提供可以基于历史或推断的政治派别或其他联系，对于那些试图接触特定受众并与志同道合者交流的人来说，这可能是一项资产，但也是有问题的。算法系统能够让故事和运动息声，阻止民间社会行为者接触更广泛的受众，放大志同道合者的声音或复制偏见和歧视，从而损害民主的发展。这些措施还会更多地影响到已被边缘化或面临风险的群体，包括妇女[93]。算法系统模糊不清，不断变化，影响着个人和群体在网上的影响力，而他们“无法调查或理解为何、如何或基于何种依据”。[94]

61. 关于用户隐私和通信安全的政策和内容也可能影响和平集会和结社权利的享有。只有少数数字技术公司允许使用假名或以其他方式来掩盖个人身份，或提供加密通信。特别报告员欢迎社交媒体平台 Grindr 努力在其平台上设计和推出安全功能，帮助保护埃及、伊朗伊斯兰共和国和黎巴嫩面临警察骚扰、酷刑和监禁的男女同性恋、双性恋、变性者和双性人。

62. 一些数字技术公司已经做出一些努力，将表达自由权和隐私权纳入风险评估和尽职调查进程，但特别报告员注意到，和平集会和结社自由权尚未得到考虑。在与数字技术公司的会晤中，他能够确定许多此类公司承认这些权利在民主社会中的价值和重要性，但尚未在这方面作出高级别政策承诺。

63. 特别报告员呼吁数字技术公司履行责任，尊重国际公认的人权标准，包括和平集会和结社自由权。为此，切实执行《工商业与人权指导原则》应该成为这些公司的优先事项。应逐步推广包含独立影响评估监督的模式，如全球网络倡议所倡导的模式[95]。数字技术公司应做出尊重和平集会和结社权利的政策承诺(在尊重表达自由和隐私权的现有承诺之外)，在涉及这些基本自由的问题上进行尽职调查，包括定期开展人权影响评估，并建立有效的补救程序，在侵权行为发生时提供赔偿和其他形式的补救。各国应通过和执行法律和政策，重点是强制要求数字技术公司进行尽职调查，以查明、预防、减轻和说明自己如何应对其企业和产品的人权影响，并规定建立健全的透明度和补救机制。这些法律和政策必须“以普遍获得和享有人权为核心目标”[96]，并符合源于国际标准和规范的指导原则。这些法律和政策必须在与相关利益攸关方进行具有充分包容性和参与性的协商后才能予以通过。

[93] A/HRC/35/9, 第 41 段。

[94] A/73/348, 第 32 段。

[95] 全球网络倡议是 2008 年推出的一个多利益攸关方平台，旨在“通过设立一套负责任公司决策全球标准，在信通技术产业保护和推进表达自由和隐私权”。见 https://globalnetworkinitiative.org/team/our-mission/。

[96] 人权理事会第 38/7 号决议，第 18 段。

64. 特别报告员认为，国际人权法框架应规范数字技术公司对政府请求的回应、内容审核和工程方案选择，包括内容的计算策略。这意味着对于公司那些影响和平集会和结社权利的决定要适用合法性、必要性和正当性标准。特别报告员援引促进和保护意见和表达自由权特别报告员最近关于在线平台内容审核和人工智能的报告，其中详细阐述了这些问题的复杂性和规模，并提出了重要建议。[97]

五. 结论和建议

65. 数字时代为享有和平集会和结社自由权开辟了新的空间，但也给这些基本权利带来了一系列新的威胁和风险。例如，严格的法律限制和政府在数字监控方面的做法有可能消灭民间社会可以集体促进或捍卫共同利益领域的空间。数字技术公司的行动和不作为加剧了这些风险，或者给寻求在线和离线行使集会和结社权利的个人和组织带来了复杂的新挑战。在日益数字化的未来，这些挑战可能会加剧。

66. 国际法保护和平集会和结社自由的权利，无论是亲自行使，还是通过今天的技术行使，还是通过未来将发明的技术行使。现有的国际人权规范和原则不仅应规定国家行为，而且应成为指导数字技术公司设计、管控和治理数字技术的框架。

67. 各国应根据国际法，确保和平集会和结社的权利在国家法律框架、政策和实践中得到尊重、保护和实施。数字技术公司必须承诺尊重和平集会和结社自由，并进行尽职调查，以确保自身不会导致、促成或共谋侵犯这些权利。国家和数字技术公司在履行各自的责任时，应遵守不歧视、观点多元化、透明、多方利益攸关方参与和有机会诉诸司法的既定原则。

68. 为此，特别报告员提出以下建议：

A. 对各国的建议

69. 国家应确保对和平集会和结社自由权的任何干涉都是“法律规定的”，并且是“民主社会为了国家安全或公共安全、公共秩序、保护公众健康或道德或者保护他人的权利和自由所必需的”[98]。对基于“国家安全”、“公共安全”和“道德保护”理由的限制应作明确和狭义地界定，以防止当局滥用这些限制。

70. 国家应促进和便利获取数字技术，不应限制其用于行使和平集会和结社自由权。政策和做法应解决互联网和数字技术的平等获取、可负担性和人人普遍参与数字时代的问题，以弥合数字鸿沟。

71. 在线结社和集会对边缘化群体发挥着特别重要的作用，对和平集会和结社自由权的干涉会更多地影响到处于弱势地位的个人和群体。国家在履行自身的义务时应特别注意，对获取和使用数字技术的限制可能对种族和宗教少数群体、政治反对派和活动人士以及男女同性恋、双性恋、变性者和双性人产生的不同影响。

[97] A/HRC/38/35, 第 61 段。

[98] 人权理事会第 15/21 号决议，第 4 段。

72. 国家应确保所有人都能获得和使用对侵犯和平集会和结社自由权的行为有效的补救措施。对受影响的权利持有人来说，补救措施应当是可获得、可负担、充分和及时的。国家应通过独立的司法、行政或立法当局或法律制度规定的任何其他独立主管当局提供补救。

73. 国家应通过以下方式为数字时代的和平集会和结社权利创建一个有利的法律框架：

(a) 废除或避免出台不适当地限制或损害和平集会和结社自由权的法律，包括反抗议法；

(b) 废除和修正任何允许中断和关闭网络的法律和政策，并避免通过此类法律和政策；

(c) 修订和修正网络犯罪法、监视法和反恐法，使其符合关于隐私权、意见和表达自由权、和平集会自由权和结社自由权的国际人权规范和标准；

(d) 促进和保护严格的加密和匿名性，包括通过法律、法规和政策，规定只将取消匿名权的权力授予法院而不是执法机构。

74. 避免并停止诸如切断互联网和电信服务的措施。应始终保持互联网和移动电话服务，包括在内乱时期。应特别尊重、保护和促进选举期间为集会和结社目的获取和使用数字技术。

75. 停止一切封锁民间社会组织和人权维护者网站的做法。

76. 禁止使用监视技术对在实体空间和网上行使和平集会和结社权利的人进行不加区别和不分目标的监视。

77. 避免使用数字工具对民间社会行为者、抗议组织者、少数群体和其他寻求行使和平集会和结社自由权利的人进行不当的定向监视。可允许的定向监视只能在满足以下条件的基础上进行：公开进行这种活动；有时间限制；依照符合法律规定、出于正当目的、必要性和相称性等国际标准开展；接受持续的独立监督，包括严格的事先批准、业务监督和审查机制。如果个人和群体的权利受到监视侵犯，应予以告知并应保障有效的补救措施。

78. 任何新形式技术监督的应用都应遵守上述原则和标准——包括域外监督。国家应进行独立的调查，审查任何监视技术的使用情况，以便公众能够评估使用这些技术的方式和频率、使用的理由、必要性和相称性，以及这些技术是否被不当或过于广泛地使用。

79. 结束所有政府支持的针对民间社会行为者的在线乱喷、恐吓和造谣行为。国家应调查这些行为，提供有效的补救措施，并采取和实施预防措施。在这方面，国家应查明并解决基于性别的在线暴力形式和阻碍妇女诉诸司法的障碍。

80. 国家应尽职履行保护和平集会和结社自由权不受工商企业侵犯的义务，采取适当步骤，通过有效的政策、立法、条例和裁决防止、调查、惩罚和纠正这种侵权行为。这方面包括通过和执行法律和政策，重点是强制要求数字技术公司开展尽职调查，以确定、预防、减轻和说明它们如何应对其商业服务和产品的任何人权影响，并要求建立健全的透明和补救机制。这些法律只有在与所有利益攸关方进行具有充分包容性和参与性的协商后才能予以通过。

81. 国家应重申承诺采取多方利益攸关方的办法，这是互联网治理进程的基石。在数字领域相关问题上的有效合作取决于个人和团体行使和平集会和结社自由权利的能力。

B. 对数字技术公司的建议

82. 公司应履行尊重国际公认的人权，包括和平集会和结社自由权的责任，采取一切必要和合法的措施，确保自身不会导致、助长或共谋侵犯人权。

83. 公司应作出高级别政策承诺，尊重和平集会和结社自由，并承认民间社会在民主和可持续发展中的重要作用。

84. 每当国家要求公司审查、监视或监测个人或团体，或提供公司所收集、处理或保留的数据时，公司应在法律允许的最大限度内，努力防止或减轻自身的参与对人权的不利影响。

85. 公司应承认国际人权法是确保自身产品和服务尊重和平集会和结社权利的权威框架，并应据此评估自己的政策。公司应确保自身的政策和社区准则足够清楚、易于获取并符合国际人权标准。公司还应提供更详细的例证或案例研究，说明自己的社区标准如何在实际中得到应用，以便用户能够了解个人数据或信息可能被访问、内容可能被限制或对服务的访问可能被阻止或限制的情况。

86. 公司应开展人权尽职调查，以查明、预防、减轻和处理侵犯和平集会和结社权利的行为，包括：

(a) 开展人权影响评估，在开发或修改其产品和服务时纳入和平集会和结社自由权。评估影响的过程应始终包括与民间社会行为者和其他专家的磋商，并由具有人权专门知识的经认可的外部第三方进行验证。

(b) 通过采取以下步骤，整合影响评估结果：通过向管理层、雇员和承包商等其他有商业联系的行为者提供培训和发布指导方针，提高对和平集会和结社权利的了解和意识；通过政策和程序，规定公司将如何评估和响应政府对通信或内容访问限制的要求；将预警系统纳入业务流程，以确定人权风险，并及时做出反应；利用自身的影响力挑战不当限制和平集会和结社自由权的政府请求；支持研究和开发针对在线骚扰、虚假信息和宣传的适当技术解决方案，包括发现和识别与国家有联系的账户和网上机器人程序的工具；采用监测指标，其中包括与和平集会和结社自由有关的具体关切。

87. 公司应采取有效措施，确保其政策和做法的透明度，包括服务条款和基于计算的审查程序的采用情况，并尊重正当程序保障。为此，公司应在其官方网站上定期发布信息，说明政府和其他第三方所提请求的法律依据、所满足请求的数量或百分比，根据公司自己的政策和社区指南限制或删除的内容或账户。

88. 公司应引入独立的监督机制来监控内容审核决定的结果，各国应考虑制订要求这种独立监督的条例。

89. 公司应与受影响的社区进行有意义的协商，建立运营层面的申诉机制，这些机制应明确具备和可用，并且在流程和补救结果方面有效。

90. 公司应加入现有多方利益攸关方倡议并提高参与和实施的质量。参与的公司应在这些倡议的框架内加强自身在尊重和平集会和结社自由权方面的作用。

91. 公司应与政府和民间社会合作，开发促进和加强人权的技术。

C. 对民间社会的建议

92. 民间社会行为者应继续创新，并与政府、公司和学术界结成伙伴关系，开发有利于行使和平集会和结社自由权的技术。

93. 民间社会行为者应确保数字安全和数字扫盲是所在组织活动的核心。

94. 民间社会行为者应扩大和改善对结社和集会权利的数据收集和数字威胁的记录：特别是在法律发展、网络中断、监控、在线骚扰和虚假信息宣传方面。他们应该分享知识，倡导数据收集标准，并在这些努力中与其他利益攸关方合作。

95. 所有民间社会团体，不仅仅是数字权利组织，都应该支持并参与理解对公民空间的数字威胁和制定有效应对威胁的进程。

D. 对人权事务委员会的建议

96. 在拟订关于《公民权利和政治权利国际公约》第二十一条的一般性意见时考虑到本报告。