联 合 国 A/HRC/39/29

大 会

Distr.: General
3 August 2018
Chinese
Original: English

人权理事会
第三十九届会议
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的报告

概要

本报告是依照人权理事会第 34/7 号决议提交的，理事会在决议中请人权事务高级专员编写报告，确定和阐明关于促进和保护数字时代隐私权的原则、标准和最佳做法，包括工商企业在这方面的责任，并提交理事会第三十九届会议。

GE.18-12799 (C) 160818 170818
1812799

一. 导言

1. 数字世界给隐私权带来挑战，应对这一挑战的需要，比以往任何时候都更加迫切。主要由私营部门推动的数字技术不断利用与人们生活相关的数据，不断向现代社会的社会、文化、经济和政治结构渗透。越来越强大的数据密集型技术，如大数据和人工智能，有可能创造出一个无孔不入的数字环境，使国家和工商企业都能够以前所未有的程度监视、分析、预测甚至操纵人们的行为。虽然不可否认的是，数据驱动的技术可以用于非常有益的用途，但这些技术发展如果不小心管理，就有可能在总体上对人的尊严、自主和隐私以及行使人权造成极大风险。

2. 国际和区域行为者越来越意识到这些挑战，并开始采取相应行动。人权理事会于 2015 年 7 月授权任命隐私权问题特别报告员。人权理事会和大会在许多决议中对国家监视措施和商业惯例带来的隐私风险表示关切。[1] 区域一级采取了若干加强数据隐私保护的措施，如欧洲联盟于近期生效并将产生全球影响的《通用数据保护条例》，欧洲委员会旨在修订《关于在自动处理个人数据方面保护个人的公约》并使之适应现代需要的议定书，以及非洲联盟委员会《非洲个人数据保护准则》。与此同时，多国政府均通过了增强监视权力的法律或立法草案，但监视方式往往不符合适用的国际人权标准。[2]

3. 本报告就如何应对数字时代隐私权面临的某些紧迫挑战提供了指导。报告简要概述国际法律框架，并讨论当前最重要的趋势。报告随后探讨国家的相关义务和工商企业的责任，包括讨论适当的保障和监督措施。最后一章就如何补救侵犯和滥用隐私行为给出了一些见解。

4. 本报告以高级专员 2014 年关于数字时代隐私权的报告(A/HRC/27/37)和 2018 年 2 月在日内瓦举行的专家研讨会上的发言和讨论为基础。[3] 报告还得益于广泛利益攸关方提交的 63 份书面材料。[4]

二. 理解数字时代的隐私权

5. 隐私权是一项基本人权，得到《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的承认。[5], [6] 隐私

[1] 例如，见大会第 68/167、第 69/166 和第 71/199 号决议，以及人权理事会第 28/16、第 34/7 号决议和第 25/117 号决定。

[2] 例如，见 Anja Seibert-Fohr, “Digital surveillance, metadata and foreign intelligence cooperation：unpacking the international right to privacy” (2018 年 4 月)，可查阅 https://ssrn.com/abstract=3168711; https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee and www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyin DigitalAge/SR_right_privacy.pdf。

[3] 参见 www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgePrivacyWorkhop.aspx，网播可查 http://webtv.un.org/search/part-1.1-un-expert-workshop-on-the-right-to-privacy-in-the-digital-age/5734527899001/?term=2018-02-19&sort=date&page=2。

[4] 所有书面材料可查阅 www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx。

[5] 例如，参见《儿童权利公约》第 16 条、《保护所有移徙工人及其家庭成员权利国际公约》14 条，以及《残疾人权利公约》第 22 条。

[6] 例如，参见《非洲儿童权利与福利宪章》第 10 条、《美洲人权公约》第 11 条，以及《欧洲人权公约》第 8 条。

权可被视为假定个人理应拥有一个享受自主发展、互动和自由的领域，一个无须同他人产生关联的“私人领地”，不受国家干预，任何人未经允许不得擅自过度干涉(例如，参见 A/HRC/13/37, 第 11 段；以及 A/HRC/23/40, 第 22 和第 42 段)。在数字环境中，信息隐私尤其重要，它涵盖关于个人及其生活的现有的或可推导得出的信息，以及在这些信息的基础上作出的决定。

6. 保护隐私权的范围很广，不仅包括通信中包含的实质性信息，也包括元数据；因为对此类数据进行整合和分析，“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”(见 A/HRC/27/37, 第 19 段)。保护隐私权不仅限于私人、私密空间，例如个人住宅，还包括公共空间和公开的信息(CCPR/C/COL/CO/7, 第 32 段)。例如，当政府监视市场或火车站等公共空间，从而观察个人时，隐私权就会受到影响。同样，社交媒体上公开的个人信息如被收集和分析，这也涉及到隐私权。[7] 公开分享信息并不会使其内容不受保护。[8]

7. 他人或算法检查或使用个人信息进行，影响到隐私权。[9] 不仅如此，即使仅仅生成和收集与个人身份、家庭或生活相关的数据，也已经影响到隐私权，因为通过这些步骤，个人失去了对可能危及其隐私的信息的部分控制(见 A/HRC/27/37, 第 20 段)。[10] 此外，大规模监视方案只要存在，即构成对隐私的干涉(同上)。[11]

8. 隐私权平等地适用于每个人。对隐私权的保护，如因国籍或任何其他理由而出现任何差异，都不符合《公民权利和政治权利国际公约》第二十六条所载的平等和不歧视权利。

9. 国家必须尊重和确保在其权力范围内或者有效控制下的任何人享有《公约》所规定的权利。即使该人不在缔约国境内。[12] 只要一个国家对数字通信基础设施行使权力或行使有效控制，无论相关基础设施位于何处(例如，直接窃听或侵入该国境外的信息基础设施)，就要适用相关的人权法。同样，如果一个国家对实际控制某人信息的第三方(如云服务提供商)行使监督管辖权，则该国的人权保护工作应涵盖因对相关信息的访问或使用，其隐私可能受到影响的人(见 A/HRC/27/37, 第 34 段)。

10. 根据《公约》第十七条，任何干涉只有在既非任意也非非法的情况下才被允许。人权机制一贯将这些话解释为指向合法性、必要性和相称性等首要原则(见

[7] 见隐私国际为本报告提交的资料。

[8] Anja Seibert-Fohr, “Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy”。

[9] 见 Paul Bernal, “Data gathering, surveillance and human rights: recasting the debate”，*Journal of Cyber Policy*, vol. 1, No. 2 (2016)。

[10] 另见欧洲人权法院，Rotaru 诉罗马尼亚，第 28341/95 号申诉，2000 年 5 月 4 日的判决；以及 Kopp 诉瑞士，第 23224/94 号申诉，1998 年 3 月 25 日的判决。

[11] 另见欧洲人权法院，Roman Zakharov 诉罗马尼亚，第 47143/06 号申诉，2015 年 12 月 4 日的判决。

[12] 见联合国人权事务委员会关于公约缔约国承担的一般法律义务性质的第 31 号一般性意见(2004 年)，第 10 段。

A/HRC/27/37, 第 21-27 段)。[13] 根据这些原则，各国只能在法律规定的范围内干涉隐私权，相关立法必须详细说明允许这种干涉的确切情况。[14] 当法律未对干涉作出规定时，或当相关干涉行为有悖于《公约》的规定、宗旨和目标时，干涉均属非法和任意。[15] 限制措施只有服务于合法目的，才可认定为合法和非任意(见 A/HRC/29/32, 第 33 段)。这种限制必须是实现合法目的所必需的，与该目的相称，而且必须是现有侵扰性最小的选择。此外，对隐私权的任何限制都不能使这项权利的实质变得毫无意义(见 A/69/397, 第 51 段)。

11. 隐私权是在线和离线享有和行使人权的核心。它是民主社会的基础之一，对实现广泛人权发挥着关键作用，其中包括言论自由(见 A/HRC/23/40 和 A/HRC/29/32, 第 15 段)、结社和集会自由 (见 A/HRC/31/66, 第 73-78 段；A/72/135, 第 47-50 段)，以及禁止歧视等等。[16] 干涉隐私权会对某些个人和(或)群体产生不成比例的影响，因而加剧不平等和歧视。[17] 隐私法规过于宽泛，也可能构成对其他权利的不当限制，特别是限制言论自由，例如当法规过度干涉合法新闻报道、艺术表达或科学研究时。由于篇幅所限，本报告无法探讨隐私权与所有其他人权之间的相互关系、隐私权对特定个人和群体的歧视性影响以及保护这些权利的方法。

三. 干涉隐私：趋势及问题

A. 政府和工商企业日益依赖个人数据

数字足迹不断增多

12. 国家和工商企业都在收集和使用与个人私生活相关的数据，其数量稳步增加。个人电脑、智能手机、智能手表、健身追踪器和其他可穿戴设备正在收集与数十亿人相关的大量数据流。安装在所谓的智能住宅和智能城市中的其他互联设备和传感器数量迅速增多，补充了更多的数据。所收集和使用的信息范围深广，既有设备标识符、电子邮件地址和电话号码，又有生物特征、健康和财务数据以及行为模式。这在很大程度上是在当事人不知情的情况下发生的，也没有得到当事人的实际同意。

数据共享与融合

13. 工商企业和国家不断交换和融合来自各种来源和数据库的个人数据，数据经纪人在其中占据关键位置。结果，个人发现自己处于无能为力的境地，因为几乎不可能追踪谁掌握着关于他们的何种信息，更不用说控制这些信息的多种使用方式了。

[13] 见人权理事会第 34/7 号决议，第 2 段。

[14] 见人权事务委员会关于隐私权的第 16 号一般性意见(1988 年)，第 3 和第 8 段。

[15] 同上，第 4 段。

[16] 见 Paul Bernal, “Data gathering, surveillance and human rights: recasting the debate”。

[17] 见大会第 71/199 号决议，第 5(g)段；人权理事会第 34/7 号决议，第 5(g)段；以及国际公民自由组织网络为本报告提交的材料。

生物识别数据

14. 国家和工商企业越来越多地部署依赖生物识别数据，例如 DNA、面部几何形状、语音、视网膜或虹膜图案及指纹的收集和使用系统。一些国家建立了巨大的中央数据库储存这类信息，用于各种目的，从国家安全和刑事调查到提供基本服务(如社会和金融服务及教育)的个人身份识别。世界各地的国家当局在城市、火车站或机场部署闭路电视摄像头，利用面部识别技术自动识别和标记人员。生物识别技术越来越多地用于控制边境和境内的移民。大型生物识别数据库的出现引起了重大的人权问题。这种数据特别敏感，因为根据定义，它与特定个人和该人的生活不可分割地联系在一起，并且有可能被严重滥用。例如，利用生物识别技术盗用身份的行为极难补救，可能严重影响个人权利。此外，生物识别数据可能被用于收集数据以外的目的，包括非法跟踪和监控个人。鉴于这些风险，应特别注意生物识别数据收集的必要性和相称性问题。在这种背景下，令人担忧的是，一些国家在没有适当的法律和程序保障的情况下，正在着手实施大量基于生物识别数据的项目。

日益强大的分析能力

15. 数据驱动型技术的分析能力一直呈指数级增长。大数据分析和人工智能使国家和工商企业越来越有能力获得关于人们生活的精准信息，推断他们的身心特征，并创建详细的人格档案。政府和工商企业使用的许多系统都是为此目的而构建的——最大限度地增加个人信息的数量，以便分析、描述、评估、分类并最终作出决策，且这一过程通常是自动化的。

16. 由此产生的环境给个人和社会带来了难以估量的风险。例如，近年来发生了大范围数据泄露的情况，使相关人员面临身份被盗和隐私信息泄露。非法的数据收集和分析已用于瞄准特定选民。个人貌相、“评分”和“排名”可用于评估医疗保健、其他保险、金融服务等方面的资格。在重大案件中，例如在量刑程序和累犯评估时，基于数据的不透明决定可能威胁到正当程序。鉴于透明度、过于宽泛、问责制和可能造成歧视性后果等问题，试图用预测性警务的办法，甄别哪些个人构成潜在安全威胁的做法引起了人们的关切。[18]

B. 国家监控和通信截取

大规模监控

17. 许多国家继续进行秘密的大规模监控和通信截取活动，收集、存储和分析所有用户使用各种通信手段(如电子邮件、电话和视频通话、短信和访问网站)的数据。虽然某些国家声称这种无差别的大规模监控是维护国家安全所必需的，但这种做法是国际人权法不允许的，“因为在采取此类措施的情况下，不可能作出个性化的必要性和适度性分析”(见 A/HRC/33/29, 第 58 段)。[19] 正如欧洲人权法院

[18] 见 Ajay Sandhu, “Data driven policing：highlighting some risks associated with predicting crime”，埃塞克斯大学人权中心。

[19] 另见 A/HRC/27/37, 第 25 段。

指出的，“为保护国家安全而建立的秘密监控系统，可能打着捍卫民主的幌子破坏甚至摧毁民主”。[20]

获取工商企业的客户数据

18. 国家经常依靠工商企业收集和截取个人数据。例如，一些国家强迫电信和互联网服务提供商允许国家直接获取通过其网络运行的数据流。这种直接获取数据的制度令人严重关切，因为它们特别容易被滥用，并往往绕过关键的程序保障。[21] 一些国家还要求获取电信和互联网服务提供商收集和存储的大量信息。各国继续对电信公司和互联网服务提供商规定强制性义务，要求它们长期保留通信数据。[22] 许多这样的法律要求公司不加区分地收集和存储所有订户和用户利用所有电子通信手段的所有流量数据。它们限制人们匿名通信的能力，造成滥用的风险，并可能有助于通过黑客或其他数据泄露方式，将数据泄露给罪犯、政治对手或商业竞争对手等第三方。这种法律超出了可视为必要和相称的限度。[23]

黑客侵入

19. 政府似乎越来越依赖侵入个人数字设备的攻击性入侵软件。这种类型的黑客攻击能够不加区分地截取和收集所有类型的通信和数据，无论是否加密，此种行为还允许远程秘密访问个人设备和存储在这些设备上的数据，从而能够对这些设备上的数据进行实时监控和操纵。[24] 这种做法威胁到的不仅是隐私权，还有在法律诉讼中使用这种证据的程序公正权。(见 A/HRC/23/40, 第 62 段)。黑客行为也引起了重大的治外法权问题，因为它可能影响到处于不同管辖范围的个人。[25] 此外，黑客依靠利用信息和通信技术系统中的漏洞，对数百万用户造成安全威胁。

试图削弱加密和匿名

20. 各国一再试图削弱加密技术并限制匿名工具的使用，同样威胁到在线通信和其他活动的安全性和保密性。一些国家要求在加密通信中设置法定后门，要求加密通信服务提供商交出加密密钥(见 A/HRC/29/32, 第 38-45 段)，甚至禁止或阻止某些安全通信应用，包括加密消息传递工具以及私有和匿名化虚拟网络。加密和匿名为个人和团体提供了一个在线隐私区，他们可以持有各种观点并行使表达

[20] 见 Roman Zakharov 诉俄罗斯，第 232 段。

[21] 见 Roman Zakharov 诉俄罗斯，第 270 段。

[22] 见 CCPR/C/ZAF/CO/1，第 42-43 段；以及 CCPR/C/PAK/CO/1，第 35-36 段。

[23] 例如，见欧洲法院第 C-203/15 和第 C-698/15 号合并案件，Tele2 Sverige AB 诉瑞典邮电局以及内政部长诉 Watson, 2016 年 12 月 21 日的判决，第 107 段；CCPR/C/ZAF/CO/1, 第 42-43 段；以及 CCPR/C/CMR/CO/5, 第 39-40 段。

[24] 见促进和保护意见和表达自由权问题特别报告员，“加密和匿名问题后续报告”(2018 年 6 月)。

[25] 见隐私国际提交的材料。

自由，不受任意和非法的干扰或攻击(A/HRC/29/32)。[26] 加密和匿名工具在世界各地被广泛使用，用户包括人权维护者、民间社会、记者、举报人和面临迫害和骚扰的持不同政见者。削弱这些工具会危害所有用户的隐私，使他们不仅受到国家的非法干涉，还受到包括犯罪网络在内的非国家行为者的非法干涉。[27] 这种广泛和不加区分的影响不符合相称性原则(见 A/HRC/29/32, 第 36 段)。

情报共享

21. 全球各国政府经常分享关于个人的情报，且不受任何法律框架制约，得不到适当监督。[28] 情报共享构成了一个严重的风险，即一个国家可能利用这种方法来规避国内法律限制，依靠他人获取并共享信息。这种做法不能通过合法性测试，并可能损害隐私权的实质(见 A/HRC/27/37, 第 30 段)。当与法治薄弱和(或)有系统侵犯人权历史的国家分享情报时，对人权保护的威胁尤其严重。一国可能是违反国际法从另一国取得情报，包括通过酷刑和其他残忍、不人道或有辱人格的待遇取得。情报分享安排目前缺乏透明度、问责制和监督，加剧了情报分享带来的人权风险(见 A/69/397, 第 44 段；CCPR/C/GBR/CO/7, 第 24 段；以及 CCPR/C/SWE/CO/7, 第 36 段)。除极少数情况外，立法没有将情报共享置于适当的法定基础上，不符合国际人权法的合法性原则。[29]

跨境获取工商企业持有的数据

22. 近来，人们一直在努力建立相关法律机制，以方便国家获取存储在国外工商企业服务器上的个人信息。毫无疑问，在刑事调查过程中获取证据是一个重要而合法的目标。然而，这种取证可能导致削弱或规避程序保障，例如要求独立机构授权和建立适当监督机制。跨境请求也可能对个人诉诸上诉和补救机制产生不利影响。尤其令人关切的是，法治薄弱和(或)人权记录有问题的国家有可能获得关于个人的敏感信息，却不充分保护人权免遭践踏。

四. 国家的责任

A. 国家有责任尊重且有义务在数字时代保护隐私权

23. 《公民权利和政治权利国际公约》第二条第 1 款要求各国“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，不得歧视。国家不得侵犯《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

[26] 另见加州大学欧文分校法学院国际私法诊所，“Selected references: unofficial companion to report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and the freedom of expression”；Amnesty International, “Encryption. A matter of human rights” (2016 年 3 月)；以及 Wolfgang Schulz and Joris van Hoboken, “Human rights and encryption”, United Nations Educational, Scientific and Cultural Organization (2016)。

[27] 见 www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=17138。

[28] 见隐私国际，《Secret Global Surveillance Networks：Intelligence Sharing between Governments and the Need for Safeguards》(2018 年 4 月)；以及 www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf。

[29] 见隐私国际提交的材料。

中任何权利进行限制。[30] 然而，国家的义务不限于尊重的义务，还包括采取“积极”措施，保护权利的享有。在隐私权方面，这意味着国家有义务采取立法和其他措施，禁止和保护免遭非法或任意干涉及攻击，无论这些干涉和攻击来自国家当局还是自然人或法人。[31]

24. 这种保护义务体现在《工商企业与人权指导原则》题为“国家保护人权的义务”的第一支柱中，该支柱阐述了国家有义务保护个人免受涉及企业的不利人权影响的含义。《指导原则》原则 1 要求采取适当步骤，通过有效的政策、法律、条例和裁定，防止、调查、惩治和补救侵犯人权行为。随后的各项原则概述了不同的法律和政策领域，各国应在这些领域采取“明智的组合措施”，即国家和国际措施、强制性措施和自愿性措施，促进企业尊重人权。[32] 信通技术部门有一些适用《指导原则》规定方法的例子，包括在欧洲联盟层面上制定的部门指南，其侧重点是信通技术企业应如何消除其活动的任何不利影响。

25. 国家有义务保护隐私权不受在其管辖范围内注册或设立的公司及其他第三方的侵犯，该义务具有域外效力。例如，各国应建立适用于监控技术的出口管制制度，规定评估目的地国使用该技术的法律框架、拟议最终用户的人权记录，以及使用监控权力的现有保障和监督程序。国家应将人权保障纳入出口许可协议。此外，各国有义务保护其管辖范围内的个人的隐私权不受域外干涉，例如截取通信或黑客攻击。

B. 国家有责任实施充分保障和有效监督

26. 隐私权的享有，在很大程度上取决于提供充分保障的法律、监管和体制框架，包括有效的监督机制。在国家和工商企业可以获取大量个人数据，而个人对如何使用关于他们及其生活的信息的了解和控制有限的时代，必须特别关注采取措施，缓解这种权力和信息的不对称对人权的影响。

1. 防止不当干涉的总体框架

27. 国家隐私保护框架的一个基石应该是制定相关法律，确定国家和私人行为者处理个人信息的标准。[33] 虽然各国可自行界定制约公司使用个人信息的明智措施组合，但《公民权利和政治权利国际公约》第十七条第 2 款规定需要依法保护个人。公共和私人数据处理之间的联系日益紧密，迄今为止的记录表明，一些工商企业经常大规模滥用个人信息，这些情况证实需要采取立法措施，从而对隐私给予足够程度的保护。[34]

[30] 见人权事务委员会第 31 号一般性意见，第 6 段。

[31] 见人权事务委员会第 16 号一般性意见，第 1 和第 9 段；第 31 号一般性意见，第 8 段。

[32] 见原则 2，评注。

[33] 见人权事务委员会第 16 号一般性意见，第 9 段；A/HRC/13/37，第 61 段；A/HRC/17/27，第 56 段。关于数据隐私立法的全球概述，见 Graham Greenleaf，新南威尔士大学向本报告提交的材料。在本报告中，“处理”被理解为包括对个人数据执行的任何操作，包括收集、保留、使用、修改、擦除、披露、转移和组合等操作。

[34] 见人权理事会第 34/7 号决议，第 5(f)段，以及第 38/7 号决议，第 17 段。

28. 对于规范国家、工商企业和其他私人行为者处理个人数据的最低标准，全球日益形成共识。体现出这种新情况的国际文书和准则有：1990 年《电脑个人数据档案的管理准则》；欧洲委员会 1981 年《关于在自动处理个人数据方面保护个人的公约》及其设定了较高的全球保护水准的现代版；[35] 1980 年经济合作与发展组织《隐私准则》(2013 年更新)；2014 年《非洲联盟网络安全和个人数据保护公约》(《马拉博公约》)；数据保护和隐私专员国际会议马德里决议，以及 2015 年《亚太经济协调隐私框架》等等。这些标准，特别是《关于在个人数据自动化处理方面保护个人的公约》，为许多国家的数据隐私框架提供了参考信息，可以为适当政策工具的设计提供指导。[36]

29. 上述文书和准则载有一系列关键原则、权利和义务，确保对个人数据的最低限度保护。首先，处理个人数据应该公平、合法和透明。应向其数据被处理的个人告知数据处理情况、处理的环境、特征和范围，包括通过透明的数据隐私政策加以告知。为了防止个人信息被任意使用，个人数据的处理应该基于当事人的自由、具体、知情和明确同意，或者法律规定的其他合法理由。[37] 个人数据处理应该是必要的，并且与处理实体应具体说明的合法目的相称。因此，数据的数量和类型及保留期需要加以限制，数据必须准确，并且尽可能使用匿名化和假名化技术。应避免未经当事人同意而改变目的，并且在改变目的时，应仅限于与最初说明的目的相一致的目的。考虑到个人数据容易在未经授权的情况下被披露、修改或删除，必须采取充分的安全措施。此外，处理个人数据的实体应对遵守适用的数据处理法律和政策框架负责。最后，敏感数据应享有特别高的保护级别。[38]

30. 上述所有文书和准则都承认，需要向数据正在被处理的个人提供某些权利。至少，受影响者有权知道个人数据已被保留和处理，有权访问存储的数据，有权纠正不准确或过时的数据，有权删除或纠正非法或不必要存储的数据。较新的文书增加了重要的补充权利，特别是反对个人数据处理的权利，至少是在处理实体没有证明处理工作合法且有充分理由的情况下。[39] 各国应特别注意提供强有力的保护，防止通过貌相分析和自动化决定干涉隐私权。上述权利也应适用于通过自动化手段获得、推断和预测出的信息，只要这些信息可以算作个人数据。法律框架必须确保这些权利不会不当限制表达自由权，包括出于新闻、艺术和学术目的处理个人数据的情况。

31. 数据隐私框架还应确立个人数据处理实体的某些义务。这些要求包括组织方面，如建立内部监督机制，但也包括强制性行动，如数据泄露通知和隐私影响评估。在日益复杂的技术环境中，这种评估在预防和减轻隐私受损方面发挥着关键

[35] 除欧洲委员会的 47 个成员国之外，毛里求斯、塞内加尔、突尼斯和乌拉圭也批准了《公约》，其他几个国家也正在加入过程中。

[36] 指南详见 https://privacyinternational.org/advocacy-briefing/2165/guide-policy-engagement-data-protection；以及立即连线组织，“Creating a data protection framework: a do’s and don’ts guide for lawmakers. Lessons from the EU general data protection regulation” (2018 年)。

[37] 见《关于在自动处理个人数据方面保护个人的公约》现代版第 5 条第(2)款；《马拉博公约》第 13 条第(1)款，以及马德里决议之原则 12。

[38] 见《关于在自动化处理个人数据方面保护个人的公约》现代版第 6 条。

[39] 同上，第 9 条第(1)款(d)项。另见《马拉博公约》一般数据保护条例第 21 条和《马拉博公约》第 18 条第(1)款。

作用。[40] 此外，与产品和服务设计相关的要求，如指定隐私[41] 和默认隐私[42]，也是保障隐私权的重要工具。

32. 在全球化的世界中，数据传输，包括大量个人数据的传输对于许多服务的运营来说是司空见惯和必要的。各国必须确保数据传输不构成或促成对隐私权的不当干涉。与此同时，严格的数据本地化要求应予避免，即不得要求所有数据处理实体必须在本国存储所有个人数据(见 A/HRC/32/38, 第 61 段)。相反，各国应侧重于确保传输到别国的个人数据得到保护，至少达到国际人权法要求的水平。

33. 国家应建立独立的个人数据处理监督机构。这些机构对于保护个人人权，防止过度处理个人数据的做法至关重要。监督机构需要一个法定地位，以便明确其任务、权力和独立性。应向此类监督机构提供必要的技术、财力和人力资源，以便有效监测国家和工商企业的数据处理活动，执行这方面的法律要求。此外，这些机构需要有足够的法律权威以履行其职能，包括对侵犯或践踏隐私权的行为处以相称的制裁。[43]

2. 针对监控和通信截取的程序保障和监督

保障措施

34. 国家必须依法开展各类与监视相关的活动(见 A/HRC/27/37, 第 28 段)，但隐私权问题特别报告员提醒人们注意此类立法普遍缺失的问题。值得注意的是，在许多管辖区域，情报和执法机构被排除在数据隐私立法的规定之外。基于必要性和相称性原则，应对这种例外加以限制，以确保政府所有部门在数据隐私方面达到适当水平。监控方面的具体立法应遵循以下最低标准。

35. 相关法律必须公开。法律的秘密规则和秘密解释不具备“法律”的必要特质(同上，第 29 段)。法律应足够准确。授予行政人员或法官的酌处权，以及如何行使这种酌处权，必须合理明确地加以限制(见 A/69/397, 第 35 段)。[44] 为此，必须说明罪行的性质和可能受到监视的人员类别。理由模糊和过于宽泛的规定，如笼统提到“国家安全”，都不能构成足够明确的法律。监视必须基于合理怀疑，授权此类监视的任何决定都必须有充分的针对性。[45] 法律必须严格赋予特定当局进行监控和获取监控成果的权限。

36. 就其范围而言，监督法律框架应涵盖国家对工商企业的各项要求。它还应涵盖获取域外信息或与其他国家分享信息的问题。需要在法律中明确建立相关结构，确保进行监控的政府组织内部的问责制和透明度。

[40] 关于对隐私影响评估的深入分析，参见 David Wright 和 Paul de Hert 编辑，《Privacy Impact Assessment》(New York, Springer, 2012)。

[41] 意思是必须从系统设计的一开始就将隐私保护纳入其中。

[42] 要求系统默认应用尊重隐私的设置。

[43] 参见，例如 https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/。

[44] 另见 Roman Zakharov 诉俄罗斯，第 230 段。

[45] 同上，第 248 和第 260 段。

37. 秘密监控的权力只有在为实现合法目的而绝对和明确必要时才是正当的(见A/HRC/23/40, 第 83(b)段)。[46] 秘密监控措施必须限于防止或调查最严重的犯罪或威胁。监视的持续时间应限制在实现既定目标所需的最低限度。使用和存储获得的数据必须遵循严格规则，必须严格根据必要性和相称性原则，明确界定收集和存储的数据在何种情况下必须删除。[47] 情报共享必须遵循同样的合法性、严格必要性和相称性原则。

38. 政府考虑采取有针对性的黑客措施时，应该采取极其谨慎的做法，只有在调查或预防最严重的犯罪或威胁的特殊情况下，并在司法部门的参与下，方可采取这种措施(见 CCPR/C/ITA/CO/6, 第 37 段)。[48] 黑客行动应严加设计，仅限获取特定目标和类型的信息。各国应避免强迫私人实体协助黑客行动，导致影响这些实体自身产品和服务的安全。强制解密只能在有针对性、逐案决定的基础上进行，而且须经司法授权和保护个人的正当程序权(见 A/HRC/29/32, 第 60 段)。

独立授权和监督[49]

39. 监控措施，包括向商业企业提出的通信数据请求和情报共享措施，应在所有阶段得到独立机构的授权、审查和监督，包括在执行这些措施的过程中和终止之后(见 CCPR/C/FRA/CO/5, 第 5 段)。[50] 授权采取特定监控措施的独立机构最好是司法当局，需要确保有充分的证据证明存在威胁，提议的监控应是有针对性的、严格必要的和相称的，并在采取监控措施之前授权(或拒绝)。

40. 监督框架可以将行政、司法和(或)议会监督结合起来。[51] 监督机构应独立于实施监控的当局，并配备适当和充分的专门知识、能力和资源。授权和监督应该在机构上分开。独立监督机构应主动调查和监测监控活动实施机构及可获取监控成果的机构的活动，并对监控能力和技术发展进行定期审查。如有要求，监控机构应提供有效监督所需的所有信息，并定期向监督机构报告，还应按要求保存采取的所有监控措施的记录。[52] 监督过程还必须透明，并接受适当的公众监督，监督机构的决定必须接受上诉或独立审查。在没有抗辩程序的情况下，让监督机构接触不同的观点，例如通过专家和多利益攸关方协商(例如，见 A/HRC/34/60, 第 36 段)，尤为重要：将“摩擦点”(对方法和理解的持续质疑)纳入其中，至关重要。[53]

[46] 另见 Szabo 和 Vissy 诉匈牙利，第 73 段。

[47] 见 Roman Zakharov 诉俄罗斯，第 231 段。

[48] 另见立即连线组织，“A human rights response to government hacking” (2016 年 9 月)，以及隐私国际，“Government hacking and surveillance: 10 necessary safeguards”。

[49] 见 A/HRC/34/60 以及欧洲联盟基本权利署，《Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II：Field Perspectives and Legal Update》(欧洲联盟出版办公室，卢森堡，2017 年)。

[50] 另见 Roman Zakharov 诉俄罗斯，第 233 段。

[51] 见大会第 71/199 号决议，第 5 (d)段。

[52] 见欧洲人权法院，Kennedy 诉联合王国，第 26839/05 号申诉，2010 年 5 月 18 日的判决，第 165 段，以及 Roman Zakharov 诉俄罗斯，第 272 段。

[53] 见埃塞克斯大学人权中心人权、大数据和技术项目为本报告提交的资料。

透明原则

41. 国家当局和监督机构还应参与公共宣传活动，介绍监控和通信截取以及其他形式的个人数据处理方面的现有法律、政策和做法，公开辩论和监督对于理解监控技术的优势和局限性至关重要(见 A/HRC/13/37, 第 55 段)。应该通知曾经受到监控的对象，事后向他们解释对其隐私权的干涉情况。他们也应有权更改和(或)删除不相关的个人信息，前提是这些信息无需继续用于任何当前或行将进行的调查(见 A/HRC/34/60, 第 38 段)。

五. 工商企业的责任

42. 《工商企业与人权指导原则》第二支柱为所有企业提供了防止和解决所有不利人权影响，包括隐私权所受影响的权威蓝图，无论其规模、所属部门、经营环境、所有制和结构如何。[54] 它概述了工商企业应尊重所有国际公认的人权的责任，这意味着它们应避免侵犯他人的人权，并应在自身卷入时，消除负面人权影响。[55] 尊重的责任适用于公司的所有活动和业务关系。无论受影响的人身在何处，尊重的责任都适用，这在数字领域尤其重要。尊重的责任独立存在，与国家是否履行自己的人权义务无关。

43. 尊重人权的责任要求工商企业：(a) 避免通过本身的活动造成负面人权影响；(b) 避免通过本身的活动直接或经由某个外部实体(政府、企业或其他实体)加剧负面人权影响；以及(c) 努力防止或缓解与其业务、产品或服务直接相关的不利人权影响，即使并非它们造成了此类影响。[56] 例如，一家公司如向政府提供用户数据，政府随后利用这些数据追踪和起诉持不同政见者，这将助长侵犯人权的行为，包括侵犯隐私权。制造和销售非法或任意入侵技术的公司也会对人权造成不利影响。

44. 如果尊重国际人权法与履行国家法律规定的义务之间存在相互冲突的要求，公司应努力尽可能尊重国际人权法，尽可能减轻任何不利影响，例如尽可能狭义地解释政府的要求。[57]

45. 尊重人权的责任要求工商企业制定适合其规模和情况的政策和程序，包括：

(a) 在最高层公开作出政策承诺，并在整个业务政策和程序中纳入尊重人权的责任；[58]

(b) 执行人权尽职调查程序，包括：

(一) 开展人权影响评估，确定和评估任何实际或潜在的不利人权影响；

[54] 《指导原则》经人权理事会第 17/4 号决议一致核可。

[55] 指导原则 11。

[56] 指导原则 13。另见另见人权高专办，《企业尊重人权的责任：解释性指南》(2012 年)。

[57] 指导原则 23。

[58] 指导原则 16。

(二) 综合这些评估起来，采取适当行动，防止和减轻已查明的不利人权影响；

(三) 跟踪这些努力的成效；

(四) 正式报告企业如何处理其人权影响；[59]

(c) 企业如果确认它们造成或加剧了不利影响，则应提供补救或在补救问题上给予合作。[60]

46. 根据《指导原则》，所有公司都有责任进行人权尽职调查，以确定和消除其活动对人权的任何影响。举一个具体的例子，销售监控技术的公司应该在任何潜在交易之前进行彻底的人权影响评估，作为尽职调查的一部分。减轻风险应包括，在合同协定中明确规定最终用途保证，辅以强有力的人权保障措施，防止任意或非法使用技术，并定期评估国家使用技术的情况。[61] 收集和保留用户数据的公司需要评估国家可能请求获取此类数据的隐私风险，包括当事国的法律和体制环境。它们必须规定适当的程序和保障措施，以防止和减轻潜在的隐私和其他人权损害。公司还需要进行人权影响评估，将其作为涉及安全与隐私的服务条款、设计和工程选择的采用，以及在特定情况下提供或终止服务的决定的一部分(见A/HRC/32/38, 第 11 段)。

47. 作为人权尽职调查进程的一部分，《指导原则》规定，工商企业应对如何消除其人权影响负责，并准备对外公布有关情况，尤其是在受影响利益攸关方提出关切时。[62] 在数字环境中，这意味着披露以下信息：收集了哪些个人数据，这些数据存储了多长时间，用于何种目的，如何使用，与谁共享以及在什么情况下共享。这包括各国收到的关于访问用户数据的请求。在国家法律法规阻止这种报告的情况下，公司应尽最大可能利用它们可能拥有的任何影响力，并鼓励公司倡导发布这种信息的可能性。

48. 作为落实其在《指导原则》下所作政策承诺的一部分，信通技术部门制定了关于如何实施人权政策的指南。这些倡议包括《全球网络倡议的言论自由和隐私原则》(全球网络倡议原则)[63] 和《电信业对话指导原则》[64]。例如，全球网络倡议原则具体规定，参与公司“将在个人信息方面采取保护措施”，并且“在面临政府要求、法律或法规以不符合国际公认法律和标准的方式损害隐私时，将尊重和努力保护用户的隐私权”。

[59] 指导原则 17-21。

[60] 指导原则 22 及本报告第六节。

[61] 见隐私国际，向促进和保护意见和表达自由权问题特别报告员提交的材料(2016 年 1 月)，可查阅 www.ohchr.org/Documents/Issues/Expression/PrivateSector/PrivacyInternational.pdf。

[62] 指导原则 21。

[63] 可查阅 https://globalnetworkinitiative.org/gni-principles/。另见全球网络倡议为本报告提交的材料。

[64] 可查阅 www.telecomindustrydialogue.org/about/guiding-principles/。

49. 数字权利排名组织的企业责任指数评估了一些互联网、移动和电信公司，特别是它们披露的影响表达自由和隐私的承诺和政策。[65] 这可作为一个有用工具，让公司对其影响用户权利的情况负责。

六. 补救办法

50. 国家和(或)工商企业侵犯或践踏隐私行为的受害者必须有机会获取有效补救。国家不仅有义务确保对国家行为者侵犯人权的行为问责并采取补救措施，还必须采取适当步骤，确保与工商企业有关的侵犯人权行为的受害者能够获得有效补救(见《工商企业与人权指导原则》第三支柱)。根据具体案件或情况的性质，受害者应该能够通过有效的司法或非司法的国家申诉机制获得补救(A/HRC/32/19, Corr.1 和 Add.1；以及 A/HRC/38/20 和 Add.1)。信通技术背景下的国家相关非司法机制包括有权监督国家和私营部门数据隐私做法的独立机构，如隐私和数据保护机构。

51. 根据《指导原则》，当工商企业确定自身造成或加剧了不利的人权影响时，则应通过合法程序补救自身造成或加剧的任何不利人权影响，或在补救问题上给予合作。[66] 任何非司法机制要想有效，都应是合法、可用、可预测、公平、权利兼容、透明的，还应有持续的学习来源，业务层面的申诉机制应立足对话和参与。[67]

52. 如果企业没有造成或加剧不利影响，但这种影响通过业务关系与其业务、产品或服务直接相关，则指导原则 19 阐述了适当的行动。这可能包括利用企业对其业务伙伴或客户可能拥有的任何影响力，寻求对其施加影响，以提供补救措施。[68]

53. 《指导原则》还强调业务层面申诉机制在直接处理申诉方面可以发挥的作用。这种机制可能采取各种形式，取决于有关公司的类型、利益攸关方的需要以及公司的人权风险状况。为了确定这些机制在信通技术部门的实际设计和运作方式，有必要在信通技术部门内部以及与利益攸关方进一步讨论。

54. 实际上，在为侵犯隐私行为提供补救途径方面，存在着巨大的差距和障碍。监控、通信截取和多种形式的个人数据处理的跨国性质和影响形成各种法律和实际挑战(见 A/HRC/34/60, 第 34 段)。此外，受害者缺乏关于不当干预的知识或证据是获得补救的常见障碍(见 A/HRC/27/37, 第 40 段)。例如，国家要求获取公司持有的数据时，往往同时下达禁止公司通知当事人的“禁令”。国家也常常不通知那些受到其他监控措施影响的人，特别在实施大规模监控的情况下。人们承认提前通知或同时通知可能危害合法监控措施的有效性，但是一旦监控工作结束，就应该通知个人(见 A/HRC/23/40, 第 82 段)。如果做不到这点，则法律应大度地

[65] 见 https://rankingdigitalrights.org/index2018/。

[66] 指导原则 22。

[67] 指导原则 31。

[68] 指导原则 19 及其评注。另见人权高专办，《企业尊重人权的责任：解释性指南》，第 48-52 页。

将诉讼权赋予那些理论上可能受到这些措施影响的人(见 A/HRC/13/37, 第 38 段)。同样，工商企业一旦发现可能影响客户权利的个人数据泄露，就应该通知其客户。

55. 在依靠算法作决策的情况下，受害者还面临着越来越多的新挑战，在这种情况下，个人可能无法获取输入数据，或者质疑算法本身得出的结论，或者质疑这些结论在决策过程是如何使用的。[69] 国家和工商企业应与其他利益攸关方合作，考虑解决这一问题的可能机制，例如建立资源充足的专家审计机构。

56. 侵犯隐私所造成伤害的性质也带来进一步挑战。侵犯隐私产生的影响很难消除，可能导致持续的后果和进一步的人权影响。数据和貌相易于保存、共享、重新调整用途和融合，这影响到数字数据的持久性，意味着个人未来的权利可能面临持续的新风险。[70]

57. 即使没有可量化的经济或其他影响，伤害隐私也会严重影响一个人的生活；伤害的性质不应妨碍受害者寻求补救。例如，可以增强消费者保护组织的权能，代表企业践踏隐私行为的受害者寻求补救。

七. 结论和建议

58. 国际人权框架为制定应对数字时代出现的多种挑战的对策奠定了坚实的基础。各国迫切需要充分履行尊重隐私权的义务，并承担其保护隐私权的责任，包括应对企业践踏隐私权的问题。为了实现这一目标，各国需要建立适当的法律和政策框架，包括充分的隐私保护立法和条例，将合法性、相称性和必要性原则纳入其中，并制定保障、监督和补救措施。

59. 本报告无法解决的许多问题有待进一步深入研究，包括隐私权与包括经济、社会和文化权利在内的其他人权之间的相互关系；侵犯隐私对处于危险中的个人和(或)群体造成的严重或歧视性影响；大数据和机器学习，包括出于预测和先发制人的目的，对享有隐私权和其他人权的影响，以及监控技术市场的监管问题。

60. 有效应对侵犯隐私权行为的补救措施的性质和形式，是另一个值得进一步关注的领域。作为第一步，应该全面确定在不同情况下适当补救行动的类型。这可用于制定进一步的指南。在进行这一分析时，应适当考虑联合国人权事务高级专员办事处(人权高专办)问责和补救项目制定的指导意见和建议。更一般地来说，应努力开发针对具体部门的商业责任指导工具，以尊重隐私权。

61. 高级专员建议各国：

(a) 认识到新技术，特别是数据驱动型技术对隐私权以及所有其他人权的全面影响；

(b) 通过强有力的和全面的隐私立法，包括关于数据隐私的立法，在保障、监督和补救措施方面遵守国际人权法，以有效保护隐私权；

[69] 见埃塞克斯大学人权、大数据和技术项目提交的材料，第 33 页。

[70] 同上，第 7 段。

(c) 确保数据密集型系统，包括涉及收集和保留生物特征数据的系统，只有在国家能够证明它们对于实现合法目标是必要和相称的情况下才能部署；

(d) 建立有权监督国家和私营部门数据隐私做法的独立机构，调查侵权行为，接受个人和组织的投诉，并对私营和公共机构非法处理个人数据的行为处以罚款和其他有效处罚；

(e) 通过适当的立法和其他手段，确保任何干涉隐私权的行为，包括通信监控和情报共享行为，均遵守国际人权法，包括合法性、合法目的、必要性和相称性原则，不论受影响个人的国籍或处所为何；并明确授权采取监控措施需有合理怀疑，即怀疑特定个人已经或正在实施刑事犯罪或正在实施对国家安全构成具体威胁的行为；

(f) 加强国家监控行为的独立授权和监督机制，确保这些机制有能力和充足的资源来监督和落实监控措施的合法性、必要性和相称性；

(g) 审查相关法律，确保这些法律不要求电信和其他公司全面、不加区分地保留通信数据；

(h) 采取步骤，加强国家获取监控技术的透明度和问责制；

(i) 充分履行国家的保护责任，防止包括信通技术部门在内的所有相关部门的工商企业不侵犯隐私权，为此应采取适当步骤，通过有效的政策、立法、规章和裁决，防止、调查、惩罚和纠正侵犯隐私权的行为；

(j) 确保侵犯和践踏隐私权行为的所有受害者都能获得有效的补救，包括在跨境案件中。

62. 高级专员建议工商企业：

(a) 尽一切努力履行企业尊重隐私权和所有其他人权的责任。工商企业至少应充分实施《工商企业与人权指导原则》，这意味着在其所有业务以及对所有人权，包括隐私权方面进行有效的人权尽职调查，并采取适当行动防止、减轻和消除实际和潜在的影响；

(b) 努力确保企业传输的任何通信及其收集、存储或以其他方式处理的个人数据具有高度的安全性和保密性。持续评估如何最好地设计和提高产品和服务的安全性；

(c) 遵守本报告第 29 至第 31 段中提到的关键隐私原则，确保涉及用户和客户隐私权的内部政策和做法尽可能透明；

(d) 通过合法程序，包括通过有效的业务层面申诉机制，对企业自身造成或加剧的不利影响提供补救或给予合作；

(e) 促进人权高专办问责和补救项目在制定指导意见和建议，以提高非国家申诉机制在数字空间践踏隐私权问题上的效力方面的工作。