O DIREITO À PRIVACIDADE NA ERA DIGITAL

Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos

Documento original

United Nations

Tradução

IRIS
INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

United Nations
Digital Library

Esta versão em português do Brasil de ***The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights*** **(A/HRC/51/17)** não é uma tradução oficial das Nações Unidas. A tradução foi realizada por Projeto Comunicações Privadas, Investigações e Direitos, do Instituto de Referência em Internet e Sociedade, que assume toda a responsabilidade pela acurácia da versão

Nações Unidas A/HRC/51/17
Assembleia Geral
Distr.: General
4 de agosto de 2022
Original: inglês

Conselho de Direitos Humanos
Quinquagésima-primeira sessão
12 de setembro a 7 de outubro de 2022
Itens 2 e 3 da agenda

Relatório anual do Alto Comissariado das Nações Unidas para os Direitos Humanos e Relatórios do Gabinete do Alto Comissariado e do Secretário-Geral
Promoção e proteção de todos os direitos humanos, civis, políticos, econômicos, sociais e culturais, incluindo o direito ao desenvolvimento

O direito à privacidade na era digital

Relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos*

TRADUÇÃO
Luíza Dutra
Paulo Renáda Silva Santarém

REVISÃO
Gustavo Rodrigues

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO
Felipe Duarte

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

DIREÇÃO

Paloma Rocillo e Gustavo Rodrigues

MEMBROS

Ana Bárbara Gomes | Coordenadora de Políticas Públicas e Pesquisadora
Felipe Duarte | Coordenador de Comunicação
Fernanda Rodrigues | Coordenadora de Pesquisa e Pesquisadora
Juliana Roman | Pesquisadora
Júlia Caldeira | Pesquisadora
Lucas Samuel | Estagiário de pesquisa
Luiza Dutra | Pesquisadora
Paulo Renã da Silva Santarém | Pesquisador
Rafaela Ferreira | Estagiária de pesquisa
Thais Moreira | Estagiária de comunicação
Victor Barbieri Rodrigues Vieira | Pesquisador
Wilson Guilherme | Pesquisadore

irisbh.com.br

I. Introdução

1. O presente relatório é entregue de acordo com a resolução 48/4 do Conselho de Direitos Humanos, na qual o Conselho solicitou ao Escritório do Alto Comissariado das Nações Unidas para os Direitos Humanos (ACNUDH) que preparasse um relatório identificando tendências e desafios recentes com relação ao direito humano à privacidade e que identificasse e esclarecesse princípios, salvaguardas e melhores práticas de direitos humanos pertinentes, e que apresentasse o relatório ao Conselho em sua quinquagésima primeira sessão. O relatório reflete as respostas recebidas à chamada por contribuições emitida pelo ACNUDH.[1]

2. Pessoas ao redor do mundo estão testemunhando desenvolvimentos tecnológicos impressionantes, bem como inovações que melhoram a vida das pessoas e impulsionam as economias. No entanto, elas também experimentam como as ferramentas digitais podem se voltar contra elas, expondo-as a novas formas de monitoramento, perfilamento e controle. Garantir o respeito ao, e a proteção do, direito à privacidade, reconhecido no artigo 12 da Declaração Universal dos Direitos Humanos, no artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos e em muitos outros instrumentos internacionais e regionais de direitos humanos,[2] pode desempenhar um papel central na gestão de novas ameaças digitais aos direitos humanos, que estão intrinsecamente ligadas aos dados pessoais que alimentam os motores das sociedades digitalizadas.

3. Com base em relatórios anteriores ao Conselho de Direitos Humanos que abordam os desafios ao direito à privacidade,[3] o presente relatório se concentra em três tendências notáveis relacionadas ao papel dos Estados na salvaguarda e promoção do direito à privacidade: (a) o abuso generalizado de ferramentas intrusivas de *hackeamento*; (b) o papel fundamental de criptografia robusta para garantir o exercício do direito à privacidade e de outros direitos; e (c) o monitoramento generalizado dos espaços públicos. O relatório destaca o risco muito real e crescente de criar sistemas de vigilância e controle abrangentes que podem eventualmente sufocar o desenvolvimento de sociedades vibrantes, prósperas e que respeitam direitos, concluindo com um conjunto de recomendações para evitar tal resultado.

II. Vigilância de dispositivos pessoais e comunicações

A. Hackeamento

4. Em julho de 2021, o Forbidden Stories, um consórcio de jornalismo investigativo, apoiado pela Anistia Internacional, publicou revelações sobre o uso do *software* Pegasus que

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

2 Ver artigo 16 da Convenção sobre os Direitos da Criança; artigo 14 da Convenção Internacional sobre a Proteção dos Direitos de Todos os Trabalhadores Migrantes e Membros de Suas Famílias; artigo 22 da Convenção sobre os Direitos das Pessoas com Deficiência; artigo 10 da Carta Africana dos Direitos e Bem-Estar da Criança; artigo 11 da Convenção Americana sobre Direitos Humanos; e artigo 8 da Convenção para a Proteção dos Direitos Humanos e Liberdades Fundamentais.

3 Ver A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 e A/HRC/48/31.

chamaram a atenção internacional para uma crise de direitos humanos que vinha crescendo há anos – ou seja, a proliferação global de ferramentas de hackeamento para a vigilância direcionada e secreta de dispositivos digitais. Embora supostamente sejam empregadas para combater o terrorismo e o crime, essas ferramentas de programas espiões têm sido frequentemente usadas por razões ilegítimas, inclusive para reprimir opiniões críticas ou dissidentes, e aqueles que as expressam, incluindo jornalistas, figuras políticas da oposição e defensores dos direitos humanos.

5. A extensão das operações com o programa espião Pegasus e o número de vítimas são impressionantes. Com base em uma lista vazada de mais de 50.000 números de telefone de alvos de vigilância potenciais e reais, e em uma análise forense de vários telefones infectados, relatórios em 2021 revelaram que pelo menos 189 jornalistas, 85 defensores de direitos humanos, mais de 600 políticos e funcionários do governo, incluindo ministros, e diplomatas foram afetados como alvos.[4] As investigações também expuseram a espionagem de juízes, advogados, médicos, líderes sindicais e acadêmicos.[5] A NSO Group, empresa que fabrica e vende o Pegasus, admitiu que seus clientes têm como alvo de 12.000 a 13.000 indivíduos anualmente.[6]

6. O programa espião Pegasus é o exemplo mais proeminente em um cenário crescente de programas espiões comercializados por empresas para governos em todo o mundo.[7] De acordo com pesquisadores, pelo menos 65 governos adquiriram ferramentas comerciais de vigilância de spyware.[8] A NSO informou que conta com 60 agências governamentais em 45 países entre seus clientes. Poucos dias antes das revelações do Pegasus, o Citizen Lab e a Microsoft lançaram um relatório que detalhava como outro programa de computador, o Candiru, havia sido usado por governos para atingir defensores de direitos humanos, dissidentes, jornalistas, ativistas e políticos.[9] Em novembro de 2021, a empresa de rede social Meta anunciou ter desativado sete entidades que tinham como alvo pessoas através da Internet em mais de 100 países. A empresa também alertou cerca de 50.000 pessoas que acreditava terem sido alvo de tais atividades.[10] Relatou-se que mais de 500 empresas desenvolvem, comercializam e vendem essas ferramentas de vigilância para governos.[11]

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

5 Ver 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 Em depoimento perante o Parlamento Europeu, comissão de inquérito para investigar o uso do Pegasus e programas espiões de vigilância equivalentes, 21 de junho de 2022, disponível em https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA.

7 Ver https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepressionReport2022_NEW_0.pdf, p. 29.

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

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

10 Ver https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/. Para outros exemplos, ver 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; e https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

11 A/HRC/41/35, para. 6; ver também https://data.mendeley.com/datasets/csvhpkt8tm/2 para um inventário global de programas espiões comerciais.

7. Os recursos das ferramentas e serviços de spyware oferecidos no mercado global são espantosos. O Pegasus, por exemplo, uma vez instalado, concede acesso completo e irrestrito a todos os sensores e informações dos dispositivos infectados, transformando efetivamente a maioria dos smartphones em dispositivos de vigilância 24 horas, acessando câmera e microfone, dados de geolocalização, e-mails, mensagens, fotos e vídeos, assim como todas as aplicações. Permite ao intruso obter um quadro detalhado da vida das suas vítimas, os seus pensamentos, preferências, atividades profissionais, pensamento político, saúde, situação financeira e vida social e íntima. Enquanto muitas ferramentas de hackeamento exigem alguma ação por parte da vítima, como clicar em um link ou abrir um anexo de uma mensagem, o Pegasus é instalado de forma furtiva, por meio do chamado "ataque de zero clique".[12] O software torna quase impossível que as vítimas evitem a infecção depois de terem sido alvejadas.

8. As operações de hackeamento podem assumir muitas formas, com graus variados de intrusão. Embora obter o controle total de um telefone celular ou computador ajude a traçar um quadro detalhado das vidas dos alvos, diversas outras técnicas de hackeamento podem ser menos intrusivas, embora ainda sejam muito sérias, incluindo obter acesso a contas de e-mail. O hackeamento também pode acessar outros dispositivos conectados, como dispositivos tecnológicos vestíveis ou veículos, que podem fornecer informações adicionais, incluindo dados de saúde e localização. Dispositivos equipados com câmeras ou microfones, como caixas de som ou televisores inteligentes, também podem ser transformados em ferramentas de vigilância audiovisual. Atacar a infraestrutura de provedores de serviços pode abrir o acesso a grandes quantidades de informações sobre milhares de clientes, incluindo suas comunicações, dados de navegação e localizações.[13] A discussão nos parágrafos seguintes concentra-se na invasão de dispositivos de comunicação pessoal.

9. O hackeamento de dispositivos de comunicação pessoal constitui uma grave interferência no direito à privacidade e pode estar relacionado a violações de uma série de outros direitos. Dado que a intrusão nos dispositivos de comunicação digital permite o acesso a rascunhos e históricos de busca e navegação, pode também permitir aprofundamentos sobre os processos de pensamento dos indivíduos sujeitos ao hackeamento, bem como suas visões e crenças políticas e religiosas, interferindo assim nas liberdades de opinião e de pensamento.[14] As operações de hackeamento podem ser experiências profundamente traumáticas, afetando a saúde mental das vítimas e de suas famílias. Há relatos de que o hackeamento teria levado à prisão e detenção de defensores dos direitos humanos e políticos, alguns dos quais teriam sido submetidos a tortura.[15] O hackeamento direcionado também tem sido associado a execuções extrajudiciais.[16]

12 Deve-se notar que o programa de computador Pegasus não é a única ferramenta com esses recursos e que o número de tais ferramentas está crescendo.

13 A investigação EncroChat da polícia na França e na Holanda, que conseguiu invadir a infraestrutura de servidores de uma rede de comunicações criptografadas, coletou informações sobre mais de 32.000 telefones em 121 países; ver Tribunal Federal de Justiça da Alemanha, decisão de 2 de março de 2022, 5 StR 457/21, para. 18.

14 A/HRC/29/32, para. 20. Para uma análise abrangente da liberdade de pensamento, ver A/76/380.

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

16 A/HRC/41/35, para. 1; ver também o documento da sala de conferências do Relator Especial sobre execuções extrajudiciais, sumárias ou arbitrárias, intitulado "Anexo ao relatório do Relator Especial: investigação sobre a morte ilegal do Sr. Jamal Khashoggi". Disponível em https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/.

10. Além disso, atacar jornalistas e meios de comunicação com ferramentas de hackeamento prejudica gravemente a liberdade da mídia, principalmente porque as fontes de informação podem temer a detecção e as repercussões. A mera existência de programas de hackeamento pode ter efeitos inibitórios sobre a liberdade de expressão, sobre o trabalho da mídia e sobre o debate e participação públicos, potencialmente desgastando a governança democrática. Nas palavras da Suprema Corte da Índia, em sua recente decisão sobre o uso do programa de computador Pegasus, o efeito inibitório da vigilância seria um "ataque ao papel vital de fiscalização pública da imprensa".[17]

11. O hackeamento também pode ter um impacto negativo nos direitos ao devido processo legal e ao julgamento justo.[18] Obter acesso a um dispositivo pode permitir que um invasor não apenas observe o conteúdo desse dispositivo e suas interações com outros dispositivos, mas também manipule o dispositivo, inclusive pela alteração, exclusão ou adição de arquivos.[19] Assim, é possível forjar provas para incriminar ou chantagear indivíduos tidos como alvo.[20]

12. Além disso, o programa espião pode afetar não apenas os alvos das operações de hackeamento, mas todos em comunicação com esses indivíduos ou, caso a câmera, o microfone ou a geolocalização do dispositivo sejam ativados, qualquer pessoa presente no mesmo local físico.[21]

13. Finalmente, o hackeamento se baseia e explora a existência de falhas de segurança em sistemas de computador. Ao manter essas vulnerabilidades abertas, ou mesmo criá-las, aqueles que recorrem ao hackeamento podem contribuir para ameaças à segurança e à privacidade de milhões de usuários e do ecossistema mais amplo de informações digitais.[22]

14. Órgãos de direitos humanos e especialistas têm alertado sobre programas espiões por anos. A Assembleia Geral e o Conselho de Direitos Humanos afirmaram repetidamente que os Estados Membros devem abster-se de vigilância ilegal ou arbitrária, inclusive por meio de hackeamento.[23] Vários relatores especiais expressaram fortes críticas às práticas de hackeamento que vão muito além do necessário para perseguir objetivos legítimos, como o combate ao terrorismo e ao crime.[24] O Comitê de Direitos Humanos também expressou suas preocupações sobre hackeamento patrocinado pelo Estado, em particular quando empregado sem a supervisão adequada ou as salvaguardas adequadas.[25] No nível regional, o ex-Relator Especial para a liberdade de expressão da Comissão Interamericana de Direitos Humanos condenou as operações de hackeamento para fins inadmissíveis

17 Suprema Corte da Índia, *Manohar Lal Sharma v. União da Índia*, despacho de 27 de outubro de 2021, para. 39.

18 A/HRC/23/40, para. 62.

19 A/HRC/39/29, para. 19.

20 Ver https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/ para um exemplo de tais alegações.

21 Ver https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

22 A/HRC/39/29, para. 19.

23 Resolução 75/176 da Assembleia Geral e Resoluções 48/4 e 45/18 do Conselho de Direitos Humanos.

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

25 Ver CCPR/C/DEU/CO/7; CCPR/C/NLD/CO/5; e CCPR/C/ITA/CO/6.

e pediu punições severas aos infratores, inclusive por ações tomadas por motivações políticas contra jornalistas e a mídia independente.[26]

15. Reagindo às revelações sobre o uso do programa de computador Pegasus, várias instituições regionais e nacionais, incluindo o Conselho da Europa, a Comissão Interamericana de Direitos Humanos, o Parlamento Europeu e a Suprema Corte da Índia, expressaram preocupação com a proliferação de programas espiões e iniciaram audiências e investigações.[27] Investigações criminais[28] e ações civis[29] também estão em andamento.

16. A orientação sobre os requisitos mínimos e as proteções necessárias para qualquer uso governamental de programas espiões pode se basear em um extenso corpo existente de análises de direitos humanos relacionadas à vigilância.[30] Os impactos adversos de longo alcance do hackeamento exigem uma abordagem particularmente cautelosa de seu uso, limitando-o às circunstâncias mais excepcionais, em estrita observância aos requisitos do direito internacional dos direitos humanos.

17. No entanto, muitas jurisdições não estabeleceram essas proteções legais essenciais e não possuem leis claras, precisas e publicamente disponíveis que regulem as operações de hackeamento. Enquanto alguns Estados promulgaram estruturas legais que cumpririam com a lei internacional de direitos humanos, outros contam com leis excessivamente amplas ou desatualizadas, promulgadas antes do advento das tecnologias modernas.

18. Como as revelações sobre o programa de computador Pegasus e relatórios relacionados mostraram, hackeamento por vários atores estatais muitas vezes parecem perseguir objetivos que não são legítimos sob a lei internacional de direitos humanos. Embora, em certas circunstâncias, medidas de vigilância intrusivas possam ser permitidas de acordo com os artigos 17 e 19 do Pacto Internacional sobre Direitos Civis e Políticos com base na proteção da segurança nacional ou da ordem pública, o hackeamento nunca pode ser justificado por razões políticas ou comerciais, o que é frequentemente o caso quando os defensores dos direitos humanos ou jornalistas são tidos como alvos.

---

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

27 Ver https://www.oas.org/en/iachr/expression/showarticle.asp?artID=998&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; e Suprema Corte da Índia, *Manohar Lal Sharma v. União da Índia*, ordem judicial de 27 de outubro de 2021.

28 Ver https://www.euronews.com/next/2021/07/20/paris-prosecutor-to-investigate-alleged-pegasus-hacking-after-complaint-by-french-journali; e 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/; https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf. Para um amplo panorama das ações legais tomadas, ver https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/.

30 Ver A/HRC/27/37; A/HRC/39/29; A/HRC/23/40 e 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; e CCPR/C/FIN/CO/7.

19. Mesmo que objetivos legítimos estejam sendo perseguidos, como objetivos de segurança nacional ou a proteção dos direitos de terceiros, a avaliação de necessidade e proporcionalidade do uso de programas espiões limita severamente os cenários em que programas espiões seriam permitidos.[31] Há fortes argumentos de que ferramentas como o Pegasus, que permitem intromissões irrestritas na vida das pessoas e podem até mesmo atingir seus pensamentos íntimos, poderiam afetar a essência do direito à privacidade[32] e interferir nos direitos absolutos à liberdade de pensamento e opinião. Dados os impactos adversos substanciais do uso de programas espiões e seu alcance muito além de qualquer alvo pretendido, seu uso deve ser limitado aos casos em que serviriam para prevenir ou investigar um crime grave específico ou ato que represente uma grave ameaça à segurança nacional. Seu uso deve ser estritamente direcionado a uma investigação da pessoa ou pessoas suspeitas de cometer ou ter cometido tais atos. Este deve ser o último recurso, ou seja, todas as medidas menos intrusivas devem ter sido esgotadas ou ter se mostrado inúteis, e devem ser estritamente limitadas em escopo e duração. Somente dados relevantes devem ser acessados e coletados.[33] As medidas também devem estar sujeitas a uma supervisão independente rigorosa; a aprovação prévia por um órgão judicial é essencial.[34] Além disso, controles de exportação robustos e transparentes que considerem explicitamente os riscos de direitos humanos podem ser uma ferramenta poderosa para prevenir violações e abusos de direitos.[35] O ACNUDH reitera seu recente apelo, bem como os de especialistas e grupos de direitos humanos, por uma moratória sobre a venda, transferência e uso de ferramentas de hackeamento até que um regime de salvaguardas baseado em direitos humanos esteja em vigência.[36]

B. Restrições à criptografia

20. Nos últimos anos, vários governos tomaram medidas que, intencionalmente ou não, correm o risco de minar a segurança e a confidencialidade das comunicações criptografadas. Isso tem implicações preocupantes para o gozo do direito à privacidade e outros direitos humanos.

21. A criptografia é um viabilizador fundamental da privacidade e segurança online, e é essencial para salvaguardar os direitos, incluindo os direitos a liberdade de opinião e de expressão, liberdade de associação e reunião pacífica, segurança, saúde e não discriminação. A criptografia garante que as pessoas possam compartilhar informações livremente, sem medo de que suas informações possam ser conhecidas por terceiros, sejam eles autoridades do Estado ou cibercriminosos. A criptografia é essencial para

31 Ver Tribunal Constitucional Federal da Alemanha, acórdão de 27 de fevereiro de 2008 (1 BvR 370, 595/07), 247 (aa).

32 Autoridade Europeia para a Proteção de Dados, ver https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, p. 8.

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

34 Ver A/HRC/39/29 sobre as salvaguardas mínimas para medidas de vigilância secreta.

35 A/HRC/39/29, para. 25; A/HRC/44/24, para. 40; A/HRC/48/31, para. 46; e A/HRC/41/35, paras. 34 e 66. A União Européia recentemente deu um passo em direção a considerações mais fortes de direitos humanos ao adotar um novo regulamento de controle de exportação.

36 Ver 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/; e https://cyberpeaceinstitute.org/news/renewed-call-moratorium-spyware/.

que as pessoas se sintam seguras ao trocar informações livremente com outras sobre uma série de experiências, pensamentos e identidades, incluindo dados sensíveis de saúde ou financeiros, conhecimento sobre identidades de gênero e orientação sexual, expressão artística e informações relacionadas ao status de minoria. Em ambientes de censura predominante, a criptografia permite que indivíduos mantenham um espaço para manter, expressar e trocar opiniões com outras pessoas. Em casos específicos, jornalistas e defensores de direitos humanos não podem fazer seu trabalho sem a proteção de criptografia robusta, amparando suas fontes e abrigando-as dos poderosos atores sob investigação. A criptografia oferece às mulheres, que enfrentam ameaças específicas de vigilância, assédio e violência online, um nível importante de proteção contra a divulgação involuntária de informações.[37] Em conflitos armados, as mensagens criptografadas são indispensáveis para garantir a comunicação segura entre civis. É notável que nos dois meses após o início do conflito armado na Ucrânia em 24 de fevereiro de 2022, o número de downloads na Ucrânia do aplicativo de mensagens criptografadas Signal aumentou mais de 1.000% em comparação com os meses anteriores.[38]

22. O papel vital da criptografia como viabilizador da privacidade e dos direitos humanos tem sido amplamente reconhecido, inclusive pelos Estados, órgãos das Nações Unidas, o Alto Comissariado das Nações Unidas para os Direitos Humanos e especialistas em direitos humanos.[39] A Assembleia Geral e o Conselho de Direitos Humanos também destacou a importância da criptografia na salvaguarda dos direitos humanos em várias resoluções, instando os Estados a se absterem de interferir nas tecnologias de criptografia[40] e incentivando as empresas a trabalharem para viabilizar soluções que garantam e protejam a confidencialidade das comunicações e transações digitais, incluindo medidas para criptografia, pseudonimização e anonimato.[41] Relatores especiais e especialistas regionais expressaram apoio à criptografia forte como viabilizadora de direitos, recomendando a promoção e proteção da criptografia forte e alertando contra medidas que restringiriam arbitrária ou ilegalmente o uso dessa tecnologia-chave.[42] O Comitê dos Direitos da Criança sublinhou que quaisquer medidas para detectar exploração sexual infantil e material de abuso em comunicações criptografadas devem ser estritamente limitadas de acordo com os princípios de legalidade, necessidade e proporcionalidade.[43] O Conselho de Direitos Humanos, as Nações Unidas e especialistas regionais em direitos humanos salientaram que a criptografia é vital para o trabalho jornalístico e a proteção de fontes.[44] Os Indicadores de Universalidade da Internet emitidos pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura ressaltam a importância da criptografia para a confiança e a segurança online.[45]

37 A/HRC/35/9, para. 18.

38 Ver https://sensortower.com/blog/signal-telegram-ukraine-russia-2022.

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

40 Resolução da Assembléia Geral 75/176 e resoluções do Conselho de Direitos Humanos 39/6, 44/12, 45/18 e 48/4.

41 Resolução 75/176 da Assembleia Geral e resolução 48/4 do Conselho de Direitos Humanos.

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

43 Comitê dos Direitos da Criança, comentário geral nº 25 (2021) sobre os direitos da criança em relação ao ambiente digital, para. 70.

44 Resolução 45/18 do Conselho de Direitos Humanos; A/HRC/29/32; e https://www.osce.org/representative-on-freedom-of-media/379351.

45 Ver https://en.unesco.org/internet-universality-indicators, indicador D.5.

23. Apesar de seus benefícios, os governos às vezes restringem o uso de criptografia, por exemplo, para proteção da segurança nacional e combate ao crime, em particular para detectar material de abuso sexual infantil. As restrições incluem a proibição de comunicações criptografadas e a criminalização por oferecer ou usar ferramentas de criptografia[46] ou registro e licenciamento obrigatórios de ferramentas de criptografia.[47] De igual modo, em alguns casos, provedores de criptografia têm sido obrigados a garantir que as autoridades policiais e outras autoridades estatais tenham acesso a todas as comunicações mediante solicitação, o que pode efetivamente equivaler a uma restrição geral de criptografia que pode exigir, ou pelo menos incentivar, a criação de algum tipo de porta clandestina (um caminho embutido para contornar a criptografia, permitindo acesso secreto a dados em texto simples).[48] Outra forma de interferência na criptografia é a exigência de que sistemas de depósito de chaves sejam criados e mantidos, e que todas as chaves privadas necessárias para descriptografar dados sejam entregues ao Governo ou a um terceiro designado.[49] A imposição de requisitos de rastreabilidade, segundo os quais os provedores precisam ser capazes de rastrear qualquer mensagem até seu suposto remetente, também pode exigir o enfraquecimento dos padrões de criptografia.[50] Recentemente, vários Estados começaram a impor ou a considerar obrigações gerais de monitoramento para provedores de comunicações digitais, incluindo aquelas que oferecem serviços de comunicações criptografadas.[51] Tais obrigações podem efetivamente forçar esses provedores a abandonar a criptografia forte de ponta a ponta ou a identificar soluções altamente problemáticas (ver os parágrafos 27-28 abaixo).

24. Não há dúvida de que os recursos de criptografia amplamente utilizados, recursos que o público exigiu como uma resposta à vigilância em massa e ao cibercrime, criam um dilema para os governos que buscam proteger as populações, em particular seus integrantes mais vulneráveis, contra crimes graves e ameaças à segurança. No entanto, conforme apontado pelo Relator Especial sobre a promoção e proteção do direito à liberdade de opinião e expressão, a regulamentação da criptografia corre o risco de minar os direitos humanos.[52] Os governos que buscam limitar a criptografia muitas vezes falharam em mostrar que as restrições que imporiam são necessárias para atender a um interesse legítimo específico, dada a disponibilidade de várias outras ferramentas e abordagens que fornecem as informações necessárias para aplicação específica da lei ou outros fins legítimos.[53] Essas medidas alternativas incluem policiamento tradicional aprimorado e com melhores recursos, operações secretas, análise de metadados e cooperação policial internacional reforçada.

46 Ver PSE 2/2017 e LBY 3/2022. Todas as comunicações mencionadas no presente relatório estão disponíveis em https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

47 Ver https://hrsly.com/wp-content/uploads/2022/06/OL-LBY-3.2022-DownLoadPublicCommunicationFile.pdf.

48 Ver GBR 4/2015, MYS 2/2018, AUS 5/2018 e AUS 6/2018.

49 Ver RUS 7/2016 e RUS 7/2018.

50 Ver IND 31/2018, IND 3/2019, BRA 6/2020 e BRA 7/2020.

51 Por exemplo, a Lei "EARN IT" adotada nos Estados Unidos da América em 2020 (ver USA 4/2020); o projeto de lei de segurança online no Reino Unido (ver GBR 5/2022); a proposta da Comissão Europeia de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual infantil, de 11 de maio de 2022 (COM (2022) 209); e do Governo da Índia, as Regras de Tecnologia da Informação (Diretrizes Intermediárias e Código de Ética de Mídia Digital), de 2021 (ver IND 8/2021).

52 Ver A/HRC/29/32.

53 Ibid., para. 39.

25. Além disso, o impacto da maioria das restrições de criptografia sobre o direito à privacidade e os direitos associados são desproporcionais, muitas vezes afetando não apenas os indivíduos tidos como alvo, mas a população em geral. Proibições definitivas por parte dos governos, ou a criminalização da criptografia em particular, não podem ser justificadas, pois impediriam que todos os usuários em suas jurisdições tivessem uma maneira segura de se comunicar. Sistemas de depósito de chaves têm vulnerabilidades significativas, pois dependem da integridade da instalação de armazenamento e expõem as chaves armazenadas a ataques cibernéticos. Além disso, portas clandestinas obrigatórias em ferramentas de criptografia criam responsabilidades que vão muito além de sua utilidade em relação a usuários específicos identificados como suspeitos de crimes ou ameaças à segurança. Elas comprometem a privacidade e segurança de todos usuários e os expõem a interferências ilegais, não apenas de Estados, mas também de atores não estatais, incluindo redes criminosas.[54] Os requisitos de licenciamento e registro têm efeitos desproporcionais semelhantes, pois exigem que o *softwares* de criptografia contenha pontos fracos.[55] Tais efeitos adversos não estão necessariamente limitados à jurisdição que impõe a restrição; em vez disso, é provável que portas clandestinas, uma vez estabelecidas na jurisdição de um Estado, tornem-se parte do programa de computador utilizado em outras partes do mundo.

26. Recentemente, o conceito da chamada varredura do lado do cliente para detectar certas formas de conteúdo censurável foi proposto para evitar muitos dos problemas descritos acima. A varredura do lado do cliente move a etapa de detecção de conteúdo dos servidores por meio dos quais as comunicações são enviadas para os próprios dispositivos pessoais. Dessa forma, o conteúdo em questão é examinado antes de ser criptografado para transporte. Em agosto de 2021, a Apple anunciou planos para introduzir tal sistema para seus serviços iMessage e iCloud, mas suspendeu a implementação da mudança proposta após fortes críticas de uma ampla gama de especialistas em segurança de tecnologia da informação, criptógrafos e grupos de direitos humanos.[56] No entanto, várias tentativas legislativas[57] podem, pelo menos indiretamente, obrigar os serviços de comunicação da Internet a implementar tais sistemas, impondo amplas obrigações de monitoramento para todas as comunicações, incluindo aquelas que são criptografadas. Se o conteúdo das mensagens, uma vez criptografado, não pode ser acessado por ninguém, exceto o remetente e o destinatário, qualquer obrigação geral de monitoramento forçaria os provedores de serviços ou a abandonar a criptografia de transporte, ou a buscarem o acesso às mensagens antes de elas serem criptografadas.

27. A imposição de uma varredura pelo lado do cliente generalizada constituiria uma mudança de paradigma que levanta uma hoste de problemas sérios com consequências potencialmente terríveis para o gozo do direito à privacidade e outros direitos. Diferente de outras intervenções, a exigência de varredura pelo lado do cliente generalizada afetaria inevitavelmente todos os que usam meios modernos de comunicação, não apenas as pessoas envolvidas em crimes e ameaças graves à segurança. A varredura obrigatória pelo lado do cliente altera a capacidade das pessoas de controlar totalmente os dispositivos de comunicação que estão intrinsecamente conectados a todas as facetas de suas

54 A/HRC/39/29, para. 20.

55 A/HRC/29/32, para. 41.

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

57 Comissão Europeia, proposta de regulamento do Parlamento Europeu e do Conselho que estabelece regras para prevenir e combater o abuso sexual infantil, de 11 de maio de 2022 (COM (2022) 209); ver também o projeto de lei de segurança online no Reino Unido da Grã-Bretanha e Irlanda do Norte, disponível em https://www.gov.uk/government/publications/draft-online-safety-bill.

vidas e a limitar quais informações esses dispositivos compartilham.[58] Além disso, na varredura generalizada de comunicações, falsos positivos frequentes não podem ser evitados, mesmo que as taxas de precisão sejam altas, implicando assim numerosos indivíduos inocentes.[59] Dada a possibilidade de tais impactos, é provável que a vigilância indiscriminada tenha um efeito inibitório significativo sobre a liberdade de expressão e de associação, com as pessoas limitando as formas pelas quais elas se comunicam e interagem com outras, e praticando autocensura.[60]

28. A varredura pelo lado do cliente também abre novos desafios de segurança, tornando mais prováveis as brechas de segurança.[61] O processo de triagem também pode ser manipulado, tornando possível criar artificialmente perfis falsos positivos ou falsos negativos.[62] Mesmo se, para os propósitos atuais, a triagem pelo lado do cliente ocorra estritamente sob medida, é provável que abrir os dispositivos para a triagem determinada pelo governo leve a futuras tentativas de ampliar o escopo do conteúdo que é alvo de tais medidas.[63] Em particular, onde o estado de direito for fraco e os direitos humanos estejam ameaçados, o impacto da triagem do lado do cliente pode ser muito mais amplo, por exemplo, poderia ser usado para suprimir o debate político ou para atingir figuras da oposição, jornalistas e defensores dos direitos humanos.[64] Dada a ampla gama de riscos significativos para a proteção dos direitos humanos a partir da triagem pelo lado do cliente generalizada obrigatória, tais requisitos não devem ser impostos sem uma consideração mais substancial de seus possíveis impactos sobre os direitos humanos, e medidas que mitiguem esses danos. Sem investigação e análise aprofundadas, parece improvável que tais restrições possam ser consideradas proporcionais sob o direito internacional dos direitos humanos, mesmo quando impostas em busca de objetivos legítimos, dada a gravidade de suas possíveis consequências.[65]

58 Submissões do Comitê Gestor da Coalizão Global da Criptografia e da Privacy International.

59 Ver https://doi.org/10.48550/arXiv.2110.07450.

60 Para mais informações sobre os efeitos inibitórios da vigilância, ver o para. 47 abaixo

61 Comparado aos ataques a servidores corporativos, os ataques a dispositivos pessoais podem ser executados por mais atores e em infraestruturas menos seguras. Os adversários podem usar seu acesso ao dispositivo para fazer engenharia reversa do mecanismo de varredura, ver https://doi.org/10.48550/arXiv.2110.07450.

62 https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha; e 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; e https://doi.org/10.48550/arXiv.2110.07450.

64 Ibidem.

65 A/HRC/39/29, para. 20, e A/HRC/29/32, para. 43. Os entendimentos do Tribunal de Justiça da União Europeia corroboram esta conclusão. O Tribunal decidiu recentemente que a análise automatizada de dados de tráfego e localização de forma geral e indiscriminada deve ser limitada ao estritamente necessário para responder a uma ameaça grave, genuína, presente ou previsível à segurança nacional. O Tribunal rejeitou qualquer outra justificativa. Ver *La Quadrature du Net and Others v. Premier ministre and others*, acórdão de 6 de outubro de 2020 (processos apensos C-511/18, C-512/18 e C-520/18), para. 177. Além disso, sua jurisprudência indica um ceticismo ainda mais forte em relação à triagem de dados de conteúdo, Tribunal de Justiça da União Europeia, *Maximillan Schrems v. Data Protection Commissioner*, acórdão de 6 de outubro de 2015 (C-362/14), para. 94.

III. Vigilância do público

29. O Alto Comissariado levantou preocupações sobre vigilância em massa em várias ocasiões, em particular em termos de interceptação em massa de comunicações.[66] Enquanto alguns Estados melhoraram as salvaguardas contra a vigilância, a prática profundamente perturbadora de vigilância das atividades online de grandes proporções da população, ou mesmo de populações inteiras, não cessou. Embora os relatórios anteriores tenham se concentrado principalmente na vigilância de comunicações privadas, eles abordaram menos as implicações de privacidade do monitoramento de locais públicos, o qual é discutido abaixo.

A. Vigilância de lugares públicos

30. Câmeras de vigilância, implantadas para monitorar vias públicas, estacionamentos, centros de transporte e outros locais públicos, tornaram-se comuns em muitos países. Esperava-se que o número de câmeras de vigilância em uso globalmente ultrapassasse um bilhão em 2021.[67] As 10 cidades do mundo com a maior densidade de vigilância por vídeo operam entre cerca de 39 a mais de 115 câmeras de vigilância por 1.000 habitantes.[68]

31. Além dos sistemas de vigilância operados pelo Estado, algumas empresas têm ferramentas de vigilância integradas para uso privado, com recursos dedicados para relatar incidentes às autoridades ou até mesmo conceder a elas o acesso direto a seus fluxos de dados.[69] Isso expande muito o espaço público sob vigilância, enquanto mina a transparência, a supervisão e a responsabilização.

32. Nos últimos anos, as ferramentas disponíveis das câmeras de vigilância aumentaram drasticamente como resultado da adição de capacidades sofisticadas de análise de vídeo. Estima-se que em 2010 menos de 2% das câmeras de rede vendidas apresentavam análise de vídeo incorporada, mas essa proporção cresceu para mais de 40% em 2016 e provavelmente continuará a crescer.[70] Os recursos analíticos dependem cada vez mais da inteligência artificial. Capacidades adicionais para realizar reconhecimento facial e identificar comportamentos como suspeitos estão entre as características mais problemáticas de sistemas sofisticados de vigilância por vídeo.[71] Além disso, o uso de drones para propósitos de vigilância foi normalizado em muitos países, onde são usados para monitorar protestos e outras reuniões.[72]

33. Sob o termo guarda-chuva "cidades inteligentes", um número crescente de iniciativas baseadas em dados está em andamento para remodelar os espaços urbanos. Os projetos de cidades inteligentes se concentram na coleta e processamento de dados para informar

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

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

68 Ver https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/; e https://surfshark.com/surveillance-cities.

69 Ver https://www.accessnow.org/amazon-ring-privacy-review/.

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

71 Ver submissão da Derechos Digitales e Rede Internacional de Organizações das Liberdades Civis – INCLO.

72 Ver submissão da Anistia Internacional e CIVICUS.

o gerenciamento das instalações da cidade, viabilizados por tecnologias de sensores cada vez mais capazes. Embora muitos dos dados coletados e processados nesses contextos sejam relacionados a questões como dados sobre fluxos de tráfego, poluição ou ruído desvinculados dos dados pessoais, outros dados coletados podem ser facilmente vinculados a indivíduos, como placas de veículos e dados de medidores inteligentes. Além disso, dados aparentemente anônimos muitas vezes podem ser deanonimizados,[73] e a infraestrutura, como câmeras instaladas para monitorar fluxos de dados de tráfego, pode ser reaproveitada para rastrear indivíduos.[74]

34. Esses desenvolvimentos geralmente ocorrem em um contexto de novos sistemas de identidade e bancos de dados biométricos ampliados. Em vários países, os sistemas de identidade estão vinculados a um amplo armazenamento central de dados pessoais, incluindo informações biométricas, como impressões digitais, geometria facial, varreduras de íris e DNA. Além disso, as bases de dados são frequentemente interligadas e disponibilizadas para busca por outras agências. Como consequência, identificar indivíduos onde quer que eles estejam se tornou cada vez mais fácil.

B. Monitoramento online

35. Paralelamente, o monitoramento do discurso público online tornou-se generalizado. Globalmente, muitas autoridades estão coletando e analisando postagens de mídia social, e redes privadas e profissionais construídas em plataformas de comunicação acessíveis ao público. Essa inteligência de mídia social varia desde a investigação de usuários específicos até a coleta, armazenamento e análise de grandes quantidades de dados. Os dados obtidos podem incluir: nomes; idades; fotos e modelos digitais relacionados; endereços; postagens e reações às postagens de outras pessoas; contatos sociais e profissionais e redes associadas; dados de localização; interesses; orientação sexual; identificação de gênero; filiação e atividades políticas; crenças religiosas; e informações de saúde.

36. Muitas vezes, vários tipos de análise preditiva fazem parte das práticas de inteligência de mídia social, incluindo tentativas de identificar possíveis focos de crime. No entanto, essa análise também pode ser usada para avaliar o comportamento passado, presente e futuro de indivíduos e atribuir pontuações de risco relacionadas à probabilidade de se tornarem infratores ou ameaças à segurança.[75] A inteligência de mídia social também é usada para prever a possibilidade de agitação.[76]

37. Essas atividades podem servir a vários objetivos legítimos e ilegítimos, desde a investigação e prevenção de crimes até a verificação de candidatos a benefícios sociais, monitoramento de protestos, medição do sentimento público e perfil da conduta social das pessoas.[77]

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

74 Para saber mais sobre os impactos das cidades inteligentes nos direitos humanos, ver https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/; e https://carrcenter.hks.harvard.edu/files/cchr/files/CCDP_006.pdf.

75 Ver https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/, p. 152.

76 Ver https://dx.doi.org/10.2139/ssrn.2702426, p. 1.

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

C. Impactos nos direitos humanos

38. As modernas tecnologias baseadas em dados estão mudando drasticamente o equilíbrio de poder entre a entidade que realiza a vigilância e as pessoas que estão sendo monitoradas. Antes do advento da vigilância automatizada em grande escala e das ferramentas de análise de dados, havia limitações práticas à vigilância que forneciam um certo nível de proteção para os indivíduos, mesmo quando em público.[78] Ferramentas digitais sofisticadas tornam essas proteções "naturais" discutíveis. Hoje, um único funcionário pode monitorar as contas de mídia social de dezenas de pessoas e, com a ajuda de avançados programas de computador e análise de *big data*, pequenas equipes podem observar e perfilar milhares de contas.[79]

39. Desenvolvimentos semelhantes aumentam a eficácia e o alcance de outras medidas de vigilância de espaços públicos. Por exemplo, o surgimento da tecnologia de reconhecimento facial juntamente com outras tecnologias de reconhecimento biométrico transformou fundamentalmente as práticas tradicionais de monitoramento audiovisual, pois aumentou drasticamente a capacidade de identificar indivíduos em espaços públicos, incluindo participantes de reuniões. A tecnologia de reconhecimento facial ao vivo permite a identificação em tempo real de indivíduos, bem como sua vigilância e rastreamento direcionados. A identificação retrospectiva de pessoas pode talvez ampliar a variedade de fontes de dados, levando a impactos que podem ser igualmente intrusivos[80] se não forem implantados com a máxima contenção.

40. O impacto da vigilância pública sobre os direitos humanos é ainda mais agravado porque as fontes de dados são cada vez mais mescladas, por exemplo, combinando *feeds* de videovigilância equipados de reconhecimento facial com dados de mídia social[81] e bancos de dados governamentais, incluindo informações sobre previdência social, migração, suspeitos de terrorismo, prisões ou mesmo listas de indivíduos sinalizados por motivos políticos.

41. Além disso, os Estados contam com vastas coletas de dados acumuladas por uma variedade de empresas privadas. Em relatórios anteriores, o Alto Comissariado e os relatores especiais destacaram a questão dos governos solicitarem acesso a dados coletados por provedores de serviços de telecomunicações e Internet, muitas vezes no contexto de leis de retenção de dados obrigatória.[82] A gama de empresas que recebem tais solicitações está crescendo de forma constante. Alguns Estados obrigam as empresas a dar-lhes acesso direto aos fluxos de dados que passam por suas redes. Esses sistemas de acesso direto são motivo de séria preocupação, pois são particularmente propensos a abusos e tendem a contornar as principais garantias processuais.[83]

42. Além disso, os Estados dependem cada vez mais de serviços de vigilância oferecidos por empresas comerciais, por exemplo, adquirindo dados de corretores de dados e outras

78 A/HRC/44/24, para. 34.
79 Ver https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media.
80 Ver submissão da Anistia Internacional.
81 Ver submissão da INCLO.
82 A/HRC/27/37, para. 26; A/HRC/39/29, para. 18; A/HRC/23/40 e A/HRC/23/40/Corr.1, paras. 65–67; e A/69/397, paras. 53–55.
83 A/HRC/39/29, para. 19.

empresas que coletam e vendem dados pessoais.[84] Tais práticas podem contornar restrições e garantias processuais cruciais, permitindo que os Estados acessem indiretamente ferramentas que eles mesmos não poderiam ter implantado sem violar suas obrigações de direitos humanos. Por exemplo, a ferramenta de reconhecimento facial desenvolvida pela empresa Clearview AI tem sido usada por milhares de agências de aplicação da lei, apesar de ter sido construída pela raspagem de fotos de bilhões de pessoas da Internet, uma invasão massiva dos direitos de privacidade.[85]

43. A vigilância sistemática de pessoas no espaço público online e offline, em particular quando combinada com formas adicionais de análise e conexão das informações obtidas com outras fontes de dados, constitui uma interferência no direito à privacidade e pode ter efeitos altamente prejudiciais no gozo de outros direitos humanos.[86] Pode constituir uma ameaça à liberdade de expressão e de reunião pacífica, de participação e à democracia e, portanto, deve ser abordada com a máxima cautela e apenas em estrita observância dos requisitos de direitos humanos. Este é o caso mesmo que as atividades monitoradas estejam ocorrendo em público, ou em plataformas de mídia social abertas, pois os indivíduos devem ter um espaço sem observação e intrusão sistemáticas, em particular por entidades governamentais. Conforme observado anteriormente pelo Alto Comissariado, a proteção do direito à privacidade se estende a espaços públicos e informações publicamente disponíveis.[87] O Comitê de Direitos Humanos rejeitou a noção de que os dados coletados em áreas públicas são automaticamente de domínio público e podem ser acessados livremente.[88] O Tribunal Europeu de Direitos Humanos reconheceu que informações publicamente disponíveis ou perceptíveis podem ser abrangidas pelo direito à privacidade, em particular quando os dados pessoais são registrados de forma sistemática ou permanente.[89]

44. Uma preocupação particular na vigilância pública diz respeito à gravação de imagens fotográficas. As imagens das pessoas incorporam atributos-chave de sua personalidade e revelam características únicas que as distinguem de outras pessoas. Gravar, analisar e

84 Ver, por exemplo, https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances; e https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf, p. 25.

85 Várias autoridades de proteção de dados, determinando que a Clearview AI violou a lei de proteção de dados, impuseram multas pesadas e/ou ordenaram o apagamento dos dados pessoais obtidos, ver https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/; ver também 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; e https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. As autoridades de proteção de dados consideraram que as forças policiais, ao usarem a ferramenta, violaram a lei de proteção de dados, ver https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en; e https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

86 Ver CCPR/C/NGA/CO/2, em que o Comitê de Direitos Humanos expressou preocupação com o monitoramento de mídias sociais, para. 40.

87 A/HRC/39/29, para. 6.

88 CCPR/C/COL/CO/7, para. 32.

89 Ver Tribunal Europeu de Direitos Humanos, *Rotaru v. Romênia*, para. 43, acórdão de 4 de maio de 2000; *Peck v. the United Kingdom*, sentença de 28 de janeiro de 2003, para. 59; *Perry v. the United Kingdom*, acórdão de 17 de julho de 2003, para. 38; e *Vukota-Bojić v. Switzerland*, acórdão de 18 de janeiro de 2017, para. 55.

reter imagens faciais de indivíduos sem o seu consentimento constitui uma interferência no seu direito à privacidade. Ao implantar a tecnologia de reconhecimento facial em espaços públicos, que exige a coleta e processamento de imagens faciais de todas as pessoas capturadas na câmera, tal interferência está ocorrendo em escala massiva e indiscriminada.[90]

45. Além disso, as medidas de vigilância pública podem levar, e muitas vezes são, a base de medidas que afetam diretamente indivíduos e comunidades, incluindo medidas coercitivas. Tais medidas incluem o aumento do monitoramento e policiamento de certos bairros, grupos ou indivíduos, às vezes levando ao interrogatório, prisão e detenção de indivíduos. Alguns grupos e indivíduos também podem ser sinalizados como ameaças ou riscos potenciais, por exemplo, como potenciais terroristas ou criminosos, muitas vezes sem uma base sólida de fatos. Vários governos usam os resultados de uma variedade de medidas de vigilância pública para identificar seus críticos ou pessoas que não estão em conformidade com as expectativas sociais, o que pode levar a assédio, detenção ou negação de serviços essenciais.[91]

46. As operações de vigilância tendem a atingir desproporcionalmente as minorias e as comunidades marginalizadas.[92] O uso de inteligência artificial corre o risco de perpetuar esses padrões de discriminação,[93] incluindo o uso de tecnologias de reconhecimento facial para perfilamento racial e étnico.[94] Os sistemas preditivos de policiamento e administração da justiça demonstraram afetar desproporcionalmente as minorias.[95]

47. Além disso, a vigilância tem efeitos consideráveis sobre como as pessoas exercem seus direitos, em particular os direitos à liberdade de expressão e de reunião pacífica.[96] Vários estudos ilustram a extensão de tais efeitos. Uma pesquisa de 2015 revelou que 25% dos participantes que estavam cientes do caso de Edward Snowden mudaram seu uso

90 A/HRC/44/24, para. 33.

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

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

93 Ver o documento de sala de conferências do Alto Comissariado sobre a promoção e proteção dos direitos humanos e liberdades fundamentais dos africanos e dos afrodescendentes contra o uso excessivo da força e outras violações dos direitos humanos por agentes da lei, paras. 93 e 94. Disponível em https://www.ohchr.org/en/hr-bodies/hrc/regular-sessions/session47/list-reports.

94 A/HRC/41/35, para. 12, e A/HRC/44/57, para. 39.

95 Comitê para a Eliminação da Discriminação Racial, recomendação geral nº 36 (2020) sobre prevenção e combate à discriminação racial por agentes da lei, pars. 33–34; A/HRC/44/57, para. 43; documento de sala de conferências do Alto Comissariado sobre a promoção e proteção dos direitos humanos e liberdades fundamentais dos africanos e dos afrodescendentes contra o uso excessivo da força e outras violações dos direitos humanos por agentes da lei, para. 93; A/HRC/48/31, para. 24; 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; e 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, para. 20; ver, em relação aos protestos: A/HRC/44/24, pars. 29, 35 e 52; Tribunal Europeu de Direitos Humanos, *Big Brother Watch and Others v. the United Kingdom*, sentença de 25 de maio de 2021 (58170/13, 62322/14 e 24960/15), para. 495; http://dx.doi.org/10.15779/Z38SS13; https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; e https://pen.org/research-resources/global-chilling/.

de várias plataformas de tecnologia.[97] Outro estudo descobriu que entre 34% e 61% dos escritores (dependendo do país em questão) evitaram ou pelo menos consideraram evitar certos tópicos em seu trabalho devido ao medo da vigilância do governo.[98] Em uma pesquisa realizada pelo Conselho Norueguês de Tecnologia, 39% dos entrevistados afirmaram que evitariam usar palavras e frases monitoradas pela polícia.[99] Conforme apontado anteriormente pelo Alto Comissariado, esses efeitos ibitórios se estendem a reuniões, incluindo protestos pacíficos.[100]

D. Requisitos de direitos humanos

48. A vigilância pública, sem dúvida, acarreta riscos substanciais aos direitos humanos e pode minar substancialmente o direito à privacidade. Portanto, é essencial que os Estados que recorrem ao uso da vigilância pública avaliem os potenciais impactos de suas ações sobre os direitos humanos e assegurem rigorosamente o cumprimento do direito internacional dos direitos humanos, que exige que qualquer interferência ou restrição seja baseada na lei, necessária para alcançar um legítimo objetivo, e proporcional. As atuais medidas de vigilância pública muitas vezes não atendem a esses requisitos.

49. Legalidade: apesar dos impactos de longo alcance das várias formas de vigilância pública, em muitos países faltam estruturas legais aplicáveis adequadas. As leis de proteção de dados são muitas vezes inexistentes, inadequadas ou abrem amplas exceções para a aplicação da lei e os serviços de inteligência.[101] Além disso, muitas vezes, as leis gerais de privacidade de dados não fornecem orientações detalhadas ou garantem limitações adequadas ao uso de ferramentas de vigilância específicas. A este respeito, são necessários instrumentos jurídicos específicos, em particular para a vigilância feita no contexto da aplicação da lei e da segurança nacional.[102] As leis e regulamentos precisam ter limitações estritas e claramente determinadas sobre o acesso e a fusão de bancos de dados governamentais. Infelizmente, há poucos sinais de que os Estados estão caminhando para regular o uso de técnicas, tecnologias e ferramentas de inteligência de mídia social. Embora existam esforços crescentes de reguladores e legisladores em nível local, nacional e regional para regular o reconhecimento facial e outras ferramentas de vigilância biométrica,[103] a maioria das autoridades continua a operar sistemas de vigilância biométrica, apesar da falta de base legal para tal atividade.

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

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

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

100 A/HRC/44/24, paras. 35 e 53.

101 A/HRC/39/29, para. 34.

102 Os requisitos mínimos para as leis de vigilância foram previamente delineados pelo Alto Comissário, ver A/HRC/27/37 e A/HRC/39/29.

103 Ver a proposta de Lei de Inteligência Artificial da União Européia; as Diretrizes do Conselho Europeu de Proteção de Dados 05/2022 sobre o uso de tecnologia de reconhecimento facial na área de aplicação da lei, Versão 1.0, disponíveis em https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_en; ver também a lei no estado de Washington, Estados Unidos da América, relativa ao uso de reconhecimento facial, disponível em https://www.securityindustry.org/report/washington-facial-recognition-law-faq/; e proibições e moratórias adotadas por legislaturas locais e regionais.

50. Objetivos legítimos: não há dúvida de que a vigilância pública pode servir a uma ampla gama de objetivos legítimos, por exemplo, a proteção da vida das pessoas ou da integridade física e a segurança da infraestrutura crítica. Lamentavelmente, a vigilância pública é rotineiramente conduzida para objetivos que não são permitidos pela lei internacional de direitos humanos. A vigilância pública tem sido usada indevidamente, entre outras coisas, para identificar e rastrear dissidentes políticos, para realizar perfilamento racial e étnico, para ter como alvo comunidades de pessoas lésbicas, gays, bissexuais, transgêneros e intersexuais, e para avaliar a conformidade das pessoas com as normas sociais.

51. Necessidade e proporcionalidade: embora a vigilância pública possa ser permitida, os Estados devem demonstrar que as medidas são necessárias e proporcionais. No entanto, a eficácia das medidas de vigilância é muitas vezes duvidosa, levantando sérias questões quanto à sua necessidade ou proporcionalidade. As evidências sobre o efeito da vigilância por vídeo na segurança e na prevenção do crime são mistas. A maioria dos estudos aponta, no máximo, reduções modestas em alguns tipos de crimes (como crimes relacionados a veículos e bens) em áreas monitoradas por câmeras de vigilância, enquanto, em geral, crimes violentos não parecem ser afetados pela presença de câmeras de vigilância.[104] Além disso, uma comparação entre vários municípios em várias jurisdições mostra pouca ou nenhuma correlação entre o número de câmeras de vigilância pública e o crime ou a segurança em um município inteiro.[105] Com relação à detecção automática de ameaças, um sistema amplamente utilizado pelas forças policiais de detecção de disparos de arma de fogo para identificar possíveis cenas de crime, mostrou-se equivocado na identificação de sons como tiros em 89% dos casos.[106] Finalmente, muitos departamentos de polícia que se inscreveram para serviços de policiamento preditivo, desde então, encerraram essas colaborações, mencionando a utilidade limitada.[107]

52. O monitoramento geral de pessoas em espaços públicos é quase invariavelmente desproporcional. As medidas de vigilância em espaços públicos devem ser direcionadas e devem abordar um objetivo legítimo concreto, como evitar uma ameaça específica à proteção da população ou à segurança pública que seja significativa o suficiente para superar seus impactos adversos sobre os direitos humanos. Tais medidas precisam ser limitadas, focadas em locais e horários específicos, por exemplo, quando as evidências indicarem ser provável que um crime ocorra ou que ameaças à segurança pública possam surgir. Nenhuma alternativa menos invasiva da privacidade deve estar disponível. É essencial impor limitações estritas à duração do armazenamento dos dados capturados e aos propósitos associados para os quais esses dados serão usados. Os sistemas remotos de vigilância biométrica, em particular, suscitam sérias preocupações no que diz respeito à sua proporcionalidade, dada a sua natureza altamente intrusiva e o seu amplo impacto sobre um grande número de pessoas.[108] Nesse contexto, o Alto Comissário saudou os esforços recentes para limitar ou proibir o uso de tecnologias de reconhecimento biométrico remoto e pediu uma moratória sobre seu uso em espaços públicos, pelo

104 Ver https://academicworks.cuny.edu/jj_pubs/256/; e https://doi.org/10.1080/01924036.2021.1879885.

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

106 Ver https://www.macarthurjustice.org/blog/shotspotter-is-a-failure-whats-next/; e 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 Ver 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, paras. 26–27; e A/HRC/44/24, paras. 33–38.

menos até que as principais salvaguardas estejam em vigência.[109] Se usadas, essas tecnologias só devem ser implantadas para responder a situações como crimes graves e ameaças graves à segurança pública, se os efeitos discriminatórios puderem ser excluídos e submetidos a supervisão adequada e eficaz, incluindo autorização independente e auditorias independentes regulares de direitos humanos.

IV. Conclusões e Recomendações

53. O presente relatório fornece uma fotografia de várias áreas-chave nas quais o direito à privacidade no domínio digital está sendo ameaçado atualmente. A rápida adoção de tecnologias digitais levanta uma série de desafios adicionais que não são abordados neste relatório, mas que merecem mais atenção. Por exemplo, a vigilância em massa secreta, discutida em relatórios anteriores do Alto Comissário,[110] continua sendo um problema sério. Da mesma forma, as implicações de direitos humanos dos sistemas de identidade digital e os vários casos de uso da biometria são pouco compreendidos, apesar de sua implantação mundial. O rastreamento generalizado de usuários da Internet por inúmeras empresas, como anunciantes, instituições financeiras e corretoras de dados, exige muito mais atenção em fóruns internacionais de direitos humanos. A pandemia da doença de coronavírus (COVID-19) e a variedade estonteante de respostas digitais a ela podem ser objeto de um relatório próprio. As formas como as violações e abusos de privacidade afetam pessoas marginalizadas e pessoas em posição vulnerável devem ser exploradas e compreendidas mais profundamente. Fenômenos emergentes, como o impulso para a adoção generalizada de blockchain, tecnologias de realidade expandida e virtual e o desenvolvimento de neurotecnologia cada vez mais poderosa, devem ser acompanhados de perto.

54. No entanto, mesmo enfocando apenas alguns desenvolvimentos importantes, o presente relatório apresenta um quadro preocupante de como o direito à privacidade está sendo constantemente minado na era digital. Esta análise não deve ser entendida como uma negação dos enormes benefícios que as tecnologias digitais estão trazendo para as sociedades – pelo contrário, as sociedades devem abraçar plenamente o progresso tecnológico que capacita as pessoas, melhora vidas, fortalece a justiça e aumenta a produtividade. Mas são profundamente alarmantes as múltiplas maneiras pelas quais a vigilância generalizada ameaça os direitos humanos e o estado de direito e pode desgastar democracias vibrantes e pluralistas. As características das modernas tecnologias digitais em rede podem torná-las formidáveis ferramentas de controle e opressão: cada ação no espaço digital deixa um rastro de dados; a tecnologia de computação em nuvem facilita a fusão e análise de fontes de dados díspares; a automação aumenta o alcance e a eficácia possíveis da vigilância; e a vigilância digital é difícil de ser observada por seus sujeitos. Além disso, a vigilância digital está intimamente ligada à falta de transparência em geral. O público muitas vezes sabe muito pouco sobre as várias práticas de vigilância que estão entrelaçadas em muitos aspectos da vida. Os governos muitas vezes não divulgam informações confiáveis sobre que tipo de sistemas de vigilância eles usam e para quais propósitos – e muitas vezes negligenciam apresentar evidências sobre a eficácia desses sistemas.

55. Medidas de vigilância incompatíveis com o direito internacional dos direitos humanos já são difundidas. Mesmo onde a vigilância serve a propósitos legítimos, a infraestrutura

109 A/HRC/48/31, paras. 27 e 59 (d).

110 Ver A/HRC/27/37 e A/HRC/39/29.

subjacente pode ser facilmente reaproveitada, muitas vezes servindo a fins para os quais não foi originalmente planejada (o chamado "desvio de função") ou seguindo mudanças no cenário político. Os tomadores de decisão devem ter isso em mente ao considerar novos projetos que aumentam os poderes para coletar e analisar dados pessoais. Debates públicos sobre os limites da vigilância são urgentemente necessários. Sem uma discussão pública ativa, as sociedades correm o risco de entrar como sonâmbulos nos sistemas de vigilância, permitindo aqueles que estão no poder a exercerem níveis sem precedentes de controle sobre a vida cotidiana.

56. Com isso em mente, o ACNUDH recomenda que os Estados:

a. Garantam que qualquer interferência no direito à privacidade, incluindo hackeamento, restrições ao acesso e uso de tecnologia de criptografia e vigilância do público, esteja em conformidade com a lei internacional de direitos humanos, incluindo os princípios de legalidade, objetivo legítimo, necessidade e proporcionalidade e não discriminação, e não prejudique a essência desse direito;

b. Conduzam sistematicamente a devida diligência em direitos humanos, incluindo avaliações regulares de impacto abrangentes sobre os direitos humanos, ao projetar, desenvolver, adquirir, implantar e operar sistemas de vigilância;

c. Levem em consideração, ao realizar a devida diligência em direitos humanos e avaliar a necessidade e proporcionalidade de novos sistemas e poderes de vigilância, todo o ambiente jurídico e tecnológico no qual esses sistemas ou poderes estão ou seriam incorporados; os Estados também devem considerar os riscos de abuso, mudança de função e redirecionamento, incluindo riscos como resultado de futuras mudanças políticas;

d. Adotem e apliquem efetivamente, por meio de autoridades independentes, imparciais e com bons recursos, a legislação de privacidade de dados para os setores público e privado que observe a lei internacional de direitos humanos, incluindo salvaguardas, supervisão e recursos para proteger efetivamente o direito à privacidade;

e. Tomem medidas imediatas para aumentar efetivamente a transparência do uso de tecnologias de vigilância, inclusive informando adequadamente o público e os indivíduos e comunidades afetados, e fornecendo regularmente dados relevantes para o público avaliar sua eficácia e impacto nos direitos humanos;

f. Promovam o debate público sobre o uso de tecnologias de vigilância e garantam a participação significativa de todos os atores nas decisões sobre aquisição, transferência, venda, desenvolvimento, implantação e uso de tecnologias de vigilância, incluindo a elaboração de políticas públicas e sua implementação;

g. Implementem moratórias sobre a venda e uso doméstico e transnacional de sistemas de vigilância, como ferramentas de hackeamento e sistemas biométricos que possam ser usados para a identificação ou classificação de indivíduos em locais públicos, até que as salvaguardas adequadas para proteger os direitos humanos estejam em vigor; tais salvaguardas devem incluir medidas de controle doméstico e de exportação, de acordo com as recomendações feitas neste documento e em relatórios anteriores ao Conselho de Direitos Humanos;[111]

111 Ver A/HRC/27/37, A/HRC/39/29, A/HRC/44/24, e A/HRC/48/31.

h. Garantam que as vítimas de violações de direitos humanos e abusos relacionados ao uso de sistemas de vigilância tenham acesso a remédios eficazes.

57. Em relação às questões específicas levantadas no presente relatório, o ACNUDH recomenda que os Estados:

Hackeamento:

a. Garantam que o hackeamento de dispositivos pessoais seja empregado pelas autoridades apenas como último recurso, usado apenas para prevenir ou investigar um ato específico que represente uma ameaça grave à segurança nacional ou um crime grave específico, e tendo como alvo estritamente à pessoa suspeita de cometer esses atos; tais medidas devem estar sujeitas a uma supervisão independente rigorosa e devem exigir a aprovação prévia por um órgão judicial;

Criptografia:

b. Promovam e protejam a criptografia forte e evitem todas as restrições diretas ou indiretas, gerais e indiscriminadas sobre o uso da criptografia, como proibições, criminalização, imposição de padrões de criptografia fracos ou requisitos para verificação geral obrigatória do lado do cliente; a interferência na encriptação de comunicações privadas de particulares só deverá ser efetuada quando autorizada por órgão judiciário independente e caso a caso, tendo como alvo indivíduos se for estritamente necessário para a investigação de crimes graves ou para a prevenção de crimes graves ou ameaças à segurança pública ou à segurança nacional;

Vigilância de espaços públicos e controle de exportação de tecnologia de vigilância:

c. Adotem estruturas legais adequadas para reger a coleta, análise e compartilhamento de inteligência de mídia social que defina claramente os fundamentos permissíveis, pré-requisitos, procedimentos de autorização e mecanismos de supervisão adequados;

d. Evitem o monitoramento geral de espaços públicos que invada a privacidade e garantir que todas as medidas de vigilância pública sejam estritamente necessárias e proporcionais para alcançar objetivos legítimos importantes, inclusive limitando estritamente sua localização e tempo, bem como a duração do armazenamento de dados, a finalidade do uso dos dados e acesso aos dados; os sistemas de reconhecimento biométrico só devem ser usados em espaços públicos para prevenir ou investigar crimes graves ou ameaças graves à segurança pública, e se todos os requisitos do direito internacional dos direitos humanos forem implementados em relação aos espaços públicos;[112]

e. Estabeleçam regimes de controle de exportação robustos e bem adaptados aplicáveis a tecnologias de vigilância, cujo uso acarreta altos riscos para o gozo dos

112 Incluindo os requisitos estabelecidos em A/HRC/44/24, para. 53 (j) (i–v), e A/HRC/48/31, para. 59 (d).

direitos humanos; os Estados devem exigir avaliações transparentes de impacto sobre os direitos humanos que levem em conta as capacidades das tecnologias em questão, bem como a situação no Estado receptor, incluindo o cumprimento dos direitos humanos, a adesão ao estado de direito, a existência e aplicação efetiva das leis aplicáveis regular as atividades de fiscalização e a existência de mecanismos independentes de fiscalização;

f. Garantam que, no fornecimento e uso de tecnologias de vigilância, as parcerias público-privadas respeitem e incorporem expressamente os padrões de direitos humanos e não resultem na abdicação da responsabilidade governamental pelos direitos humanos.

Esta versão em português do Brasil de ***The right to privacy in the digital age : report of the Office of the United Nations High Commissioner for Human Rights*** **(A/HRC/51/17)** não é uma tradução oficial das Nações Unidas. A tradução foi realizada por Projeto Comunicações Privadas, Investigações e Direitos, do Instituto de Referência em Internet e Sociedade, que assume toda a responsabilidade pela acurácia da versão.

iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE