联 合 国 A/HRC/27/37

大 会

Distr.: General
30 June 2014
Chinese
Original: English

人权理事会
第二十七届会议
议程项目 2 和 3
联合国人权事务高级专员的年度报告和高级专员办事处及秘书长的报告

增进和保护所有人权——公民权利、政治权利、经济、社会和文化权利，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

大会第 68/167 号决议请联合国人权事务高级专员向人权理事会第二十七届会议和大会第六十九届会议提交一份报告，说明在国内及域外监控和/或截获数字通信以及收集个人数据情形下，包括大规模进行的情形下保护和促进隐私权的问题，并提出意见和建议，以供会员国审议。本报告应此要求提交。高级专员办事处还将根据大会的要求，将报告提交大会第六十九届会议。

GE.14-06870 (C) 050814 060814
1406870

目录

一. 导言

1. 互联网、移动智能手机和无线上网装置等数字通信技术已成为日常生活的组成部分。通信技术领域的创新通过大幅度改进获取信息的途径和实时通信，推动言论自由，为全球辩论提供便利，并加强了民主参与。这些强有力的技术通过放大人权维护者的声音以及为他们提供记录和曝光不法行为的新的工具，为促进享有人权带来了希望。由于当代人的生活越来越离不开网络，互联网无处不在，隐私性越来越强。

2. 数字时代的通信技术还促进了政府、企业和个人监控、截获和收集数据的能力。正如言论和见解自由权问题特别报告员指出，技术进步意味着国家进行监控的效力不再受到规模或持续时间的限制。技术和数据存储成本的不断下降使进行监控的资金和实际阻碍因素不复存在。国家进行实时、侵入性、定点和大规模监控的能力比以往任何时候都强。[1] 换句话说，全球政治、经济和社会生活所日益依赖的技术平台不仅容易受到大规模监控，事实上还可能为这类监控提供便利。

3. 随着全球许多国家利用数字通信技术在电子监控和截获数据方面的脆弱性而制定政策和做法事件的曝光，使人们产生了深切的担忧。全球各国公开和秘密的数字监控行为层出不穷，政府大规模监控已成为一项危险的习惯而非例外措施。据报告，一些国家政府向电信和无线设备公司发出威胁，除非它们提供直接接触网络内容的途径，允许出于监控目的窃听光纤电缆，否则将禁止其提供服务，还要求这些公司一致披露有关其顾客和雇员的批量信息。此外，据报告，一些国家利用通信网络监控手段对付政治反对派成员和/或政治异见者。有报告称，一些国家当局长期对所有电话内容录音，并保留用作分析，一些东道国政府对全球活动的通信内容进行监测。据报告，一个国家当局要求在该国销售的所有个人电脑配备可能具有其他监控能力的过滤软件。据称甚至一些非国家团体也在建设非常复杂的数字监控能力。大规模监控技术已进入全球市场，加大了数字监控摆脱政府控制的可能性。

4. 2013 年和 2014 年曝光的事件显示，美利坚合众国国家安全局和大不列颠及北爱尔兰联合王国通讯总部合作研制技术，获取大量全球互联网内容，提取在美国的记录、个人电子通讯录及大量其它数字通信内容，事件曝光使人们更加深感忧虑。据报告，这些技术是通过跨国网络部署的，包括政府之间的战略情报合作、对私营公司的监管控制及商业合同。

5. 由于会员国和其它利益攸关方对这类监控作法对人权的负面影响深表关切，大会于 2013 年 12 月未经表决通过了关于数字时代的隐私权的第 68/167 号决议。该决议由 57 个会员国联合提出，大会在决议中申明人们在网下享有的各种

[1] A/HRC/23/40, 第 33 段。

权利也应在网上受到保护，并促请所有国家尊重并保护数字通信方面的隐私权。大会还促请各国审查其涉及通信监控和截获以及个人数据收集的程序、做法和立法，强调国家应确保充分而有效地履行其按照国际人权法承担的义务。

6. 大会还在第 68/167 号决议中请联合国人权事务高级专员向人权理事会第二十七届会议和大会第六十九届会议提交一份报告，说明在国内及域外监控和/或截获数字通信以及收集个人数据的情形下，包括大规模进行的情形下保护和促进隐私权的问题，并提出意见和建议，以供会员国审议。本报告按照此要求提交。高级专员办事处(人权高专办)还将根据第 68/167 号决议的要求，将报告提交大会第六十九届会议。

二. 背景和方法

7. 人权高专办铭记第 68/167 号决议的要求，参加了一些活动并从各种资料来源收集信息。2014 年 2 月 24 日，高级专员在题为“数字时代的隐私权”的专家研讨会上作主旨发言，该研讨会由奥地利、巴西、德国、列支敦士登、墨西哥、挪威和瑞士主办，由日内瓦国际人道主义法和人权学院主持。

8. 2013 年 11 月至 2014 年 3 月，人权高专办请联合国大学参加关于在政府数字监控的国家制度中适用国际人权法的研究项目。人权高专办对联合国大学表示感谢，承认大学通过该研究项目，为编写本报告作出了重大实质性贡献。

9. 作为公开磋商的一部分，人权高专办于 2014 年 2 月 27 日通过会员国驻日内瓦和纽约常驻代表团向它们发出一份调查问卷，同时向一些国际和区域组织、国家人权机构、非政府组织和企业实体发出调查问卷。人权高专办在调查问卷中请它们就大会在第 68/167 号决议中处理的问题提供投入。人权高专办创办了专门网页，以便就调查问卷和所有投入进行公开磋商，以及为投入提供更多机会。共收到来自所有地区 29 个会员国、5 个国际和/或区域组织、3 个国家人权机构、16 个非政府组织和 2 个私营部门的答复。[2]

10. 许多答复详细介绍了现有国家法律框架和为确保在数字时代尊重和保护隐私权采取的其他措施，以及为制定和落实程序性保障和有效监管采取的举措。一些答复提及在落实数字时代的隐私权方面遇到的挑战，提供了可在国际层面采取举措的建议。这些建议包括鼓励人权事务委员会更新相关一般性意见，尤其是关于《公民权利和政治权利国际公约》第十七条的一般性意见；由人权理事会设立关于隐私权的特别程序任务；及/或由现有相关特别程序任务负责人联合或单独采取举措，处理与在数字监控背景下的隐私权相关的问题，并提供良好做法指导。

[2] 所有答复，见 www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

11. 依照大会第 68/167 号决议的要求，本报告基于对拟定报告时可用资料的评估，提供一些反思和建议，同时还参考了收到的各类答复所反映的丰富内容。

三. 与数字时代的隐私权相关的问题

12. 正如大会在第 68/167 号决议中重申，国际人权法为评估对个人隐私权的干涉行为提供了普遍框架。《世界人权宣言》第十二条规定：“任何人的私生活、家庭、住宅和通信不得任意干涉，他的荣誉和名誉不得加以攻击。人人有权享受法律保护，以免受这种干涉或攻击。”迄今为止已得到 167 个国家批准的《公民权利和政治权利国际公约》第十七条规定：“任何人的私生活、家庭、住宅或通信不得加以任意或非法干涉，他的荣誉和名誉不得加以非法攻击”。该条还声明：“人人有权享受法律保护，以免受这种干涉或攻击”。

13. 其它国际人权文书载有类似条款。区域和国家层面的法律也规定所有人的私人和家庭生活、住宅和通信受到尊重的权利，或承认和尊重其尊严、人身完整或名誉的权利。换句话说，隐私权和确保隐私权在法律和实际中受到保障的必要性、其根本重要性和持久相关性得到普遍承认。

14. 虽然本报告的任务重点在于讨论隐私权，但应强调的是，其他权利也可能因大规模监控、截获数字通信内容和收集个人数据行为而受到影响。这些权利包括意见和言论自由权、寻求、接受和传递信息的自由权；和平集会和结社自由；家庭生活权——所有这些权利都与隐私权密切相关且越来越多地通过数字媒体行使。健康权等其他权利也可能受到数字监控做法的影响，例如：一个人可能害怕自己的匿名身份暴露，因此不愿意寻求或传递与健康相关的敏感信息。有可信资料表明，数字技术被用于收集信息，进而导致酷刑和其他虐待行为。还有报告表明，来自电子监控的元数据被用于分析，以识别目标地点，用于致命的无人机打击。这类打击一直令人对遵守国际人权法和人道主义法的状况以及对相关侵权行为追究责任等问题提出严重关切。大规模监控与对人权造成的其他这类影响之间的关系虽然超越了本报告的范围，但值得进一步探讨。

A. 私生活、家庭、住宅或通信免受任意或非法干涉的权利

15. 一些答复强调，对电子通信数据的监控行为如果遵守法律，包括国际人权法，就可能成为合理执法或收集情报方面的必要和有效措施。然而，曝光的有关大规模数字监控事件提出了一些问题，即这类措施在多大程度上符合国际法律标准，以及是否需要更强的监控保障，以防止人权受到侵犯。具体而言，监控措施不得任意或非法干涉任何人的私生活、家庭、住宅或通信；政府必须采取具体措施，确保提供法律保护，防止发生这类干涉行为。

16. 对所收到的不同答复的审查表明，处理这些问题需要对以下要点进行评估：在数字通信背景下哪些行为构成干涉隐私？“任意和非法”的含意；哪些

人的权利受到国际人权法的保护？以及在何处受到保护？以下各节讨论不同答复中强调的问题。

1. 干涉隐私

17. 国际和区域人权条约机构、法院、委员会和独立专家都提供了与隐私权的范围和内容相关的指导，包括“干涉”个人隐私的含意。人权事务委员会在第16号一般性意见中强调，要遵守《公民权利和政治权利国际公约》第十七条，就必须在法律上和实际上保障通信的完整和机密。“信件应送达收信人，不得拦截、启开或拆读”。[3]

18. 有人认为，通过电子手段传输和交流个人资料是一种有意识的妥协，表明个人自愿交出有关自身及其关系的信息，以换取通过数字手段获得商品、服务和信息。然而，这一行为引发了严肃的问题，即消费者究竟在多大程度上真正了解他们共享了哪些数据，如何共享、与谁共享，以及这些数据用于何种用途。根据一份报告，“有关大量数据的一个现实是，一旦数据被收集起来，就很难使其保持匿名身份。虽然存在一些前景可观的研究努力，旨在在大量数据背景下对可识别的个人信息进行模糊处理，但目前却投入了更多努力，用于重新识别看似‘匿名’的数据。用于数据整合能力的总体投资数倍于可加强隐私的技术投资”此外，该报告的作者指出：“侧重于控制对个人数据的收集和保留虽然重要，但可能已不足以保护个人隐私”，其部分原因是“大宗数据使得新的、并非显而易见但以出人意料的强大方式使用数据成为可能”。[4]

19. 同样，也有人认为截获或收集有关一份通信的数据与通信内容相反，其本身并不构成干涉隐私。从隐私权的角度来看，这一区分不具有说服力。对通常被称为“元数据”的资料进行整合，可能使人窥见一个人的行为、社会关系、个人喜好以及身份，这方面的内容甚至超越通过获取私人通信内容所获得的信息。欧洲法院近来指出，通信中的元数据“作为一个整体，可用于非常确切地总结被保留数据的个人的私人生活。”[5] 承认这一发展已促进对现有政策和做法进行改革以确保加强保护隐私的举措。

20. 此外，采集通信数据是对隐私的潜在干涉，而收集和保留通信数据则构成对隐私的干涉，不论这些数据后来是否被参考或使用。即使通信信息被采集的可

[3] 大会正式记录，第四十三届会议，补编第40号(A/43/40)，附件六，第8段。

[4] 美国总统行政办公室，“大宗数据：抓住机会，保存价值”，2014年5月(见：www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf)，第54页。

[5] 欧洲联盟法院，对C-293/12和C-594/12号联合案件的判决，爱尔兰数字权利和Seitlinger及其他人，2014年4月8日的判决，第26-27段及37段。另见，总统行政办公室，“大宗数据及隐私：技术视角”(见：www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014pdf)，第19页。

能性已造成干涉隐私，[6] 它对权利，包括对言论和结社自由权产生潜在的“寒蝉效应”。大规模监控方案只要存在，即构成对隐私的干涉。国家有责任表明这类干涉既不是任意的，也不是非法的。

2. 何为“任意”或“非法”？

21. 只有在并非任意或非法的情况下干涉个人隐私权受到国际法的许可。人权事务委员会在第 16 号一般性意见中解释指出，“非法”一词的意思是“除法律所设想的个案以外不得有干涉情事。国家授权的干涉必须根据法律，但法律本身必须符合《公约》的规定和目标”。[7] 换句话说，如果国内法与《公民权利和政治权利国际公约》的条款相冲突，则该国内法律所允许的干涉也是“非法的”。“任意干涉”一词也可推广引申，使之适用于法律所规定的干涉。委员会解释说，使用这个概念“的用意是确保法律所规定的干涉都符合《公约》的规定和目标，而且无论如何要在个别情况中合情合理”。[8] 委员会将合理性的要求解释为“对隐私的任何干涉都必须与所追求的目标成比例，应当为任何特定案件情节所必须”。[9]

22. 与《公约》其它某些条款不同的是，第十七条不包括明确的限制条款，但对“任意性或非法”这些限定词语含意的指导可参考“关于《公民权利和政治权利国际公约》的各项限制条款和可克减条款的锡拉库扎原则”；[10] 人权事务委员会的做法，体现于委员会第 16、27、29、34 和 31 号一般意见，对个人来文的结论，[11] 以及结论性意见；[12] 区域和国家判例法；[13] 及独立专家的意见。[14] 例如，人权事务委员会在关于《公约》缔约国的一般法律义务的性质的第 31 号一般性意见中规定，缔约国不得侵犯《公约》所承认的权利，“只有在符合《公约》有关条款的情况下才能对其中的权利进行限制。在进行限制时，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

[6] 见欧洲人权法院，Weber 和 Saravia 诉德国，第 78 段；Malone 诉联合王国，第 64 段。

[7] 大会正式记录(见脚注 3)，第 3 段。

[8] 同上，第 4 段。

[9] 第 488/1992 号来文，Toonan 诉澳大利亚，第 8.3 段；另见第 903/1999 号来文，第 7.3 段，和第 1482/2006 号来文，第 10.1 和 10.2 段。

[10] 见 E/CN.4/1985/4,附件。

[11] 例如，第 903/1999 号来文，2004 年，Van Hulst 诉荷兰。

[12] CCPR/C/USA/CO/4。

[13] 例如，欧洲人权法院，Uzun 诉德国，2010 年 9 月 2 日；Weber 和 Soravia 诉德国，第 4 段；及美洲人权法院，Escher 诉巴西，判决，2009 年 11 月 20 日。

[14] 见 A/HRC/13/37 和 A/HRC/23/40。另见“在通信监控中适用人权的国际原则”，见 https://en.necessaryandproportionate.org/text。

保护《公约》权利。”[15] 委员会还强调，“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”。

23. 这些权威资料来源凸显出合法性、必要性和相称性的总体原则，收到的许多答复也强调了这些原则。首先，对第十七条规定的隐私权施加任何限制必须由法律作出规定，而法律必须便于了解把握，足够清楚和确切，使任何一名个人都能够参考法律确定哪些人有权力以及在何种情况下进行数据监控。施加的限制对于实现合理目标而言必须是必要的，并且与目标相称，采用侵入性最小的办法。[16] 此外，对权利施加的限制(例如，出于保护国家安全或他人生命权的目的干涉隐私)必须能够表明有实现目标的可能性。限制权利的当局有义务表明施加的限制与合法目标相关。此外，对隐私权的限制不得使权利的实质失去意义，同时必须遵守其他人权，包括禁止歧视。施加的限制如果不符合这些标准，就属于非法限制，以及/或干涉隐私权则具有任意性。

24. 政府常常以国家安全为由，包括以恐怖主义造成的危险为由，作为数字通信监控方案的理由。一些答复指出，由于数字通信技术可能被并且曾经被一些个人用于犯罪目的(包括恐怖主义行为招募人员以及为这类行为筹资和实施这类行为)，所以合法和具有针对性的数字通信监控可能成为情报和/或执法实体的必要和有效措施，但前提是监控行为遵守国际和国内法。以国家安全或防止恐怖主义或其他罪行为由实施的监控可能成为从《公约》第十七条的角度出发进行评估的“合理目标”。但是，必须从实现目标的措施的必要性以及为实现这一目标可产生实际收益的角度出发，评估干涉的程度。

25. 关于评估一项措施必要性的问题，人权事务委员会在关于《公民权利和政治权利国际公约》第十二条的第 27 号一般性意见中强调，“限制不应破坏权利最根本的内容[……]；权利与限制及规范与例外之间的关系不得倒置”。[17] 委员会进一步解释指出：“限制仅仅有利于可允许的意图是不够的；它们必须是为保护这些意图而必不可少才行。”此外，这类措施必须具有相称性：“必须是可用来实现预期结果的诸种手段中侵犯性最小的一个”。[18] 在具备合理目的和适当保障措施的情况下，可允许一国采取侵入性较强的监控办法；但政府有义务证明干涉行为即是必要的，而且与所应对的具体风险相称。就此举例而言，即使大规模或“成批”监控方案拥有合理目标，并且基于适用的法律制度，这些方案仍可能被视为具有任意性。换句话说，仅仅为了在“草堆”中找到某些“针”而采取

[15] CCPR/C/21/Rev.1/Add.13, 第 6 段。

[16] CCPR/C/21/Rev.1/Add.9, 第 11-16 段。另见 A/HRC/14/46, 附件，做法 20。

[17] CCPR/C/21/Rev.1/Add.9, 第 11–16 段。另见欧洲人权法院，*Handyside* 诉联合王国，第 48 段；及 *Klass* 诉德国，第 42 段。

[18] CCPR/C/21/Rev.1/Add.9, 第 11–16 段。

措施是不够的；恰当的标准是比照可能遭受的危害判断所采取的措施对“草堆”的影响；也就是说，采取的措施是否是必要和相称的。

26. 关于获得和使用数据是否符合特定合理理由的关切还引发了另外的问题，即政府越来越依靠私营部门行为者保留数据，只是为了政府“有备无患”。强制第三方保留数据已成为许多国家监控制度的重复特征，即政府要求电话公司和互联网服务供应商储存其顾客通信的元数据及地址，以供执法和情报机构今后使用，这一做法似乎既无必要性也无相称性。[19]

27. 在确定相称性方面必须考虑的一项因素在于如何处理批量数据，以及一旦数据收集起来，哪些人可接触这些数据。许多国家框架缺乏“使用限制”，只是允许为一个合理目的收集数据，但后来将其用作其它用途。缺乏有效使用限制的现象自 2001 年 9 月 11 日以来进一步恶化，刑事司法和保护国家安全之间的界线变得极为模糊。执法机构、情报机构和其它国家部门之间共享数据很有可能违反《公约》第十七条，这是因为，监控措施可能对一项合理目标而言是必要和相称的，但对另一项目标而言则不尽然如此。对国家政府获取第三方数据做法的审查表明，“国家安全机构和执法机构可首先极为轻松地获得私营部门数据，在这一背景下，不同机构之间出于超越收集信息的目的共享和使用信息有了更大的自由度，使传统的数据保护受到严重削弱。”[20]一些国家的数据共享制度因这一理由被司法复审否决。另一些国家认为，这类使用限制是确保一国有效履行《公约》第十七条之下义务的良好做法，[21] 不遵守义务的行为应受到有效制裁。

B. 法律保护

28. 《公民权利和政治权利国际公约》第十七条第 2 款明确声明，人人有权享受法律保护，以使其隐私免受非法或任意干涉。这一点表明任何通信监控方案必须基于便于公众了解把握的法律，而这一法律反过来必须遵守国家本身的宪法制度和国际人权法。[22] “便于了解把握”要求不仅公布法律，而且法律足够确切，能够使受影响者调整自己的行为，并可事先预见某行动可能导致的后果。国家必须确保对隐私、家庭、住宅或通信权利的干涉得到法律授权，这些法律应当：(a) 便于公众了解把握；(b) 包括确保为合法目的收集、获得和使用通信数据的条文；(c) 足够准确，并详细说明允许此类干涉的确切情况、授权程序、可

[19] 见欧洲联盟法院佐审官 Cruz Villalón 关于 C-293/12 和 C-594/12 号联合案件的意见，该意见认为第 2006/24/EU 号指令(关于因提供电子通信服务产生或处理的数据的保留)“总体上”违反《欧洲联盟基本权利宪章》，因为该指令未对保留这类数据施加严格限制。另见 CCPR/C/USA/CO/4,第 22 段。

[20] Fred H. Cate、James X. Dempsey 和 Ira S. Rubinstein，“政府系统性获取私营部门数据”，《国际数据隐私法》，第二卷，第 4 号，2012 年，第 198 页。

[21] 见 A/HRC/14/46, 附件，做法 23。

[22] 见同上，附件。

监控人员的类别、监控期限、使用和储存所收集数据的程序；(d) 提供有效保障，防止权力滥用。[23]

29. 因此，法律的秘密规则和秘密解释，甚至是秘密司法解释都不具备“法律”的必要特质。[24] 法律或规则也不能给予行政当局，如安全和情报机构过分的酌处权；行使权威酌处权的范围与方式必须以合理明确的方式 (在法律本身当中或在已发布的具有约束力的准则中)予以说明。便于了解把握但没有可预见影响的法律并不适当。特定监控权力的秘密性质导致任意行使酌处权的更大风险，因此要求有关行使酌处权的规则更为精确，还需要额外的监管。一些国家还要求通过议会的基本立法辩论制定法律框架，而非简单地由行政机构颁布附属规则，这项要求有利于确保法律框架遵守《公民权利和政治权利国际公约》第二十五条，不仅在通过之后，而且在制定期间可为公众了解把握。[25]

30. 便于了解把握的要求对于评估一些国家将监控任务外包给其它国家的新出现的做法也非常重要。有可信资料表明，一些政府一贯通过对隐私的保障较为薄弱的管辖区收集路由数据并进行分析。据报告，一些政府利用一连串法律漏洞，运营一个跨国情报机构网络，其中涉及协调监控做法，以避开国内法律制度提供的保护。毫无疑问，这类做法未通过合法性测试，正如针对本报告的一些答复指出，这种做法使受其影响的人无法预见监控制度的操作。它可能破坏《公民权利和政治权利国际公约》第十七条所保护权利的实质，因此也为该《公约》第五条所禁止。国家也没有采取有效措施，保护在其管辖下的个人免受其他国家或商业实体的非法监控行为，因此违反了它们自己的人权义务。

C. 谁受到保护？在何处受到保护？

31. 收到的几份答复讨论了对域外数字监控适用《公民权利和政治权利国际公约》的问题。很明显，近来暴露的监控方案的某些方面涉及监控国的域内义务，域外监控和截获通信的行为也引发了更多关切。

32. 《公民权利和政治权利国际公约》第二条要求每一缔约国尊重和保证在其领土内和受其管辖的一切个人享有该《公约》所承认的权利，不分种族、肤色、性别、语言、宗教、政治或其他见解、国籍或社会出身、财产、出生或其他身份等任何区别。人权事务委员会在第 31 号一般性意见中强调，第二条第 1 款规定，缔约国必须尊重和保证在其领土内和受其管辖的一切个人享有《公约》所承认的权利。这就意味着缔约国必须尊重和确保在其权力范围内或者有效控制下的

[23] CCPR/C/USA/CO/4, 第 22 段。另见欧洲人权法院，Malone 诉联合王国，第 8691/79 号申诉，1984 年 8 月 2 日，第 67 和 68 段；以及 Weber 和 Saravia 诉德国，第 54934/00 号申诉，2006 年 6 月 29 日，法院在其中列举了成文法中应规定的最低保障。

[24] 见 CCPR/C/USA/CO/4,第 22 段。

[25] 另见 A/HRC/14/46。

任何人享受《公约》所规定的权利，其中甚至包括不在缔约国领土上的一些人的权利。”[26] 这一点引申至属于其“管辖权限”范围内的个人。[27]

33. 人权事务委员会受这一原则指导，曾在最早的判例中指出，一国不可通过在境外采取在“本国”受到禁止的行动而逃避其国际人权义务。[28] 这一立场与国际法院的观点一致，国际法院指出，《公民权利和政治权利国际公约》适用于一国“在其领土外行使管辖权”所实施的行为，[29] 上述立场也与《维也纳条约法公约》第三十一和三十二条相一致。“权力”和“有效控制”的概念是一国是否行使“管辖权”或政府权利的标志，对人权的保护旨在限制对这些权力的滥用。一个国家不可简单地借助于将这些权力划在法律范畴以外，以避免其人权责任。提出与此相异的结论不仅会破坏受到国际人权法保护的权利的普遍性和实质，而且为国家之间相互外包监控活动提供了结构性激励。

34. 因此，只要一个国家的监控涉及对数字通信基础设施行使权力或有效控制(例如，直接窃听或侵入基础设施)，则这类数字监控即关乎国家的人权义务。同样，如果一个国家对实际控制数据的第三方行使监督管辖权，则该国也应承担《公约》之下的义务。如果一个国家因为私人公司在该国成立公司而试图对其数据行使管辖权，则必须对隐私受到干涉的人提供人权保护，不论是在成立公司的国家还是该国之外。不论行使这类管辖权是否合法，在实际中是否违反另一国主权，这一点都是如此。

35. 鉴于目前正在讨论在国家安全监控制度中“外国人”和“公民”是否拥有平等的隐私保护的问题，所以这一结论同样重要。一些法律制度对针对国民或在一国领土内生活者及非国民和在领土外生活者承担的义务作了区分，[30] 或者为外国或外部通信提供较低程度的保护。如果不确定某些数据为外国还是国内数据，情报机构通常将其视为外国数据(因为数字通信通常从某一点 “出国转一圈”)，进而允许收集和保护这些数据。这样做导致对外国人和非公民提供的隐私保护远远低于对公民的保护，甚至根本没有保护。

---

[26] CCPR/C/21/Rev.1/Add.13, 第 10 段。

[27] 见《大会正式记录，第三十六届会议，补编第 40 号》(A/36/40)，附件十九，第 12.2 段；另见附件二十。另见 CCPR/CO/78/ISR, 第 11 段；CCPR/CO/72/NET, 第 8 页；CCPR/CO/81/BEL, 第 6 段；及美洲人权委员会，Coard 及其他人诉美国，第 10.951 号案件，第 109/99 号报告，1999 年 9 月 29 日，第 37、39、41 和 43 段。

[28] 见《大会正式记录，第三十六届会议》(见脚注 27)，附件十九，第 12.2-12.3 段，及附件二十，第 10.3 段。

[29] “国际法院对在被占领巴勒斯坦领土修建隔离墙的法律后果发表的咨询意见”，2004 年 7 月 9 日(A/ES-10/273 和 Corr.1)，第 107-111 段。另见国际法院，关于在刚果领土内的武装活动的案件(刚果民主共和国诉乌干达)，判决，2005 年，第 168 页。

[30] 例如，见美国，《外国情报监视法》，S1881(a)；联合王国，《调查权监管法案》，2000 年，s8(4)；新西兰，《国家安全局法》，2003 年，s. 15A；澳大利亚，《情报机构法》，S. 9；及加拿大，《国防法》，S. 273.64 (1)。

36. 国际人权法明确规定了不歧视原则。《公民权利和政治权利国际公约》第二十六条规定：“所有的人在法律面前平等，并有权受法律的平等保护，无所歧视”，以及“在这方面，法律应禁止任何歧视并保证所有的人得到平等的和有效的保护，以免受基于种族、肤色、性别、语言、宗教、政治或其他见解、国籍或社会出身、财产、出生或其他身份等任何理由的歧视。”这些条款应与第十七条一并解读，第十七条规定：“任何人的私生活不得加以任意干涉”，以及“人人有权享受法律保护，以免受这种干涉或攻击”，该条还应与第二条第 1 款一并解读。在这方面，人权事务委员会强调采取“措施，确保对隐私权的任何干涉符合合法性、相称性和必要性原则，与通信受直接监控者的国籍或所在地无关”的重要性。[31]

D. 程序性保障和有效监督

37. 《公民权利和政治权利国际公约》第十七条第 2 款声明，人人有权受到法律保护，免受非法或任意干涉或攻击。“法律保护”必须通过有效的程序性保障予以落实，包括有效划拨充分资源的体制安排。但是，很明显，缺乏有效的监督导致在数字环境下任意或非法侵犯隐私权的行为未被追究责任。没有独立、外部监测的内部保障措施经证明对非法或任意监控措施无效。虽然这类保障措施可采取各种形式，但政府所有分支部门参与对监控方案的监督以及设立独立的民事监督机构对于确保有效的法律保护至关重要。

38. 满足独立性、公正性和透明度等国际标准的司法参与更有可能促进总体法律制度满足国际人权法要求的最低标准。同时，不应将司法参与监督视为万灵药；在一些国家，司法批准或审查情报和/或执法机构的数字监控活动只是相当于“橡皮图章”式的走形式。因此，越来越多的注意力开始转向行政、司法和议会监督的混合模式，就本报告提交的一些答复强调了这一点。在监控授权程序内部设立“倡导公众利益”的岗位尤其吸引关注。由于互联网服务供应商等第三方的作用日益重要，所以有必要考虑允许这些方面参加影响其利益的监控措施的授权行为，或允许他们对现有措施提出质疑。一些相关判例认为，通过独立顾问、监测和/或审查，确保对在法定监控制度之下采取的措施进行严格审查是颇为积极的举措。议会委员会也可发挥重要作用，但议会委员会也可能缺乏查明侵权行为的独立性、资源或意愿，也可能受到规章约束。区域层面的判例强调，应设立一个完全独立的监督机构，专门负责对经批准的监控措施的执行情况进行监督。[32] 因此，反恐中注意增进与保护人权和基本自由问题特别报告员于 2009 年建议，“不得在独立监督机构的审查范围之外设立秘密监视系统，所有干涉措施一律由独立机构授权。”[33]

[31] CCPR /C/USA/CO/4, 第 22 段。

[32] 例如，见欧洲人权法院，Ekimdzhiev 诉保加利亚，第 62540/00 号申诉，2007 年 6 月 28 日。

[33] A/HRC/13/37, 第 62 段。

E. 获得有效补救的权利

39. 《公民权利和政治权利国际公约》要求缔约国确保为《公约》之下权利受到侵犯的受害者提供有效补救。第二条第 3 款(乙)项进一步要求《公约》缔约国承担“保证任何要求此种补救的人能由合格的司法、行政和立法当局或由国家法律制度规定的任何其他合格当局断定其在这方面的权利；并发展司法补救的可能性”。国家还必须保证相关当局在准与此等补救时确能付诸实施。正如人权事务委员会在第 31 号一般性意见中强调，如果缔约国不对侵犯权利行为的指控进行调查，可能会引起对于《公约》的再次违反。[34] 此外，制止目前还在进行的侵权行为是有效补救权利的关键内容。

40. 因此，对通过数字监控侵犯隐私行为的有效补救可采取司法、立法或行政等不同形式。有效的补救通常具有某些共同特点。首先，这类补救必须为声称其权利受到侵犯的个人所知晓，可为其提供。因此，通知(制定了一般的监控制度或具体的监控措施)和申诉权(质疑这类措施)是确定有效补救途径的重要问题。各国在通知方面采取不同方针：一些国家要求在调查结束时对监控目标进行事后通知，但许多国家不要求通知。一些国家可能正式要求在发生刑事案件的情况下进行这类通知；但在实际中，这一约束似乎常被忽视。在国家层面，有关个人质疑司法的申诉权的方针也各不相同。欧洲人权法院的裁决指出，虽然监控制度的存在可能干涉隐私，但只有在有“合理可能性”认为一个人实际受到非法监控的情况下，才可由法庭审理所称权利受到侵犯的指控。[35]

41. 第二，有效的补救涉及对所称侵权行为快速、彻底和公正的调查。这也许应由一个“在民主社会所允许的限度内接受充分的正当程序保障和司法监督的独立监督机构[……]”提供。[36] 第三，有效的补救必须能够制止正在进行的侵权行为，例如命令删除数据或提供其他赔偿。[37] 这类补救机构“可不受任何障碍地接触一切有关信息；拥有进行调查所必要的资源和专门知识；有权下达具有约束

[34] CCPR/C/21/Rev.1/Add.13, 第 15 段。

[35] 见 Esbester 诉联合王国，第 18601/91 号申诉，委员会 1993 年 4 月 2 日的裁决；Redgrave 诉联合王国，202711/92 号申诉，委员会 1993 年 9 月 1 日的裁决；以及 Matthews 诉联合王国，第 28576/95 号申诉，委员会 1996 年 10 月 16 日的裁决。

[36] “关于监控方案及其对言论自由的影响的联合声明”，由增进和保护见解和言论自由权问题特别报告员和美洲人权委员会言论自由问题特别报告员联合发布，2013 年 6 月(见 www.oas.org/en/iachr/expression/showarticle.asp？artID=927&lID=1)，第 9 段。

[37] 例如，见欧洲人权法院，Segersted-Wiber 及其他人诉瑞典，第 62332/00 号申诉，2006 年 6 月 6 日。另见 CCPR/C/21/Rev.1/Add. 13, 第 15-17 段。

力的命令”。[38] 第四，当侵犯人权行为升级至严重侵犯程度时，非司法补救将不再适当，因为需要提出刑事起诉。[39]

四. 企业发挥何种作用？

42. 强有力的证据表明，政府越来越依赖私营部门进行和加强数字监控。位于各个大洲的国家政府都同时利用正式法律机制和隐秘的方法获取通信内容及元数据，这一进程变得越来越正规化：由于电信服务从公共部门转为由私营部门提供，因此出现了“以‘自我监管’或‘合作’为幌子，向互联网中介分配执法和准司法责任的做法”。[40]法律要求企业网络“便于监听”尤为令人关切，这样做为便利大规模采取监控措施创造了环境。

43. 一个国家要求某信息和通信技术公司提供用户数据可能存在合理理由；然而，如果国家的要求违反国际法之下的隐私权，而公司应该要求提供数据或用户信息，或公司在没有适当保障的情况下向国家提供大规模监控技术或设备，或信息被用于违反人权的用途，则该公司就涉嫌合谋或参与侵犯人权。人权理事会于2011 年核可的“工商业与人权指导原则”为防止和处理与商业活动相关的负面人权影响提供了全球标准。尊重人权的责任适用于一家公司的全球业务，不论公司用户所在地在何处，也不论国家是否履行其自身人权义务。

44. 多利益攸关方已做出重要努力，澄清“指导原则”对通信和信息技术部门的适用性。例如，提供内容或互联网服务的企业或提供使数字通信成为可能的技术与设备的企业应制定明确的政策声明，表明其在公司所有活动中尊重人权的承诺。它们还应制定适当的克尽职责政策，以查明、评估、防止和减轻任何不利影响。公司应当评估其服务条款或收集及共享客户数据的政策是否可能以及如何对其用户的人权产生不利影响。

45. 当企业接到政府不符合国际人权标准的获取数据要求时，应尽最大可能遵守其人权原则，并表明在这方面持续作出努力。这可能意味着尽可能狭义地解释政府的要求，要求政府澄清其要求的范围和法律依据，在满足政府的数据要求之前请法院发布命令，并与用户明确沟通所涉风险及遵守政府要求的情况。在这方面既有单独企业、也有多利益攸关方举措的行业积极行动实例。

46. “指导原则”对克尽人权职责的界定的重点是与受影响的利益攸关方进行切实磋商。就信息和通信技术公司而言，这一职责也包括确保用户充分透明地了

[38] A/HRC/14/46。

[39] “严重违反国际人权法和严重违反国际人道主义法行为受害人获得补救和赔偿的权利基本原则和导则”(大会第 60/147 号决议，附件)。

[40] 见《欧洲数字权》“从‘自我监管’向企业审查的转变”，布鲁塞尔，2011 年 1 月，见 www.edri.org/files/EDRI_selfreg_final_20110124.pdf。

解其数据如何被收集、储存、使用和可能与他人共享，使他们能够提出关切问题，作出知情决策。“指导原则”明确指出，当企业发现其造成或推动造成负面人权影响时，有责任通过提供直接补救或与合法补救进程合作，以确保提供补救。为了尽可能较早提供补救，企业应在业务层面设立申诉机制。如果在企业开展业务的国家权利得不到适当保护，缺乏司法和非司法补救的途径，则这类机制可能尤为重要。除补偿和恢复原状等要素以外，补救措施还应包括提供相关资料，说明有哪些数据与国家当局共享及如何共享这些数据。

五. 结论和建议

47. 国际人权法为增进和保护私隐权，包括在国内和域外监控、截获电子通信及收集个人数据的情形下增进和保护隐私权提供了明确和普遍的框架。然而，许多国家的做法表明，这方面缺乏充分的国家立法及/或执法不力，程序性保障薄弱，且监管无效，所有这些因素导致任意或非法干涉隐私权的行为未被追究责任。

48. 在应对落实私隐权问题的重大空白时，提出了两项意见。第一，与国内和域外监控政策及做法相关的信息不断涌现。持续的调查旨在收集有关电子监控和收集及储存个人数据方面的信息，并评估其对人权的影响。国家和区域法院正在对电子监控政策和措施的合法性进行审查。基于国际人权法对监控政策和做法进行的任何评估必须随着该问题性质的不断变化进行调整。第二项相关意见认为，政府在监控政策、法律和做法方面缺乏透明度，该现象令人不安，阻碍了评估这些政策、法律和做法是否符合国际人权法及确保问责制的努力。

49. 有效处理与在现代通信技术背景下的隐私权相关的挑战需要多利益攸关方持续、一致的合作。该进程应该包括会员国、民间社会、科学和技术界、企业部门、学术界和人权专家等所有利益攸关方参与的对话。随着通信技术的不断发展，领导才能将变得至关重要，以确保发挥这些技术的潜力，以促进享有国际法律框架所载人权。

50. 在铭记上述意见的同时，明显迫切的需要是提高警惕，通过制定防止侵犯权利的有效保障，确保任何监控政策和做法遵守国际人权法，包括隐私权。作为应尽快采取的措施，各国应审查各自的国内法律、政策和做法，确保充分遵守国际人权法。如果存在缺陷，各国应采取步骤处理缺陷，包括制定一项清楚、确切、可了解把握、全面和不歧视的法律框架。应采取步骤，确保制定有效和独立的监管制度与做法，关注受害者获得有效补救的权利。

51. 在数字时代增进和保护隐私权存在许多实际的重大挑战。除本报告对一些问题所作初步探讨以外，还有必要进一步讨论和深入研究与有效的法律保护、程序性保障、有效监管和补救相关的问题。对这些问题的深入分析有助于基于国际人权法对以下问题提供实际指导：与监控做法相关的必要性、相称性和合法性原则；有效、独立和公平监督措施；以及补救措施。进一步分析还可帮助商业实体

履行尊重人权的责任，包括克尽职责和风险管理保障措施，以及促进这些实体在提供有效补救方面发挥作用。