联 合 国 A/HRC/29/32

大 会

Distr.: General
22 May 2015
Chinese
Original: English

人权理事会
第二十九届会议
议程项目 3
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

增进和保护见解和言论自由权问题特别报告员大卫·凯伊的报告*

内容提要

在按照人权委员会第 25/2 号决议提交的本报告中，特别报告员讨论在数字通信中使用加密和匿名的问题。借鉴关于国际和国家准则和判例的研究以及国家和民间社会的建言，本报告的结论认为，加密和匿名可使个人在数字时代行使见解和言论自由权，因此应得到有力的保护。

* 迟交。

目录

一. 导言

1. 现代数字技术为政府、公司、罪犯和恶作剧者干涉见解和言论自由权提供了前所未有的能力。在线检查、大规模和有针对性的监控和数据收集、对民间社会的数字攻击和由于在线言论产生的压制迫使世界各地的人们寻求安全，以便持有主张不受干涉和寻求、接收和传递信息和各种思想。许多人寻求通过加密、数据扰频保护其安全，以便仅指定接收人可访问数据，这种方法可适用于传输过程中的数据(例如，电子邮件、短信、互联网电话)和静态数据(例如硬盘、云服务)。其他人寻求匿名等额外保护，使用复杂技术隐匿其身份和数字足迹。加密和匿名是当今在线安全的首要途径，它向个人提供保护隐私的方法，使他们能够浏览、阅读、构思和分享意见和信息而不受干涉，使记者、民间社会组织、少数民族或宗教团体成员、因性取向或性别认同受到迫害的人士、活动家、学者、艺术家和其他人能够行使见解和言论自由权。

2. 然而，正如电话可用来向警察报告犯罪也可用来密谋犯罪那样互联网也可被滥用，干扰其他人的权利、国家安全或公共秩序。执法机构和情报部门经常宣称，由于匿名或加密通信，很难调查金融犯罪、非法毒品、儿童色情制品和恐怖主义。人们对流氓和罪犯使用新技术加强骚扰表达了合理关切。一些国家限制或禁止以这些和其他理由使用加密和匿名，其他一些国家建议或实施执法途径，以规避这些保护并访问个人通信。

3. 鉴于这些挑战，本报告研讨两个相互关联问题。首先，私隐权和见解与言论自由权是否保护安全的在线通信，具体而言，通过加密或匿名？第二，假设答案是肯定的，在何种程度上，按照人权法，政府可限制加密和匿名？本报告力图回答这些问题，审评国家实践实例并提出建议。它并不打算处理数字技术提出的每一个技术或法律问题，但它为未来报告技术确定重要的问题。

4. 在编写本报告时，特别报告员向各国分发了一份问卷，征求各国国内法、条例、政策和做法方面的相关信息。截至 2015 年 4 月 1 日，16 个国家对该请求作出了答复。[1] 特别报告员还呼吁非政府利害攸关方提交资料，并于 2015 年 3 月在日内瓦召开了一次专家会议。政府的答复以及民间社会组织和个人提交的 30 多份资料可在任务负责人的网页参阅，这些资料对编写本报告作出了重大贡献。

5. 对 2014 年 8 月特别报告员任期开始以来活动的全面回顾，可在任务负责人的网页上查阅。本报告是当前任务负责人的首份报告，旨在推进关于数字时代言论自由挑战问题的工作。

[1] 收到了下列国家的答复：奥地利、保加利亚、古巴、德国、希腊、危地马拉、爱尔兰、哈萨克斯坦、黎巴嫩、卡塔尔、摩尔多瓦共和国、挪威、斯洛伐克、瑞典、土耳其和美利坚合众国。

二. 数字时代的安全和私人通信

A. 现代加密和匿名

6. 现代私人和安全通信方法利用数千年来人类已有的观念。电子数据存储、互联网和大规模数据收集和保留，这种崛起明确表明，需采取复杂手段，以保护个人、公司和政府数据。随着电子邮件、即时消息、语音互联网协议、视频会议和社交媒体从特色服务转向占主导地位的和容易监控的通信模式，人们产生了在线安全需要，使他们能够寻求、接收和传递信息，而其见解或言论没有反弹、泄露、被监视或其他不当使用的风险。

7. ——“将讯息、信息或数据转换成除指定接收人外任何人都不能读取形式的一种数学过程”[2] ——保护内容机密性和完整性不让第三方访问或操纵。强度加密，曾经是军队和情报部门的专有领域，现在已向公共开放而且经常是免费提供，以保障电子邮件、语音通信、图像、硬盘和网站浏览器的安全。“公钥加密”是保障传输中数据端到端安全性的主要形式，发件人使用接收人的公钥来加密消息及其附件，收件人使用他(或她)自己的私钥进行解密。加密也可用于创建数字签名，以确保一份文件及其发件人是真实的，以证实和验证服务器的身份，保护客户端通信的完整性不被第三方篡改或操控传输(例如，“中间人”攻击)。既然传输中的数据加密并不能确保这些数据在任何一个端点处于静态时不遭攻击(也不能保护个人私钥的安全)，我们也可加密存储在便携式计算机、硬盘、服务器、平板电脑、手机和其他设备上的静态数据。在线做法也可离开本文所述系统并转向“前向保密”或“查无记录”技术，在这种技术下，密钥是临时保有的，尤其是用于即时通信等用途。

8. 有些人呼吁作出努力，削弱或减损加密标准以便只有政府才能享有加密通信使用权。然而，对于有技能发现和利用弱点的人而言，无论是国家或非国家，合法的或犯法的，减损的加密不能对其保密。技术人员似乎普遍持有以下立场：没有一种特别访问权可以仅向政府当局提供，即使原则上以公众利益为考量的特别访问权。在当代技术环境中，蓄意破坏加密，即使是为可以说是合法的目的，也会削弱每个人的在线安全性。

9. 值得注意的是，加密保护通信内容，但不保护识别因素，例如称为元数据的互联网协议(IP)地址。如果用户不使用匿名工具，第三方可通过元数据分析收集关于个人身份的重要信息。匿名是避免被识别的条件。人类的一个共同愿望是，保护个人身份不被人群识别。与使用真实身份相比，匿名可使用户更加自由地探索和传播思想和意见。个人在线时可使用假名(或者，例如，虚假的电子邮件或社交媒体账号)隐藏其身份、形象、声音、位置等，但通过这种假名提供的隐私

[2] 见系统网路安全协会，“加密历史” (2001 年)。

是表面的，很容易被政府或拥有必要技术的其他人所干扰；如果不组合使用加密和匿名工具，用户留下的数字痕迹可使其身份很容易被发现。用户为确保充分匿名或掩盖其身份(例如隐藏原始 IP 地址)不遭政府或罪犯侵入，可使用虚拟专用网络、代理服务、匿名化网络和软件以及对等网络等工具。[3] Tor 网络是一个为人熟知的匿名工具，在全世界部署了 6000 多台分散式计算机服务器多次接收和接转数据，以隐藏端点的识别信息，为其用户建立强度匿名性。

10. 数字时代的一个主要特点是，技术不断变化以满足用户需要。虽然本报告论述有助于加密和匿名的当代技术，但它的分析和结论普遍适用于当前技术背后的理念，随着新技术取代旧技术，也应能够适用。

B. 技术的使用

11. 互联网对见解和言论自由有着深远价值，因为它放大了声音，将信息多重复制，送到可上网的每个人面前。在很短的时间内，它已成为具有核心地位的全球公共论坛。因此，在享受当今的言论自由方面，应将开放和安全的互联网列为主要的前提条件之一。但这种安全不断受到威胁，也存在这样一个空间——并非与物质世界不同——在其中，发生犯罪活动、有针对性的压制和大规模的数据收集。因此，十分关键的是，个人应找到方法，确保自己的上网安全；政府应在法律和政策中提供这种安全；公司行为方应设计、开发和营销缺省安全产品和服务。在这些要务中，没有一项是新的。在数字时代之初，各国政府认识到加密在全球经济安全方面发挥的重要作用，使用或鼓励使用加密以保障政府发放的身份号码、信用卡和银行信息、企业所有权文件和对网上犯罪本身进行调查。[4]

12. 加密和匿名，可单独或共同创建保护见解和信仰的隐私区域。例如，它们可促成隐私通信，保护见解不受外部审查，这在敌对的政治、社会、宗教和法律环境中特别重要。在国家通过过滤和其他技术进行非法审查的情况下，使用加密和匿名可使个人绕过障碍，在没有当局侵扰的情况下获取信息，接触见解。记者、研究人员、律师和民间社会依赖加密和匿名以保护自己(及其资料来源、客户和合作伙伴)不受监控和骚扰。搜索网络、构思观念和安全通信的能力可能是许多人可藉以探索其身份基本层面(例如性别、宗教、种族、民族或性)的唯一途径。艺术家依靠加密和匿名保障和保护其言论权，特别是在以下情况下：不仅国家设置限制，而且社会也不容忍非传统见解或言论。

[3] 代理服务通过一个中介或“代理服务器”发送数据，它以用户的名义发送数据，用自己的 IP 地址有效地向终端接收人隐蔽用户的 IP 地址。对等网络在相互连接的服务器中分割和存储数据，然后加密这些存储的数据，使集中式服务器无权访问识别信息。例见 Freenet。

[4] 见经合组织，密码政策指南(1997)。

13. 加密和匿名的“黑暗”面所反映的是，离线不法行为也在网上发生。执法和反恐官员表示关切的是，恐怖分子和普通罪犯使用加密和匿名隐藏他们的活动，使政府难以防止和调查恐怖主义、非法贩毒、有组织犯罪和儿童色情制品，以及实现其他政府目标。骚扰和网络欺凌可依赖匿名作为歧视行为(特别是针对弱势群体成员)的一种懦弱面具。然而，同时，执法部门经常使用同样工具以确保开展秘密行动时的安全，弱势群体成员可使用这些工具确保他们在面临骚扰时的隐私。此外，政府拥有广泛的备选工具，例如搭线窃听、定位和跟踪、数据挖掘、传统的实体监控和许多其他工具，这些工具加强了现代执法和反恐。[5]

三. 加密、匿名、见解与言论自由权和隐私权

14. 加密和匿名人权法律框架要求，首先，评估有关权利的范围并将其适用于加密和匿名；第二，评估是否可以对增进和保护隐私权和见解与言论自由权的技术使用施加合法限制，如何可以，在何种程度上可施加这种限制。

15. 隐私权[6] 和见解与言论自由[7] 已明确列入国际和区域人权文书，条约机构和区域法院对其进行解释，人权理事会特别程序对其进行评估而且在普遍定期审查期间也进行评估。《公民权利和政治权利国际公约》为隐私、见解和言论规定了普遍标准，168 个国家是该公约的缔约国。即使对于不受约束的其他国家而言，《公约》至少提供了一个成就标准而且经常反映了习惯法律规范；根据《维也纳条约法公约》第 18 条，已签署但尚未批准《公约》的国家有义务尊重其目标和宗旨。国家法律制度也保护隐私、见解和言论，有时有相关的宪法条款或基本法或解释。一些全球民间社会项目也令人信服地展示了在数字时代应适用的法律，例如“在通信监控中适用人权的国际原则”和“关于国家安全和获得信息权的全球原则”。尽管具体标准可能会因权利不同而不同，或因文书不同而有异，但法律的一个共同思路是，因为隐私权和言论自由权对于人的尊严和民主治理而言具有根本意义，限制必须严格界定，依法设立并严格执行，而且仅在特殊情况下。在数字时代，保护这种权利需要特别警觉。

[5] 见民主和技术中心，“‘走向黑暗’与‘监控的 黄金时代’”(2011 年)。

[6] 《世界人权宣言》第 12 条、《公民权利和政治权利国际公约》第 17 条和《儿童权利公约》第 16 条、《残疾人权利公约》第 22 条、《保护所有移徙工人及其家庭成员权利国际公约》第 14 条、《欧洲人权公约》第 8 条和《美洲人权公约》第 11 条保护隐私权。

[7] 《世界人权宣言》和《公民权利和政治权利国际公约》第十九条、《非洲人权和人民权利宪章》第 9 条、《美洲人权公约》第 13 条和《欧洲人权公约》第 10 条保护言论自由。

A. 隐私作为见解和言论自由的途径

16. 加密和匿名向个人和团体提供一个在线隐私区域，以保持意见和行使言论自由不受任意和非法干涉或攻击。前任任务负责人指出，“隐私权和言论自由权相互关联”，并认为，加密和匿名由于在确保这些权利方面可发挥的关键作用而得到保护(A/HRC/23/40 和 Corr.1)。《公民权利和政治权利公约》第十七条对《世界人权宣言》第 12 条作出了响应，它具体保护个人的“私生活、家庭、住宅或通信不得加以任意或非法干涉”，其“荣誉和名誉不得加以非法攻击”，并且规定，“人人有权享受法律保护，以免受这种干涉或攻击”。大会、联合国人权事务高级专员和特别程序任务负责人认识到，隐私是享受其他权利特别是见解和言论自由的一个途径(见大会第 68/167 号决议，A/HRC/13/37 和人权理事会第 20/8 号决议)。

17. 加密和匿名对于构思和分享意见特别有用，这种共享经常通过在线通信(例如电子邮件和短信)和其他在线互动进行。加密提供安全性，使个人能够“核实他们的通信仅送达其指定的收件人，不受干涉和改动，并且他们收到的通信也同样不受侵扰”(见 A/HRC/23/40 和 Corr.1, 第 23 段)。鉴于元数据分析在明示“个人行为、社会关系、私人偏好和身份”方面的能力(见 A/HRC/27/37, 第 19 段)，匿名在确保通信安全方面可发挥关键作用。除通信外，国际和区域机制将隐私解释为也包括一系列其他情形。[8]

18. 个人和民间社会可能会受到国家和非国家行为方的干扰和攻击，加密和匿名可提供保护免遭这种干扰和攻击。《公民权利和政治权利国际公约》第十七条第 2 款规定，国家有义务保护隐私免受非法和任意干涉和攻击。在这种积极义务下，国家应确保制定国内法律，禁止对隐私的非法和任意干涉和攻击，不论肇事人是政府或非政府组织行为方。这种保护必须包括侵权行为补救权。[9] 为使获得补救权具有实际意义，在出现对其隐私的任何损害情况时(例如通过削弱加密或强制披露用户数据)，个人应得到通知。

B. 持有主张不受干涉的权利

19. 《世界人权宣言》第一条承认，人人都“赋有理性和良心”，人权法进一步发展了这一原则，使其包括，除其他外，保护见解、言论、信仰和思想。《公民权利和政治权利国际公约》第十九条第 1 款也反映了《世界人权宣言》，它规

[8] 人权事务委员会关于尊重隐私、家庭、住宅和通信权以及保护荣誉和声誉问题的第 16(1988)号一般性意见。亦见欧洲人权法院，关于保护数据问题的概况(www.echr.coe.int/Documents/FS_Data_ENG.pdf) and right to protection of one’s image (www.echr.coe.int/Documents/FS_Own_image_ENG.pdf)。

[9] 见人权事务委员会第 16 号一般性意见和关于《公约》缔约国一般法律义务性质的第 31 号一般性意见；以及 CCPR/C/106/D/1803/2008。

定，“人人有权持有主张，不受干涉”。见解和言论紧密相关，因为对接收信息和思想权利的限制可能会干扰持有主张的能力，干扰持有主张必然会限制这些主张的表达。然而，人权法在两者之间作了概念区分。在关于《公约》起草问题的谈判期间，“形成主张并通过推理发展这种主张的自由被视为是绝对的，与言论自由不同的是，不允许通过法律或其他权力加以限制”。[10] 自由持有主张的能力被视为人的尊严和民主自治的一项基本要素，这一保障如此重要，《公约》不允许任何干扰、限制或约束。因此，第十九条第 3 款中允许的限制明确仅适用于第十九条第 2 款中的言论自由权。形成对照的是，干扰持有主张的权利本身 违反了第十九条第 1 款。

20. 与言论自由权相比，评论家和法院对持有主张的权利给予的关注少得多。然而，更多的关注是必要的，因为在数字时代，持有主张的机制演变了，使个人面临重大的脆弱性。个人经常以数字形式持有主张，例如，在硬盘、云端和在电子邮件存档中保存他们的意见和搜索与浏览历史，私人和公共当局通常会长时间或无限期保留这些资料。同样，民间社会组织也以数字形式准备和存储备忘录、论文和出版物，这些都涉及形成和持有主张。换言之，在数字时代，持有主张并非局限于心中可能存有的一个抽象概念。然而，今天，在数字空间中持有主张会遭受攻击。在离线状态下，对持有主张权利的干扰可能涉及身体骚扰、拘留或因其主张对个人进行惩罚的微妙努力(见 CCPR/C/78/D/878/1999, 附件，第 2.5、7.2 和 7.3 段)。干扰也可包括以下行为：有针对性的监控、分布式拒绝服务攻击、以及在线和离线恐吓、入罪和骚扰。有针对性的数字干扰个人和民间社会组织以多种形式持有的主张。加密和匿名使个人能够避免或减轻这种骚扰。

21. 持有主张不受干涉的权利也包括形成主张的权利。监控系统(有针对性的和群体性的)可破坏形成主张的权利，因为担心在线活动的非情愿披露，例如搜索和浏览，可能会妨碍个人访问信息，特别是如果这种监控导致压制后果。由于所有这些原因，必须评估对加密和匿名的限制，以确定这些限制是否等同对持有主张权的不可允许的干涉。

C. 言论自由权

22. 《公民权利和政治权利国际公约》第十九条第 2 款下的言论自由权扩大了《世界人权宣言》已经十分广泛的保障，保护“寻求、接受和传递各种消息和思想的自由，而不论国界，也不论口头的、书写的、印刷的、采取艺术形式的、或通过他所选择的任何其他媒介”。联合国和区域人权系统内的判例、特别程序报告和决议的大量积累强调，言论自由“是享有其他人权和自由的根本条件，是建立民主社会和增强民主的根本支柱”(人权理事会第 25/2 号决议)。人权理事会、

[10] Manfred Nowak, *UN Covenant on Civil and Political Rights：CCPR Commentary*(1993)，p.441.

大会和各国宣称，个人在线享有他们离线享有的相同权利。[11] 本报告不再重复这一共识的所有内容。在加密和匿名方面，案文的三个方面值得特别强调(见下文第 23-26 段)。

23. **寻求、接收和传递信息和思想的自由：**在审查做法盛行的环境中，个人可能被迫依赖于加密和匿名，以绕过限制和行使寻求、接收和传递信息的权利。一些国家用多种工具限制了访问。例如，国家审查有时对获得信息权构成不可逾越的障碍。一些国家实行基于内容的、往往是歧视性的限制或将在线言论入罪，恐吓政治反对派和持不同政见者并适用诽谤和冒犯皇权法使记者、维权人士和活动家沉默。虚拟专用网络连接，或使用 Tor 或代理服务器，同时使用加密，可能是个人可在这种环境中获得或共享信息的唯一途径。

24. 值得强调的是，人权法也保护寻求、接收和传播科学信息和思想的权利。《世界人权宣言》和《经济、社会和文化权利国际公约》保护受教育权和“享受科学进步及其应用利益”的权利。加密和保密技术使个人能够在以下情况下享有这种信息：如不使用这种技术他们会被拒绝访问；他们本身是科学进步的实例。这些技术的使用可使个人能够获得可能会被政府削弱的科学进步利益。文化权利领域特别报告员指出，“科学权和文化权均应理解为包括以自我决定的和自我扶持方式接触和利用信息和通信及其他技术的权利”(见 A/HRC/20/26, 第 19 段)。

25. **不论国界：**保障言论自由的主要文书明确承认该项权利的跨国界范围。个人享有从境外地点获得信息并向境外地点传输信息和各种思想的权利。[12] 然而，一些国家在关键字基础上过滤或阻碍数据，通过部署依赖于文本访问的技术拒绝访问。加密使个人能够避免这种过滤，允许信息跨国界流动。此外，个人并不控制──通常他们也不知道──他们的通信如何或是否跨越国界。在信息通过位于第三国的过滤内容服务器传输时，加密和匿名可保护所有个人的信息。

26. **通过任何媒体：**在《世界人权宣言》和《公民权利和政治权利国际公约》第十九条起草时，远见卓识地将未来技术进步纳入考量(A/HRC/17)。《公约》缔约国选择使用“通过任何其他媒体”这种宽泛的措词而不是列举当时存在的媒体。部分地在此基础上，国际机制多次承认，保护言论自由适用于互联网活动。区域法院也同样承认，保护适用于在线活动。[13] 欧洲人权法院，在讨论《欧洲保护人权及基本自由公约》对言论的类似保护时指出，藉以传输和接收信息的形

[11] 例见大会第 68/167 号决议，人权理事会第 26/13 号决议和欧洲委员会向成员国提出的关于互联网用户人权指南的 CM/Rec(2014)6 号部长委员会建议。

[12] 欧洲人权法院已承认这一点。见 Ahmet Yildirim 诉土耳其，(2012)；Cox 诉土耳其，(2010)；格罗佩拉广播公司等诉瑞士(1990)。

[13] 欧洲人权委员会，Neij and Sunde Kolmisoppi 诉瑞典，(2013)；欧洲人权法院，Perrin 诉联合王国，(2005)；非洲人权和人民权利法院，津巴布韦人权律师和人权与发展研究所(代表 Meldrum) 诉津巴布韦(2009)；Herrera Ulloa 诉哥斯达黎加一案，Herrera Ulloa 诉哥斯达黎加，初步反对意见、法律依据、赔偿和费用，C 系列第 107 号，IHRL1490(美洲人权法院 2004)。

式和途径本身受保护，因为对途经施加的任何限制必然会干扰接收和传播信息权。[14] 在这种意义上而言，加密和匿名技术是个人行使言论自由的专门媒介。

D. 公司的角色

27. 不同部门公司的在推进或干扰隐私、见解和言论(包括加密和匿名)方面可发挥作用。很多在线通信(在一些国家几乎所有在线通信)是在私人公司拥有和经营的网络上进行的，其他公司拥有和管理其内容大量由用户生成的网站。另一些公司是监控和间谍软件市场的积极参与者，向政府提供硬件和软件，损害个人的上网安全。还有一些公司为安全和私人在线存储提供服务。电信实体、互联网服务提供商、搜索引擎、云服务和许多其他公司行为方——它们经常被称为中介机构——促进、规范或损害在线隐私和言论。中介机构可存储大量用户数据，政府经常要求访问这些数据。这些公司行为方都可能促进或损害加密和匿名。

28. 全面探讨公司在保护用户在线安全方面的作用超出了本报告的范围，本报告侧重于国家义务。然而，仍很重要的是，应强调，“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。”(见 A/HRC/27/37, 第 43 段)。在最低限度，公司应适用例如《工商企业和人权问题指导原则》、《全球网络倡议的言论自由和隐私问题原则》、《欧盟委员会的信通技术部门执行联合国工商企业和人权问题指导原则的指南》和《电信行业对话指导原则》中规定的原则，这些原则鼓励公司承诺保护人权，恪尽职守，以确保其工作产生积极的人权影响并矫正其工作对人权的不利影响。在未来，特别报告员将侧重于公司在维护个人安全行使见解和言论自由方面应发挥的作用。

四. 评估对加密和匿名的限制

A. 法律框架

29. 对隐私权的可被允许的限制应严谨地理解，特别是在普遍存在在线监控(消极的或积极的，群体性的或有针对性的)的时代，不论可适用的标准是《公民权利和政治权利国际公约》第十七条下的“非法和任意的”、《世界人权宣言》第 12 条下的“任意的”、《美洲人权公约》第 11 条下的“任意或滥权的”、或《欧洲保护人权与基本自由公约》第 8 条下的“一个民主社会所必要的”(见 A/HRC/13/37, 第 14-19 段)。限制行使见解和言论自由的隐私干涉，例如本报告

[14] 见奥特罗尼克公司诉瑞士 (1990)；De Haes and Gijsels 诉比利时 (1997)，第 48 段；News Verlags GmbH and Co.KG 诉奥地利(2000)。

所描述的干涉，不得在任何情况下干扰持有主张的权利，限制言论自由的隐私干扰必须由法律规定，而且对于实现若干合理目标而言是必要的和相称的。

30. 对持有主张权的任何限制都不可能不产生干扰；《公约》第十九条第 3 款下的限制仅适用于第十九条第 2 款下的言论。在个人主张，即便是在线持有的主张，可导致监控或骚扰的环境中，加密和匿名可提供必要的隐私。对这种安全工具的限制可能会干扰个人持有主张的能力。

31. 对作为言论自由权促成工具的加密和匿名的限制，必须满足为人熟知的三部分测试：对言论的任何限制都必须由法律规定；仅可为(《公约》第十九条第 3 款规定的)合法理由施加限制；必须符合必要性和相称性的严格测试。

32. 首先，欲使加密或匿名受到“法律规定的”限制，这种限制必须准确、公开和透明，并避免向国家当局提供适用限制的无限自由裁量权(见人权事务委员会第 34 号一般性意见(2011 年))。对加密或匿名施加限制的建议应征求公众意见，仅可按照常规立法程序通过。也应使用有力的程序性和司法保障，以保障在使用加密或匿名时受到限制的任何个人的正当程序权。特别是，法院、法庭或其他独立裁决机构必须监督限制的适用情况。[15]

33. 第二，限制的正当理由只能是保护明确规定的利益：他人的权利或名誉；国家安全；公共秩序；公共卫生或道德。即使国家“按照《公约》第二十条的规定，”通过法律禁止“构成煽动歧视、敌意或暴力的鼓吹民族、种族或宗教仇恨的主张，但对言论的任何限制必须符合第十九条第 3 款(A/67/357)。任何其他理由都不能成为限制言论自由的合理理由。此外，由于合理目标经常被用作非法目的的借口，限制本身的适用必须十分严格。[16]

34. 第三，国家必须证明，对加密或匿名的任何限制对于实现合理目标而言是“必要的”。[17] 欧洲人权法院的适当结论是，“《欧洲保护人权及基本自由公约》第 10 条中的“必要的”一词意味着，这种限制必须是超越“有用的”、“合理的”或“可取的”。[18] 一旦实现了合理目标，限制就不得再适用。鉴于涉及基本权利，限制应受独立和公正司法机构的监督，特别是为了维护个人的正当程序权利。

[15] 见《公民权利和政治权利公约》，第二条第 3 款(乙)项；CCPR/C/79/Add.110，第 22 段；《关于国家安全、言论自由和获得信息权利问题的约翰内斯堡原则》。

[16] 见人权事务委员会关于见解和言论自由问题的第 34 号一般性意见，第 30 段，和第 31 号一般性意见。

[17] 见人权事务委员会第 34 号一般性意见，第 2 段；第 2156/2012 号来文、2014 年 10 月 10 日通过的意见。

[18] 见“《星期日泰晤士报》诉联合王国一案”，1979 年 4 月 26 日的判决，第 59 段。

35. 必要性也意味着评估限制使用和获得在线安全的措施的相称性。[19] 相称性评估应确保，这种限制“在可实现预期结果的各种手段中，侵扰性最小”。[20] 限制必须有具体目标，而非不当地侵犯目标人士的其他权利，对第三方权利的干扰必须受到限制，必须有侵扰所支持的利益作为正当理由。这种限制也必须“与欲保护的利益相称”。[21] 一个重要的合法国家利益面临损害，这种高风险可为对言论自由的有限侵扰提供正当理由。相反，如果限制措施对于对政府合法利益不构成威胁的个人产生了很大影响，国家为这种限制措施提供正当理由的负担就会很高。[22] 此外，相称性分析必须考虑到对加密和匿名的侵扰可能会被限制措施本欲阻遏的罪犯和恐怖分子网络所利用。无论如何，“详细和基于证据的公开理由”是促成开展关于涉及并可能损害言论自由的限制措施的透明的公开辩论之关键(见 A/69/397, 第 12 段)。

B. 国家实践：实例与关切

36. 关于在线安全和隐私问题的趋势令人忧虑。国家经常不提供公共理由以支持限制。加密和匿名通信可困扰执法和反恐官员，而且使监控复杂化，但国家当局通常未确定限制措施对于实现合法目标是必要的情况──即使考虑到可能需要保密，也未作出大体上的说明。国家低估传统非数字化工具在执法和反恐努力包括跨国合作中的价值。[23] 因此，公众缺乏机会，藉以衡量对其在线安全的限制是否会由于国家安全和预防犯罪方面的任何实际利益而获得正当性。限制加密和匿名的努力也常常是针对恐怖主义采取的快速反应措施，即使攻击者本人并未被指称利用了加密或匿名以策划或实施攻击。此外，即便限制措施可以说是为了寻求合法利益，许多法律和政策经常不符合必要性和相称性标准，而且，对所有个人自由行使隐私权和见解与言论自由权的能力产生广泛的有害影响。

37. 也值得注意的是，联合国本身并未向其工作人员或向希望访问联合国网站的人提供有力的通信安全工具，这就使面临威胁的人难以安全地在网上访问联合国的人权机制。[24]

---

[19] 见非洲人权和人民权利法院，Lohe Issa Konate 诉布基纳法索，第 004/2013 号申请，第 148 和 149 段(2014)；欧洲人权法院，“星期日泰晤士报案件”，第 62 段。

[20] 见人权事务委员会、关于行动自由问题的第 27 号一般性意见(1999)，第 14 段。

[21] 见同上，第 14 段。

[22] 见美洲人权委员会，OEA/Serv.L/V/II.149, 第 134 段。

[23] 但请参阅：Centre for International Governance Innovation and Chatham House, *Toward a Social Compact for Digital Privacy and Security：Statement by the Global Commission on Internet Governance* (2015)。

[24] 例如，人权事务高级专员办事处(人权高专办)在日内瓦的工作人员没有使用端对端电子邮件加密，人权高专办网站也未加密。

1. 加密

38. 一些政府力图保护或促进加密，以确保通信隐私。例如，[25] 2014 年通过的巴西《互联网民事框架法》保障用户在线通信的不可侵犯性和保密性，仅允许法院命令作出的例外。奥地利《电子商务法》和《电信法》并不限制加密，政府开展了公共宣传活动，向公众宣传数字安全。希腊法律和条例促进有效使用加密和匿名工具。德国、爱尔兰和挪威允许和促进使用加密技术，反对削弱加密协议的任何努力。同样，瑞典和斯洛伐克法律不限制使用在线加密。美利坚合众国鼓励使用加密，美国国会应进一步考虑在国会提出的一部安全数据法，该法将禁止政府要求公司削弱产品安全性或插入后门进入措施。若干国家政府，包括加拿大、荷兰、瑞典、大不列颠及北爱尔兰联合王国和美国，提供资金，资助为共享或培训使用加密和匿名技术，以帮助个人逃避审查和保护其在线安全所作的努力。此外，凡可能，出口条例应便利转让加密技术。尽管本报告并不对各国的加密方法进行全面法律评估，但这些要素——不限制或全面保护、对任何具体限制要求作出法庭命令、公众教育——值得更广泛的应用，作为保护和促进见解和言论自由权的方法。

39. 然而，对加密的管理在两个主要方面往往无法达到言论自由标准。首先，通常无法表明，某些限制措施是为了维护某项正当利益而有必要采取的措施。鉴于其他工具(例如传统意义上的维持治安和情报和跨国合作)的广度和深度——这些工具也许已经可以为具体的执法或其他正当目的提供大量信息——这一点就更加突出了。第二，限制措施会严重影响目标人士或公众享有的见解和言论自由权。

禁止个人用途加密

40. 直接禁止个人使用加密技术会过度限制言论自由，因为在未具体指称使用加密进行非法目的的情况下，这种禁令剥夺了某个管辖区的所有在线用户开辟私人空间以发表见解和言论的权利。

41. 国家加密条例可能等同于禁令，例如如下规则：(a) 使用加密要求有许可证；(b) 对加密设置较弱的技术标准；(c) 控制加密工具的输入和输出。通过将加密工具限制在政府批准的标准范围内和控制加密技术的进口或出口，政府确保了加密软件保持弱点，使政府能够获得通信内容。例如，尽管法律可能处于变动之中，印度规定，服务提供商不可在网络上部署“批量加密”，法律还限制个人在未事先批准的情况下使用大于便于破解的 40 位密钥长度，并要求使用更强加密的任何人向政府提供加密密钥副本。[26] 报告指出，中国加密产品可能被要求

[25] 本段中的很多实例节录自政府提交有关的资料。

[26] 印度政府，通讯和信息技术部，提供互联网服务许可协议，(2007)。可在以下网址参阅：http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf。尤请参见第 2.2(七)条。

遵守政府批准的其安全性未经同行评议的加密算法。[27] 巴基斯坦电信管理局要求，使用虚拟专用网络和加密须事先获得批准。[28] 古巴要求对使用加密的人进行监管授权。[29] 在埃塞俄比亚，政府有权设定加密技术标准，它最近颁布了条例，将未经许可制造、装配或输入任何通讯设备定为犯罪。[30] 这种条例践权地干扰了个人在通信中对加密的使用。

蓄意削弱加密

42. 一些国家已实施或提议实施商业产品的所谓后门进入，迫使开发商设置弱点使政府当局能够访问加密通信。一些政府开发或购买了工具，以允许为国内监督目的进行这种数据访问。[31] 联合王国和美国的高级官员似乎在倡导要求后门进入。[32] 支持这种措施的国家经常声称，后门进入法律框架对于截取加密通信内容而言是必要的。然而，提议后门进入的政府未证明，罪犯或恐怖分子对加密的使用是执法目标的不可逾越障碍。此外，基于现有技术，蓄意缺陷无例外地损害所有在线用户的安全，因为一个后门程序，即使仅供政府使用，可被未经授权的实体(包括其他国家或非国家行为方)使用。鉴于其广泛和恣意影响，后门进入程序可不相称地对所有在线用户产生影响。

43. 关于这一问题的辩论强调了一个关键点，要求加密后门进入，即使是为合法目的，也是对不受妨碍地行使言论自由权所必需的隐私权的威胁。后门进入有实际限制；利用有意的弱点可使加密内容容易受到攻击，即使提供这种进入的唯一意图是允许政府或司法控制。在保护言论自由的义务与防止侵犯生命权或身体完整性(恐怖主义和其他犯罪行为使其受到威胁)的义务相冲突时，政府当然面临一个困境。但国家可采用其他手段要求披露加密信息，例如通过司法保证。在这种情况下，国家必须表明，对加密提供的安全所作的一般限制是必要的和相称的。国家必须公开和透明地表明，其他侵扰性较低的手段不可用或已经失败，只有强侵入性措施，例如后门程序，可实现合法目的。无论如何，对大批人员施加普遍适用的限制措施，而不是经过逐案评估，几乎肯定无法满足相称性。

---

[27] 例见，《反恐怖主义法》，第 15 条(2014 年 11 月 8 日初稿)。可在以下网址参阅：http://chinalawtranslate.com/en/ctldraft/.

[28] 见 www.ispak.pk/Downloads/PTA_VPN_Policy.pdf。

[29] 古巴提交的资料。

[30] 见埃塞俄比亚电信诈骗罪公告 761/2012 号，第 3-10 条。

[31] 见 Morgan Maquis-Boire and others, *For Your Eyes Only* (2013, Citizen Lab).

[32] 见首相戴维·卡梅伦 2015 年 1 月 12 日在保守党 2015 年大选承诺会议上的讲话；James Comey, 联邦调查局局长，2014 年 10 月 16 日的讲话，题为“走向黑暗：技术、隐私和公共安全相互抵触吗？”，布鲁金斯学会，华盛顿特区。

密钥托管

44. 密钥托管系统允许个人使用加密，但要求用户将其私用密钥交给政府或一个“可信任的第三方”保存。然而，密钥托管有很大脆弱性。例如，密钥托管系统取决于负责保护私人密钥安全的人员、部门或系统的诚信，密钥数据库本身可能容易受到攻击，使任何用户的通信安全和隐私受到损害。在美国 1990 年代所谓的加密之战中，经过重大辩论，密钥托管系统(以及后门程序)被拒绝；这种系统目前已在几个国家使用，在其他一些国家也已提议使用。2011 年，土耳其通过条例，要求加密供应商在将其加密工具提供给用户前向政府监管机构提供加密密钥副本。[33] 密钥托管固有的脆弱性使它们成为行使言论自由安全的严重威胁。

强制性密钥披露与有针对性的解密命令

45. 在执法或国家安全可为监控通信请求提供正当理由的情况下，当局可能有两个选择：命令解密某些通信，或者，由于不信任目标当事方会遵守解密命令，可命令披露解密所必需的密钥。与密钥披露相比，有针对性的解密命令可被视为局限性更大，而且，较不可能产生相称性关切，因为它侧重于具体的通信而不是某个密钥加密的个人全部通信。相比之下，密钥披露暴露私人数据的程度远远超出某种情况所必需的内容。[34] 此外，密钥泄露或解密命令经常迫使公司与政府合作，对在线个人用户构成严重挑战。在许多欧洲国家，存在法律要求密钥披露的情况。[35] 然而，在这两种情况下，这种命令应基于向公众公开的法律，明显限制范围，侧重于一个具体目标，由独立和公正司法机构负责实施，尤其是为了保持目标人士的正当程序权，而且仅在必要时和在侵扰性较低的调查手段不可用的情况下作出这种命令。这类措施仅可在针对特定用户(一人或多人)使用时才有正当理由，而且受司法监督。

法律推定

46. 一些国家可能将使用加密技术本身视为非法行为。例如，对埃塞俄比亚 9 区博客集体的控罪包括这种罪名：通信安全培训 本身是犯罪行为证据。[36] 这种推定未能满足可被允许的限制的标准。同样地，国家如果惩罚制作和流通工具以便利活跃分子上网，就损害了隐私和言论自由权。

---

[33] 关于规范互联网广播和打击通过互联网广播犯罪的第 5651 号法。

[34] 欧洲委员会反恐怖主义协调员已促请对强制性密钥披露进行审议。见欧洲联盟理事会，总秘书处、会议文件 D1035/15 (2015)。

[35] 例见，联合王国，调查权力法条例(强制性密钥披露)；法国，第 2001-1062 号法(法官授权披露加密密钥)；西班牙《电信法》25/2007(密钥披露)。

[36] See http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/.

2. 匿名

47. 人们认识到，匿名在保障和推进隐私、言论自由、政治问责、公众参与和辩论方面发挥重要作用。[37]《世界人权宣言》和《公民权利和政治权利国际公约》未涉及匿名问题。在谈判《公约》期间，有人提议，在第十九条第 1 款中列入“匿名不被允许”等字句。然而，这一提议被拒绝了，“理由是，除其他外，有时可能需要匿名以保护作者”，而且，“这种条款可能防止使用笔名”。[38] 美洲人权委员会言论自由问题特别报告员认为，“思想和言论自由权和私生活权保护匿名言论不受政府限制”。[39] 有几个国家在政治文化中享有悠久的称赞匿名的传统，但很少有国家在法律中为匿名表达提供一般保护。一些国家对离线和在线匿名施加很大压力。然而，由于匿名极其有助于在线见解和言论，国家应保护匿名，一般不应限制提供匿名的技术。若干国家的司法机关对匿名作出过保护，至少在有限的案例中。例如，加拿大最高法院最近判决，未经授权的收集在线匿名用户身份无效。[40] 大韩民国宪法法院以违宪为由判决反匿名法律无效。[41] 美国最高法院一贯保护匿名言论权。[42] 欧洲人权法院承认匿名对于言论自由的重要性，但允许在为实现合法目标所必需的情况下加以限制。

48. 许多国家承认保持记者来源匿名的合法性。墨西哥最高法院和墨西哥《刑事诉讼法》承认记者有权维护消息来源的匿名性；然而对记者的压力实际上很严重。[43] 阿根廷、巴西、厄瓜多尔和巴拉圭的《宪法》明确保护消息来源；智利、萨尔瓦多、巴拿马、秘鲁、乌拉圭和委内瑞拉(玻利瓦尔共和国)以法律保护消息来源。[44] 莫桑比克《宪法》保护消息来源；安哥拉打算以成文法加以保护。[45] 澳大利亚、加拿大、日本和新西兰建立了逐案司法平衡测试，以分析消

[37] 例见：美洲人权委员会，OEA /Serv.L/V/II.149,第 134 段；美国，McIntyre 诉俄亥俄选举委员会(1995)；Lord Neuberger, speech to RB Conference on the Internet, entitled, “What’s a name? Privacy and Anonymous Speech on the Internet”(2014)。

[38] Marc J. Bossuyt, *Guide to the “Travaux Préparatoires” of the International Covenant on Civil and Political Rights* (1987)，pp. 379-80.

[39] 见美洲国家组织，新闻稿 17/15。

[40] *R.*v. *Spencer* (2014).

[41] 2010 Hun-Ma 47, 252 (consolidated)号决定，2012 年 8 月 28 日宣布。

[42] McIntyre 诉俄亥俄选举委员会(1995)，第 342 和 343 页。

[43] 见新的《联邦刑事诉讼法》，第 244 条。

[44] 见阿根廷《宪法》，第 43 条；巴西《宪法》，第二篇，第一章第 5 条，XIV；厄瓜多尔《宪法》，第 20 条；巴拉圭《宪法》，第 29 条第 1 款。另请参阅智利《19,733 号法》；萨尔瓦多《刑事诉讼法》；巴拿马《第 67 号法》，第 21 条；秘鲁《刑事诉讼法》；乌拉圭《16.099 号法》；委内瑞拉玻利瓦尔共和国《4.819 号新闻法》，第 8 条。

[45] 参见：莫桑比克《宪法》第 48(3)条；安哥拉《第 7/06 号新闻法》，第 20 条第 1 款。

息来源保护，不过，随着时间推移，对记者的压力可损害这种保护。[46] 即使法律有规定，国家在实践中也经常侵犯来源匿名性。

禁止匿名

49. 禁止网上匿名干扰了言论自由权。许多国家禁止匿名，不论是否有任何具体的政府利益。《巴西宪法》(第 5 条)禁止匿名言论。《委内瑞拉玻利瓦尔共和国宪法》(第 57 条)也禁止匿名。2013 年，越南取缔使用假名，迫使有个人博客的个人公开真实姓名和住址。[47] 2012 年，伊朗伊斯兰共和国要求登记国内正在使用的所有 IP 地址，并要求网吧用户在使用计算机前登记实名。[48] 厄瓜多尔法律要求网站评论人和手机持有人实名登记。[49]

50. 某些国家通过了法律，要求在线活动实名登记，这是一种对匿名的禁令。在俄罗斯联邦，每日有 3000 或更多读者的博客作者必须向媒体监管人员登记并公开身份；据报告，网吧用户必须提供身份以连接公共无线设施。[50] 据报告，中国宣布了法规，要求互联网用户浏览某些网站实名登记并避免传播损害国家利益的内容。[51] 南非还要求在线和移动电话用户实名登记。[52]

51. 同样，政府经常要求 SIM 卡登记；例如，非洲近 50 个国家要求或正在作出要求，在激活 SIM 卡时，登记个人身份数据。[53] 2011 年以来，哥伦比亚制定了强制性手机登记政策；2010 年以来，秘鲁将所有 SIM 卡与国民身份证号码相联。[54] 其他国家正在考虑这种政策。这种政策直接影响匿名性，特别是对于仅可通过移动技术上网的人而言。强制性 SIM 卡登记可向政府提供监测个人和记者的能力，远远超出了政府的任何合法利益。

---

[46] 澳大利亚 2007 年《证据修订(记者特权)法》；加拿大，阿尔伯塔省王座法院，Wasylyshen 诉加拿大广播公司(2005)；日本，2006(Kyo)第 19 号案件(2006)；新西兰《证据法》，第 68 条(2006)。

[47] 人权观察社，“越南：新法令惩罚新闻界”，2011 年 2 月 23 日；自由之家，“越南：新闻自由”，2012 年；第 19 条，越南社会主义共和国总理对 2011 年关于新闻和出版活动的行政责任问题的第 02 号法令的评论 (2011 年 6 月)。

[48] 伊朗伊斯兰共和国，第 106 号法案，通信监管局。

[49] 参见：厄瓜多尔《通信组织法》(2013 年)。

[50] 428884-6 号法案修订《信息、信息技术和保护信息联邦法》和俄罗斯联邦关于使用信息和通信网络简化信息交换问题的若干法律；路透社，“俄罗斯要求互联网用户出示身份以使用公共 WiFi, ”2014 年 8 月 8 日。

[51] 《中国版权与媒体、互联网用户账号名称管理条例》，第 5 条(2015)。

[52] 南非，通信侦听条例与 2003 年与通信相关的第 70 号信息法的规定；另请参见 2002 年“电子通信和交易法(要求对服务提供商进行实名登记)。

[53] Kevin P. Donovan and Aaron K. Martin, “The Rise of African SIM Registration”，3 February 2014.

[54] 见：Colombia, Decree 1630 of 2011；Perú21, *Los celulares de prepago en la mira*，27 May 2010.

52. 通过拒绝提供使用途径，政府也试图打击匿名工具，例如 Tor、代理服务器和虚拟专用网络。长期以来，中国阻止使用 Tor；[55] 据报告，俄罗斯政府官员提供了超过 10 万美元用于识别匿名 Tor 用户的技术。[56] 此外，据报告，埃塞俄比亚、伊朗[57] (伊斯兰共和国)[58] 和哈萨克斯坦[59] 设法阻止 Tor 流量。因为这种工具可能是个人安全行使见解和言论自由的唯一机制，应保护和促进这些工具的使用。

公众骚乱期间的限制

53. 匿名言论对活跃分子和示威者是必要的，但在抗议期间，政府经常试图禁止或截取匿名通信。这种干扰言论自由的举动非法所追求的不正当目标是，破坏《世界人权宣言》和《公民权利和政治权利国际公约》下的和平抗议权。

中介责任

54. 一些国家和区域法院已开始对互联网服务提供商和媒体平台规定责任，以监管在线匿名用户的评论。例如，在《通信组织法》中，厄瓜多尔要求中介机构制定机制，记录个人数据，以便能够确定张贴评论的人员。在“Delfi 诉爱沙尼亚”(第 64569 号申请)中，欧洲人权法院维护了一部爱沙尼亚法律，该法律规定，媒体平台承担在其网站上贴载匿名诽谤言论的责任。此类中介责任很可能会导致实名登记政策，从而破坏匿名，或者，无法实施筛查程序的网站可能完全取消帖子，因而会对较小的独立媒体造成伤害。一个民间社会组织联盟起草的《关于中介方责任的马尼拉原则》最近获得通过，该《原则》为国家、国际和区域机制提供了保护在线言论的一套健全的指南。

数据保留

55. 广泛强制数据保留政策会限制个人保持匿名的能力。国家可要求互联网服务和电信提供商收集和存储记载所有用户在线活动的记录，这不可避免地导致国家掌握每个人的数字足迹。国家收集和保留个人记录的能力扩大了它进行监控的能力，增加了个人信息被盗或泄露的可能性。

---

[55] MIT Technology Review, *How China Blocks the Tor Anonymity Network*，4 April 2012.

[56] 最初报价见以下网址：http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html？regNumber=0373100088714000008.

[57] Runa Sandvik, Ethiopia Introduces Deep Packet Inspection, The Tor Blog (31 May 2012)；see also Article 19，12 January 2015.

[58] “Phobos”，“Iran partially blocks encrypted network traffic”，The Tor Blog (10 February 2012).

[59] “Phobos”，“Kazakhstan upgrades censorship to deep packet inspection”，The Tor Blog (16 February 2012).

五. 结论和建议

56. 加密和匿名，以及背后的安全理念，为在数字时代行使见解和言论自由权提供了必要的隐私和安全。这种安全对于行使其他权利(包括经济权、隐私权、正当程序、和平集会和结社自由以及生命权和身体完整)而言可能极其重要。由于加密和匿名对见解和言论自由权的重要性，必须按照合法性、必要性、相称性和目标正当性原则，严格限制对加密和匿名采取的限制措施。因此，特别报告员建议如下：

A. 国家

57. 国家应酌情修改或制订国家法律和法规，以增进和保护隐私权和见解与言论自由权。关于加密和匿名，国家应制定不限制或全面保护政策，仅在逐案基础上采取限制措施，这些限制满足合法性、必要性、相称性和目标正当性的要求，而且，任何具体限制均需有法院命令，并通过公众教育促进在线安全和隐私。

58. 对加密和匿名的讨论往往仅侧重于它们在恐怖主义时期可能用于犯罪目的。但是，紧急情况并不免除国家确保尊重国际人权法的义务。修订或制定个人在线安全限制措施的立法提案应进行公开辩论并按照正规、公开、知情的和透明的立法程序通过。国家必须促进广泛的民间社会行为方和少数群体有效参与这种辩论和进程，并避免在加速立法程序下通过这种法律。一般性辩论应强调加密和匿名尤其向面临非法干涉最大风险的群体提供的保护。任何这种辩论还必须考虑到，限制措施应受到严格测试：如果它们干扰了持有主张权，限制措施不得通过。可产生限制言论自由影响的对隐私的限制──就本报告而言，对加密和匿名的限制──必须由法律规定，对于实现很少数目的合法目标中的一个目标而言必须是必要的和相称的。

59. 国家应促进强大的加密和匿名。国家法律应承认，个人可自由使用允许匿名在线的加密技术和工具，保护其数字通信的隐私。保护人权维护者和记者的法律和法规还应包括某些条款，允许使用保障通信安全的技术并提供相关支持。

60. 国家不应限制加密和匿名，加密和匿名便利于而且经常促成见解和言论自由权。全面禁止是不必要的和不相称的。国家应避免采取削弱个人可在线享有的安全的各种措施，例如后门程序、弱化的加密标准和密钥托管。此外，国家不应将用户身份查验作为使用数字通信和在线服务的条件，不应要求手机用户登记 SIM 卡。公司也应考虑限制加密和匿名(包括通过使用假名)的自身政策。在不违反本国法律和国际法的情况下，法院命令的解密，只有在以下情况下才可被允许：它产生于透明的和向公众公开的法律，仅在有针对性的逐案基础上对个人适用(即不适用于大众)，而且须经司法授权和保护个人的正当程序权。

B. 国际组织、私人部门和民间社会

61. 国家、国际组织、公司和民间社会团体应促进在线安全。鉴于新通讯技术在增进人权和发展方面的相关性，所有有关人员应系统地促进使用加密和匿名的途径，不加歧视。特别报告员紧急呼吁联合国系统各机构，特别是参与人权和人道主义保护的机构，支持使用通信安全工具，以确保与其互动的人能够安全互动。联合国机构必须修订它们的通信惯例和工具，投资资源，提高通过数字通信与本组织互动的众多利害攸关方的安全性和保密性。人权保护机制在请求民间社会、人权侵权行为的证人和受害者提交资料和管理这些资料时必须特别注意。

62. 虽然本报告不就公司对通信安全的责任作出结论，然而，十分明确的是，鉴于对在线言论自由的威胁，公司应审查它们的做法相对于人权准则的适当性。在最低限度，公司应坚持《工商企业和人权问题指导原则》、《全球网络倡议的言论自由和隐私问题原则》、《欧盟委员会的信通技术部门执行联合国工商企业和人权问题指导原则的指南》，和《电信行业对话指导原则》中规定的原则。与政府一样，公司也不应阻止或限制传输加密通信，而应允许匿名通信。应注意作出努力，扩大加密数据中心链接的现有量，支持网站安全技术和开发广泛的默认端对端加密。提供技术损害加密和匿名的公司行为方在产品和客户方面应做到特别透明。

63. 应鼓励使用加密和匿名工具和提高数字素养。特别报告员认识到，加密和匿名工具的价值取决于对它们的广泛采用。他鼓励各国、民间社会组织和公司参与开展一个运动，使世界各地用户享有设计和默认加密，并且，在必要时，确保向面临风险的用户提供工具，以安全行使其见解和言论自由权。