Naciones Unidas A/HRC/51/17

Asamblea General

Distr. general
4 de agosto de 2022
Español
Original: inglés

Consejo de Derechos Humanos
51er período de sesiones
12 de septiembre a 7 de octubre de 2022
Temas 2 y 3 de la agenda
Informe anual del Alto Comisionado de las Naciones Unidas para los Derechos Humanos e informes de la Oficina del Alto Comisionado y del Secretario General

Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

El derecho a la privacidad en la era digital

Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos*

Resumen

En este informe, presentado en cumplimiento de la resolución 48/4 del Consejo de Derechos Humanos, se analizan las tendencias y los problemas recientes en relación con el derecho a la privacidad. El informe se centra, en particular, en: a) el uso excesivo de herramientas de piratería informática invasivas; b) la función fundamental del cifrado en el disfrute del derecho a la privacidad y otros derechos; y c) la vigilancia generalizada de los espacios públicos. En él se hace hincapié en el riesgo de crear sistemas de vigilancia y control omnipresentes que pueden socavar el desarrollo de sociedades pujantes y respetuosas de los derechos.

* Se acordó publicar este informe tras la fecha prevista debido a circunstancias que escapan al control de quien lo presenta.

I. Introducción

1. Este informe se presenta en cumplimiento de la resolución 48/4 del Consejo de Derechos Humanos, en la que el Consejo pidió a la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) que preparase un informe en el que se describieran las tendencias y los problemas recientes en relación con el derecho humano a la privacidad, que determinara y aclarara los principios de derechos humanos, las salvaguardias y las mejores prácticas conexas, y que presentase el informe al Consejo en su 51er período de sesiones. El informe expone las respuestas recibidas a la solicitud de información realizada por el ACNUDH[1].

2. En todo el mundo se observan impresionantes avances tecnológicos e innovaciones que mejoran la vida de las personas e impulsan las economías. Sin embargo, también se observa cómo las herramientas digitales pueden volverse contra las personas, exponiéndolas a nuevas formas de vigilancia, aplicación de perfiles y control. Garantizar el respeto y la protección del derecho a la privacidad, reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos, en el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y en muchos otros instrumentos internacionales y regionales de derechos humanos[2] es quizás un factor fundamental para enfrentar las nuevas amenazas digitales contra los derechos humanos, que están inextricablemente vinculadas a los datos personales que accionan los mecanismos de las sociedades digitalizadas.

3. Tomando como base informes presentados anteriormente al Consejo de Derechos Humanos, en los que se trataba el tema de los problemas que se plantean al derecho a la privacidad[3], el presente informe se centra en tres tendencias notables relacionadas con el papel de los Estados en la salvaguarda y promoción del derecho a la privacidad: a) el uso excesivo de herramientas de piratería informática invasivas; b) la función fundamental del cifrado en el disfrute del derecho a la privacidad y otros derechos; y c) la vigilancia generalizada de los espacios públicos. En el informe se destaca el riesgo muy real e invasor que entraña la creación de sistemas de vigilancia y control omnipresentes que, a la larga, pueden estrangular el desarrollo de sociedades pujantes, prósperas y respetuosas de los derechos; como conclusión se formula una serie de recomendaciones para evitar ese resultado.

II. Vigilancia de dispositivos y comunicaciones personales

A. Piratería informática

4. En julio de 2021, Forbidden Stories, un consorcio de periodismo de investigación, apoyado por Amnistía Internacional, publicó unas revelaciones sobre el uso del programa Pegasus, que llamaron la atención internacional sobre una crisis de derechos humanos que llevaba años creciendo: la proliferación mundial de herramientas de piratería informática para la vigilancia selectiva y encubierta de dispositivos digitales. Aunque supuestamente se desplieguen para combatir el terrorismo y la delincuencia, esas herramientas de espionaje se han utilizado a menudo con motivos ilegítimos, incluida la represión de opiniones críticas o disidentes y de quienes las expresan, como periodistas, figuras políticas de la oposición y defensores de los derechos humanos.

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

[2] Véanse el artículo 16 de la Convención sobre los Derechos del Niño; el artículo 14 de la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares; el artículo 22 de la Convención sobre los Derechos de las Personas con Discapacidad; el artículo 10 de la Carta Africana sobre los Derechos y el Bienestar del Niño; el artículo 11 de la Convención Americana sobre Derechos Humanos, y el artículo 8 del Convenio para la Protección de los Derechos Humanos y de las Libertades Fundamentales.

[3] Véanse A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 y A/HRC/48/31.

5. El alcance de las operaciones del programa espía Pegasus y el número de víctimas son asombrosos. A partir de una lista filtrada de más de 50.000 números de teléfono de objetivos de vigilancia potenciales y reales, y de un análisis forense de numerosos teléfonos infectados, los informes de 2021 revelaron que al menos 189 periodistas, 85 defensores de los derechos humanos, más de 600 políticos y funcionarios del gobierno, incluidos ministros del gabinete, y diplomáticos se veían afectados en cuanto objetivos[4]. Las investigaciones también sacaron a la luz el espionaje a jueces, abogados, médicos, líderes sindicales y académicos[5]. NSO Group, la empresa que fabrica y vende Pegasus, ha admitido que las actividades de sus clientes están dirigidas a entre 12.000 y 13.000 personas al año[6].

6. El programa espía Pegasus es el ejemplo más destacado en un contexto cada vez más amplio de programas espía comercializados por empresas a Gobiernos de todo el mundo[7]. Según los investigadores, al menos 65 Gobiernos han adquirido herramientas comerciales de vigilancia mediante programas espía[8]. NSO ha informado de que cuenta con 60 organismos gubernamentales de 45 países entre sus clientes. Pocos días antes de las revelaciones sobre Pegasus, Citizen Lab y Microsoft publicaron un informe en el que se detallaba cómo otro programa, Candiru, había sido utilizado por los Gobiernos para atacar a defensores de los derechos humanos, disidentes, periodistas, activistas y políticos[9]. En noviembre de 2021, la empresa de redes sociales Meta anunció que había inhabilitado a siete entidades que habían atacado a personas a través de Internet en más de 100 países. La empresa también alertó a unas 50.000 personas que creía que habían sido objeto de tales actividades[10]. Se ha informado de que más de 500 empresas desarrollan, comercializan y venden tales herramientas de vigilancia a los Gobiernos[11].

7. Las capacidades de las herramientas y servicios espía que se ofrecen en el mercado mundial son formidables. Pegasus, por ejemplo, una vez instalado, ofrece un acceso completo y sin restricciones a todos los sensores e información de los dispositivos infectados, convirtiendo de hecho la mayoría de los teléfonos inteligentes en dispositivos de vigilancia las 24 horas del día, accediendo a la cámara y el micrófono, los datos de geolocalización, los correos electrónicos, los mensajes, las fotos y los vídeos, así como a todas las aplicaciones. Permite al intruso obtener una imagen detallada de la vida de sus víctimas, sus pensamientos, preferencias, actividades profesionales, pensamiento político, salud, situación financiera y vida social e íntima. Mientras que muchas herramientas de piratería informática requieren alguna acción por parte de la víctima, como hacer clic en un enlace o abrir un archivo adjunto a un mensaje, Pegasus se instala de forma sigilosa, a través del llamado “ataque sin clic”[12]. El programa hace casi imposible que las víctimas eviten la infección una vez que han sido atacadas.

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

[5] Véase 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] Según testimonio ante el Parlamento Europeo, comisión de investigación sobre el uso del programa espía de vigilancia Pegasus y otros equivalentes, 21 de junio de 2022; puede consultarse en: https://multimedia.europarl.europa.eu/en/webstreaming/pega-committee-meeting_20220621-1500-COMMITTEE-PEGA.

[7] Véase https://freedomhouse.org/sites/default/files/2022-05/Complete_TransnationalRepression Report2022_NEW_0.pdf, pág. 29.

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

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

[10] Véase https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/. Pueden verse otros ejemplos en: 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 y https://blogs.microsoft.com/on-the-issues/2020/12/21/cyber-immunity-nso/.

[11] A/HRC/41/35, párr. 6; véase también https://data.mendeley.com/datasets/csvhpkt8tm/2, donde figura un inventario mundial de programas espía comerciales.

[12] Cabe señalar que el programa Pegasus no es la única herramienta con estas capacidades y que el número de herramientas de este tipo está aumentando.

8. Las operaciones de piratería informática pueden adoptar muchas formas con distintos grados de intrusión. Si bien obtener el control total de un teléfono móvil o un ordenador ayuda a hacerse una idea detallada de la vida de las personas atacadas, hay otras técnicas de piratería que pueden ser menos invasivas, aunque siguen siendo muy graves, como la obtención de acceso a las cuentas de correo electrónico. Mediante la piratería informática también se puede acceder a otros dispositivos conectados, como los dispositivos tecnológicos o vehículos ponibles, que pueden proporcionar información adicional, incluso sobre datos de salud y localización. Los dispositivos equipados con cámaras o micrófonos, como los altavoces o los televisores inteligentes, también pueden convertirse en herramientas de vigilancia audiovisual. Atacar la infraestructura de los proveedores de servicios puede abrir el acceso a grandes cantidades de información sobre miles de clientes, incluyendo sus comunicaciones, datos de navegación y ubicaciones[13]. En los siguientes párrafos se centrará la atención en la piratería informática de los dispositivos de comunicación personales.

9. La piratería informática de los dispositivos de comunicación personales constituye una grave vulneración del derecho a la privacidad y puede vincularse a violaciones preocupantes de otra serie de derechos. Dado que la intrusión en los dispositivos de comunicación digital permite acceder a los borradores y a los historiales de búsqueda y navegación, también puede permitir conocer en profundidad los procesos de pensamiento de las personas sometidas a la piratería informática, así como sus opiniones y creencias políticas y religiosas, interfiriendo así en las libertades de opinión y pensamiento[14]. Las operaciones de piratería informática pueden ser experiencias profundamente traumáticas, que afectan a la salud mental de las víctimas y sus familias. Según se informa, la piratería informática ha dado lugar a la detención de defensores de los derechos humanos y políticos, algunos de los cuales habrían sido sometidos a tortura[15]. La piratería informática selectiva también se ha relacionado con ejecuciones extrajudiciales[16].

10. Además, atacar a los periodistas y a los medios de comunicación con herramientas de piratería informática socava gravemente la libertad de los medios, sobre todo porque las fuentes de información pueden temer ser detectadas y sufrir las consecuencias de ello. La mera existencia de programas de piratería informática puede tener efectos disuasorios en la libertad de expresión, la labor de los medios de comunicación y el debate y la participación públicos, lo que a su vez puede erosionar la gobernanza democrática. Según manifestó el Tribunal Supremo de la India en su reciente sentencia sobre el uso del programa informático Pegasus, el efecto disuasorio de la vigilancia supondría una "amenaza a la función vital de la prensa como 'guardián público'"[17].

11. La piratería informática también puede tener repercusiones negativas en los derechos al debido proceso y a un juicio imparcial[18]. Obtener acceso a un dispositivo puede permitir a un intruso no solo observar el contenido de ese dispositivo y sus interacciones con otros dispositivos, sino también manipularlo, incluso alterando, borrando o añadiendo archivos[19].

[13] La investigación sobre EncroChat de la policía de Francia y los Países Bajos, que había logrado interferir en la infraestructura de servidores de una red de comunicaciones cifrada, permitió recopilar información sobre más de 32.000 teléfonos en 121 países; véase Tribunal Federal de Justicia de Alemania, decisión de 2 de marzo de 2022, 5 StR 457/21, párr. 18.

[14] A/HRC/29/32, párr. 20. Para un análisis exhaustivo de la libertad de pensamiento, véase A/76/380.

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

[16] A/HRC/41/35, párr. 1; véase también el documento de sesión del Relator Especial sobre las ejecuciones extrajudiciales, sumarias o arbitrarias titulado "Annex to the report of the Special Rapporteur: investigation into the unlawful death of Mr. Jamal Khashogg". Puede consultarse en: https://www.timesofisrael.com/nsos-pegasus-used-to-target-khashoggis-wife-before-his-murder-washington-post/.

[17] Tribunal Supremo de la India, *Manohar Lal Sharma v. Union of India*, orden de 27 de octubre de 2021, párr. 39.

[18] A/HRC/23/40, párr. 62.

[19] A/HRC/39/29, párr. 19.

De ese modo es posible falsificar pruebas para incriminar o chantajear a determinadas personas[20].

12. Además, es posible que los programas espía no afecten únicamente a las personas a quienes están dirigidas las operaciones de piratería sino también a todas las personas que se comunican con ellas o, si se activa la cámara, el micrófono o la geolocalización del dispositivo, a cualquier persona presente en el mismo lugar físico[21].

13. Por último, la piratería informática se basa en la existencia de fallos de seguridad en los sistemas informáticos, y los aprovecha. Al mantener expuestas esas vulnerabilidades, o incluso creándolas, quienes recurren a la piratería informática pueden incidir en las amenazas a la seguridad y la privacidad que afectan a millones de usuarios y al ecosistema de información digital en general[22].

14. Los órganos de derechos humanos y los expertos en el tema llevan años dando la voz de alarma sobre los programas espía. La Asamblea General y el Consejo de Derechos Humanos han declarado en repetidas ocasiones que los Estados Miembros deberían abstenerse de toda práctica de vigilancia ilegal o arbitraria, lo que incluye la piratería informática[23]. Varios relatores especiales han criticado duramente las prácticas de piratería informática que van más allá de lo necesario para perseguir fines legítimos, como la lucha contra el terrorismo y la delincuencia[24]. El Comité de Derechos Humanos también ha expresado su preocupación por la piratería informática patrocinada por el Estado, en particular cuando se recurre a ella sin una supervisión o unas salvaguardias adecuadas[25]. A nivel regional, el anterior Relator Especial para la libertad de expresión de la Comisión Interamericana de Derechos Humanos condenó las operaciones de piratería informática con fines no permitidos y pidió que se castigara con dureza a los infractores, incluso por medidas adoptadas por motivos políticos contra periodistas y medios de comunicación independientes[26].

15. Como reacción a las revelaciones sobre el uso del programa Pegasus, varias instituciones regionales y nacionales, como el Consejo de Europa, la Comisión Interamericana de Derechos Humanos, el Parlamento Europeo y el Tribunal Supremo de la India, han expresado su preocupación por la proliferación de programas espía y han iniciado audiencias e investigaciones[27]. También se están llevando a cabo investigaciones penales[28] y demandas civiles[29].

---

[20] Véase https://www.wired.com/story/modified-elephant-planted-evidence-hacking-police/ como ejemplo de tales alegaciones.

[21] Véase https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, pág. 8.

[22] A/HRC/39/29, párr. 19.

[23] Resolución 75/176 de la Asamblea General y resoluciones 48/4 y 45/18 del Consejo de Derechos Humanos.

[24] A/HRC/17/27; A/HRC/20/17; A/HRC/23/40, párr. 62; A/HRC/41/35; A/HRC/41/41 y A/73/438; véase también https://www.ohchr.org/en/press-releases/2021/08/spyware-scandal-un-experts-call-moratorium-sale-life-threatening.

[25] Véanse CCPR/C/DEU/CO/7; CCPR/C/NLD/CO/5; y CCPR/C/ITA/CO/6.

[26] Véase https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=998&lID=2.

[27] Véanse https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=1207&lID=2; https://www.oas.org/es/cidh/jsForm/?File=/es/cidh/prensa/comunicados/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, y Tribunal Supremo de la India, *Manohar Lal Sharma v. Union of India*, orden de 27 de octubre de 2021.

[28] Véanse https://www.euronews.com/next/2021/07/20/paris-prosecutor-to-investigate-alleged-pegasus-hacking-after-complaint-by-french-journali y 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/ y https://cdn.ca9.uscourts.gov/datastore/opinions/2021/11/08/20-16408.pdf. En

16. La orientaciones sobre los requisitos mínimos y las salvaguardias necesarias para cualquier uso gubernamental de programas espía pueden basarse en un amplio conjunto de análisis de derechos humanos relacionados con la vigilancia[30]. Debido a la magnitud de los efectos adversos de la piratería informática es necesario ser sumamente cautelosos al utilizarla, limitándose a las circunstancias más excepcionales y en estricto cumplimiento de los requisitos del derecho internacional de los derechos humanos.

17. Sin embargo, muchas jurisdicciones no han establecido tales sistemas de protección jurídica esenciales y no tienen leyes claras, precisas y disponibles públicamente por las que deban regirse las operaciones de piratería informática. Si bien algunos Estados han promulgado marcos jurídicos que cumplirían con el derecho internacional de los derechos humanos, otros se basan en leyes demasiado amplias o anticuadas, promulgadas antes de que aparecieran las tecnologías modernas.

18. Como han demostrado las revelaciones sobre el programa Pegasus y los consiguientes informes, la piratería informática practicada por diversos agentes estatales parece perseguir a menudo objetivos que no son legítimos según el derecho internacional de los derechos humanos. Aunque, en determinadas circunstancias, las medidas de vigilancia invasiva podrían permitirse en virtud de los artículos 17 y 19 del Pacto Internacional de Derechos Civiles y Políticos por motivos de protección de la seguridad nacional o del orden público, la piratería informática nunca puede justificarse por motivos políticos o comerciales, lo que suele ocurrir cuando se ataca a los defensores de los derechos humanos o a los periodistas.

19. Incluso si se persiguen fines legítimos, como los objetivos de seguridad nacional o la protección de los derechos de las demás personas, la evaluación de la necesidad y la proporcionalidad del uso de programas espía limita en gran medida las circunstancias en las que podría permitirse su utilización[31]. Existen argumentos de peso para afirmar que herramientas tales como el programa Pegasus, que permiten una intrusión sin límites en la vida de las personas y que pueden llegar incluso a sus pensamientos íntimos, podrían afectar a la esencia del derecho a la privacidad[32] e interferir en los derechos absolutos a la libertad de pensamiento y opinión. Dadas las considerables repercusiones negativas del uso de los programas espía y de su alcance, que trasciende los objetivos previstos, su uso debería limitarse a los casos en que sirva para prevenir o investigar un delito grave concreto o un acto que suponga una grave amenaza para la seguridad nacional. Debería limitarse a la investigación de una persona o de varias personas sospechosas de cometer o haber cometido tales actos. Debería aplicarse como medida de último recurso, es decir, una vez agotadas todas las demás medidas menos invasivas o bien cuando estas han demostrado que no han sido útiles, y limitarse estrictamente su alcance y duración. Solo deberían utilizarse y recogerse los datos pertinentes[33]. Las medidas también deberían estar sujetas a una rigurosa supervisión independiente; es imprescindible la aprobación previa de un órgano judicial[34]. Además, unos controles de exportación sólidos y transparentes, que tengan en cuenta explícitamente los riesgos para los derechos humanos pueden ser una poderosa herramienta para prevenir las violaciones y los abusos de los derechos[35]. El ACNUDH reitera su reciente llamamiento, así como el de los expertos y grupos de derechos humanos, a favor de una

https://citizenlab.ca/2018/12/litigation-and-other-formal-complaints-concerning-targeted-digital-surveillance-and-the-digital-surveillance-industry/ figura un extenso resumen de las acciones legales emprendidas.

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

31 Véase Tribunal Constitucional Federal de Alemania, sentencia de 27 de febrero de 2008 (1 BvR 370, 595/07), en 247 aa).

32 Supervisor Europeo de Protección de Datos, véase https://edps.europa.eu/system/files/2022-02/22-02-15_edps_preliminary_remarks_on_modern_spyware_en_0.pdf, pág. 8.

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

34 Véase A/HRC/39/29 sobre las garantías mínimas de las medidas de vigilancia secretas.

35 A/HRC/39/29, párr. 25; A/HRC/44/24, párr. 40; A/HRC/48/31, párr. 46 y A/HRC/41/35, párrs. 34 y 66. Con la reciente adopción de una nueva normativa sobre el control de las exportaciones, la Unión Europea ha demostrado el mayor énfasis puesto en los derechos humanos.

moratoria para la venta, transferencia y uso de herramientas de piratería informática hasta que se establezca un régimen de salvaguardias basado en los derechos humanos[36].

B. Restricciones del cifrado

20. En los últimos años, varios Gobiernos han tomado medidas que, intencionadamente o no, atentan contra la seguridad y la confidencialidad de las comunicaciones cifradas. Tal situación preocupa, por sus consecuencias para el disfrute del derecho a la privacidad y otros derechos humanos.

21. El cifrado es un elemento clave para la privacidad y la seguridad en línea y es esencial para salvaguardar derechos, tales como los derechos a la libertad de opinión y expresión, la libertad de asociación y reunión pacífica, la seguridad, la salud y la no discriminación. Garantiza que las personas puedan compartir información libremente, sin temor a que sus datos sean conocidos por otros, ya sean autoridades estatales o ciberdelincuentes. El cifrado es esencial para que las personas se sientan seguras al intercambiar libremente información con otras sobre una serie de experiencias, pensamientos e identidades, incluida información delicada sobre temas de salud o financieros, información sobre identidades de género y orientación sexual, expresiones artísticas e información relacionada con la condición de minoría. En entornos de censura generalizada, el cifrado ofrece a las personas un espacio para sostener, expresar e intercambiar opiniones con los demás. En determinados casos, los periodistas y los defensores de los derechos humanos no pueden realizar su trabajo sin un cifrado de alta seguridad, que protege a sus fuentes y las resguarda de los poderosos actores investigados. El cifrado proporciona a las mujeres, que se enfrentan a amenazas particulares de vigilancia, acoso y violencia en línea, un importante nivel de protección contra la divulgación involuntaria de información[37]. En los conflictos armados, la mensajería cifrada es indispensable para garantizar la seguridad de las comunicaciones entre los civiles. Cabe destacar que en los dos meses posteriores al inicio del conflicto armado en Ucrania, el 24 de febrero de 2022, el número de descargas de la aplicación de mensajería cifrada Signal aumentó en Ucrania más de un 1.000 % en comparación con los meses anteriores[38].

22. El papel fundamental del cifrado como un elemento que habilita la privacidad y el goce de los derechos humanos ha sido ampliamente reconocido, entre otros, por los Estados, los organismos de las Naciones Unidas, el ACNUDH y varios expertos en derechos humanos[39]. La Asamblea General y el Consejo de Derechos Humanos también han recalcado la importancia del cifrado en la protección de los derechos humanos en varias resoluciones, en las que se pide a los Estados que se abstengan de interferir en las tecnologías de cifrado[40] y se anima a las empresas a trabajar para habilitar soluciones técnicas que aseguren y protejan la confidencialidad de las comunicaciones digitales, incluido el cifrado, el uso de seudónimos y el anonimato[41]. Varios relatores especiales y expertos regionales han expresado su apoyo al cifrado de alta seguridad como elemento habilitador de derechos, recomendando promover y proteger tal tipo de cifrado y advirtiendo acerca de medidas que podrían restringir arbitraria o ilegalmente el uso de esta tecnología clave[42]. El Comité de los Derechos del Niño ha

[36] Véanse 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/ y https://cyberpeaceinstitute.org/news/renewed-call-moratorium-spyware/.

[37] A/HRC/35/9, párr. 18.

[38] Véase https://sensortower.com/blog/signal-telegram-ukraine-russia-2022.

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

[40] Resolución 75/176 de la Asamblea General y resoluciones 39/6, 44/12, 45/18 y 48/4 del Consejo de Derechos Humanos.

[41] Resolución 75/176 de la Asamblea General y resolución 48/4 del Consejo de Derechos Humanos.

[42] Véanse A/HRC/29/32; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf; A/HRC/41/41; https://www.ohchr.org/sites/default/files/Documents/Issues/Opinion/JointDeclaration10July2019_English.pdf; https://www.osce.org/representative-on-freedom-of-media/379351 y https://www.oas.org/es/cidh/docs/anual/2020/capitulos/rele.PDF.

subrayado que cualquier medida que permita detectar material de explotación y abuso sexuales de niños en las comunicaciones cifradas debe estar estrictamente limitada según los principios de legalidad, necesidad y proporcionalidad[43]. El Consejo de Derechos Humanos, las Naciones Unidas y los expertos regionales en derechos humanos han recalcado que el cifrado es fundamental para el trabajo periodístico y la protección de las fuentes[44]. Los indicadores de la universalidad de Internet publicados por la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (UNESCO) destacan la importancia del cifrado para la confianza y la seguridad en línea[45].

23. A pesar de sus ventajas, los Gobiernos a veces restringen el uso del cifrado, por ejemplo, para proteger la seguridad nacional y combatir la delincuencia, en particular para detectar material que muestre abusos sexuales de niños. Tales restricciones incluyen la prohibición de las comunicaciones cifradas y la penalización por ofrecer o utilizar herramientas de cifrado[46] o bien el registro y la licencia obligatorios de las herramientas de cifrado[47]. Del mismo modo, en algunos casos se ha exigido a los proveedores de sistemas de cifrado que garanticen que las fuerzas del orden u otros organismos gubernamentales tengan acceso a todas las comunicaciones cuando lo soliciten, lo que, de hecho, equivale a una restricción general del cifrado que podría requerir, o al menos fomentar, la creación de algún tipo de puerta trasera (una vía incorporada para eludir el cifrado, que permita el acceso encubierto a los datos en texto plano)[48]. Otra forma de interferencia con el cifrado es la exigencia de que se creen y mantengan sistemas de custodia de claves, y que todas las claves privadas necesarias para descifrar datos se entreguen al Gobierno o a un tercero designado[49]. La imposición de requisitos de trazabilidad, según los cuales los proveedores deben ser capaces de rastrear cualquier mensaje hasta su supuesto originador, también podría requerir el debilitamiento de las normas de cifrado[50]. En fecha reciente, varios Estados han empezado a imponer o a estudiar la posibilidad de imponer obligaciones generales de vigilancia a los proveedores de comunicaciones digitales, incluidos los que ofrecen servicios de comunicaciones cifradas[51]. Estos deberes podrían obligar efectivamente a esos proveedores a abandonar el cifrado de alta seguridad de un extremo a otro o a encontrar soluciones alternativas muy problemáticas (véanse los párrafos 27 y 28 más abajo).

24. No cabe duda de que las capacidades de cifrado tan ampliamente utilizadas, capacidades que el público ha exigido como respuesta a la vigilancia masiva y a la ciberdelincuencia, crean un dilema para los Gobiernos que tratan de proteger a las poblaciones, en particular a sus miembros más vulnerables, contra delitos graves y amenazas a la seguridad. Sin embargo, como señaló el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, la reglamentación del cifrado puede socavar los derechos humanos[52]. Los Gobiernos que pretenden limitar el cifrado muchas veces no logran demostrar que las restricciones que impondrían son necesarias para satisfacer un interés legítimo particular, dado que se dispone de varias otras herramientas y enfoques que proporcionan la información necesaria para fines específicos en materia de cumplimiento

[43] Comité de los Derechos del Niño, observación general núm. 25 (2021), relativa a los derechos de los niños en relación con el entorno digital, párr. 70.

[44] Resolución 45/18 del Consejo de Derechos Humanos; A/HRC/29/32 y https://www.osce.org/representative-on-freedom-of-media/379351.

[45] Véase https://es.unesco.org/internetuniversality, indicador D.5.

[46] Véanse PSE 2/2017 y LBY 3/2022. Todas las comunicaciones mencionadas en el presente informe pueden consultarse en el siguiente enlace: https://spcommreports.ohchr.org/Tmsearch/TMDocuments.

[47] Véase https://hrsly.com/wp-content/uploads/2022/06/OL-LBY-3.2022-DownLoadPublicCommunicationFile.pdf (LBY 3/2022).

[48] Véanse GBR 4/2015, MYS 2/2018, AUS 5/2018 y AUS 6/2018.

[49] Véase RUS 7/2016 y RUS 7/2018.

[50] Véase IND 31/2018, IND 3/2019, BRA 6/2020 y BRA 7/2020.

[51] Por ejemplo, la Ley “EARN IT” aprobada en los Estados Unidos de América en 2020 (véase USA 4/2020); el proyecto de ley de seguridad en línea en el Reino Unido (véase GBR 5/2022); la propuesta de la Comisión Europea de un reglamento del Parlamento Europeo y del Consejo en el que se establezcan normas para prevenir y combatir los abusos sexuales de niños, 11 de mayo de 2022 (COM(2022) 209), y Gobierno de la India, Reglamento sobre Tecnología de la Información (Directrices de Intermediación y Código de Ética de los Medios Digitales), 2021 (véase IND 8/2021).

[52] Véase A/HRC/29/32.

de la ley o para otros fines legítimos[53]. Tales medidas alternativas incluyen la mejor dotación de recursos para los servicios policiales tradicionales, las operaciones encubiertas, el análisis de metadatos y el refuerzo de la cooperación policial internacional.

25. Además, las consecuencias de la mayoría de las restricciones que se imponen al cifrado en el derecho a la privacidad y otros derechos relacionados son desproporcionadas, ya que a menudo afectan no solo a las personas a las que está destinada la medida sino también a la población en general. Las prohibiciones absolutas por parte de los Gobiernos, o la criminalización del cifrado en particular no pueden justificarse, ya que impiden que todos los usuarios dentro de sus jurisdicciones tengan una forma segura de comunicación. Los sistemas de custodia de claves tienen importantes vulnerabilidades, porque dependen de la integridad de los sistemas de almacenamiento y exponen las claves almacenadas a ciberataques. Además, las puertas traseras obligatorias en las herramientas de cifrado crean responsabilidades que superan con creces su utilidad respecto de usuarios específicos identificados como sospechosos de delitos o amenazas a la seguridad. Atentan contra la vida privada y la seguridad de todos los usuarios, que quedan expuestos a las interferencias ilícitas no solo de los Estados, sino también de agentes no estatales, incluidas las redes delictivas[54]. Los requisitos de licencia y registro tienen efectos desproporcionados similares, por cuanto exigen que el programa de cifrado tenga puntos débiles que puedan explotarse[55]. Estos efectos adversos no se limitan necesariamente a la jurisdicción que impone la restricción; lo que es más probable que suceda es que, una vez establecidas en la jurisdicción de un Estado, las puertas traseras pasen a formar parte del programa utilizado en otras partes del mundo.

26. En los últimos tiempos se ha propuesto el concepto del escaneo del lado del cliente para detectar ciertas formas de contenido objetable, con el fin de evitar muchos de los problemas señalados anteriormente. El escaneo del lado del cliente traslada el paso de la detección de contenidos de los servidores a través de los cuales se envían las comunicaciones a los propios dispositivos personales. De este modo, el contenido en cuestión se examina antes de ser cifrado para su transporte. En agosto de 2021, Apple anunció que tenía previsto introducir un sistema de este tipo para sus servicios de iMessage e iCloud, pero suspendió la aplicación del cambio propuesto tras las fuertes críticas recibidas de numerosos expertos en seguridad informática, criptógrafos y grupos de derechos humanos[56]. Sin embargo, varias iniciativas legislativas[57] pueden obligar, al menos indirectamente, a los servicios de comunicaciones por Internet a implantar dichos sistemas, imponiendo amplias obligaciones de control para todas las comunicaciones, incluidas las cifradas. Dado que el contenido de los mensajes, una vez cifrados, no puede ser consultado por nadie más que el remitente y el destinatario, cualquier obligación general de vigilancia obligaría a los proveedores de servicios a abandonar el cifrado del transporte o a buscar el acceso a los mensajes antes de cifrarlos.

27. Imponer el escaneo general del lado del cliente constituiría un cambio de paradigma, que plantea una serie de problemas graves con consecuencias potencialmente nefastas para el disfrute del derecho a la privacidad y otros derechos. A diferencia de otras intervenciones, la obligatoriedad de realizar un escaneo general del lado del cliente afectaría inevitablemente a todas las personas que utilizan los medios de comunicación modernos, y no solo a aquellas involucradas en delitos y amenazas de seguridad graves. El escaneo obligatorio del lado del cliente cambia la capacidad de las personas de controlar plenamente los dispositivos de comunicación que están intrínsecamente conectados a todas las facetas de sus vidas y de limitar la información que comparten esos dispositivos[58]. Además, no puede evitarse que el escaneo general de las comunicaciones produzca frecuentes falsos positivos, por elevados

[53] *Ibid.*, párr. 39.
[54] A/HRC/39/29, párr. 20.
[55] A/HRC/29/32, párr. 41.
[56] Véase https://cdt.org/wp-content/uploads/2021/08/CDT-Coalition-ltr-to-Apple-19-August-2021.pdf.
[57] Comisión Europea, propuesta de un reglamento del Parlamento Europeo y del Consejo en el que se establezcan normas para prevenir y combatir los abusos sexuales de niños, 11 de mayo de 2022 (COM(2022) 209); véase también el proyecto de Ley de Seguridad en Línea en el Reino Unido de Gran Bretaña e Irlanda del Norte, que puede consultarse en: https://www.gov.uk/government/publications/draft-online-safety-bill.
[58] Comunicaciones del Comité Directivo de Global Encryption Coalition y de Privacy International.

que sean los índices de precisión, lo que afecta a numerosas personas inocentes[59]. Dada la posibilidad de que se deriven esas consecuencias, es probable que la vigilancia indiscriminada tenga un importante efecto disuasorio en la libertad de expresión y de asociación, y que las personas limiten las formas de comunicarse e interactuar con los demás y se autocensuren[60].

28. El escaneo del lado del cliente también plantea nuevos retos en materia de seguridad, haciendo más probable las vulneraciones de la seguridad[61]. El proceso de escaneo también puede ser manipulado, lo que permite crear artificialmente perfiles falsos positivos o falsos negativos[62]. Incluso si, para los fines actuales, el escaneo del lado del cliente es sumamente específico, cabe pensar que el hecho de que los Gobiernos permitan el escaneo de los dispositivos haga que en el futuro se intente ampliar el alcance de los contenidos a los que se dirigen esas medidas[63]. En particular, cuando el estado de derecho es frágil y los derechos humanos corren peligro, los efectos del escaneo del lado del cliente podrían ser mucho más amplios, por ejemplo, podría utilizarse para suprimir el debate político o para atacar a figuras de la oposición, periodistas y defensores de los derechos humanos[64]. En vista de la gran diversidad de riesgos significativos para la protección de los derechos humanos que se derivan del escaneo del lado del cliente, estos requisitos no deberían imponerse sin un examen más exhaustivo de sus posibles repercusiones en los derechos humanos y medidas para mitigar esos daños. A falta de una investigación y un análisis en profundidad, parece poco probable que estas restricciones puedan considerarse proporcionadas en virtud del derecho internacional de los derechos humanos, incluso cuando se imponen para perseguir fines legítimos, dada la gravedad de sus posibles consecuencias[65].

III. Vigilancia del público

29. El Alto Comisionado ha planteado en varias ocasiones su preocupación por la vigilancia masiva, en particular por la interceptación masiva de comunicaciones[66]. Aunque algunos Estados han mejorado las salvaguardias contra la vigilancia, la práctica profundamente preocupante de vigilar las actividades en línea de grandes partes de la población, o incluso de poblaciones enteras, no ha cesado. Si bien los informes anteriores se han centrado sobre todo en la vigilancia de las comunicaciones privadas, no se han referido tanto a las consecuencias de la vigilancia de los lugares públicos para la privacidad, cuestión que se analiza a continuación.

[59] Véase https://doi.org/10.48550/arXiv.2110.07450.

[60] Para más información sobre los efectos disuasorios de la vigilancia, véase el párrafo 47 más adelante.

[61] En comparación con los ataques a servidores de empresas, los ataques a dispositivos personales pueden ser ejecutados por más actores y en una infraestructura menos segura. Los adversarios pueden utilizar su acceso al dispositivo para aplicar técnicas de ingeniería inversa al mecanismo de escaneo, véase https://doi.org/10.48550/arXiv.2110.07450.

[62] https://www.usenix.org/conference/usenixsecurity21/presentation/kulshrestha y 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 y https://doi.org/10.48550/arXiv.2110.07450.

[64] *Ibid*.

[65] A/HRC/39/29, párr. 20 y A/HRC/29/32, párr. 43. Las opiniones del Tribunal de Justicia de la Unión Europea respaldan esta conclusión. El tribunal dictaminó recientemente que el análisis automatizado de datos de tráfico y localización de forma general e indiscriminada debía limitarse a lo estrictamente necesario para responder a una amenaza grave, real, presente o previsible para la seguridad nacional. El tribunal rechazó cualquier otra justificación. Véase *La Quadrature du Net and Others v. Premier ministre and Others*, sentencia de 6 de octubre de 2020 (asuntos acumulados C-511/18, C-512/18 y C-520/18), párr. 177. Además, su jurisprudencia indica un escepticismo aún mayor respecto del análisis de los datos de contenido, Tribunal de Justicia de la Unión Europea, *Maximillan Schrems v. Data Protection Commissioner*, sentencia de 6 de octubre de 2015 (C-362/14), párr. 94.

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

A. Vigilancia de lugares públicos

30. Las cámaras de vigilancia, desplegadas para controlar las vías públicas, estacionamientos, centros de transporte y otros lugares públicos, se han convertido en algo habitual en muchos países. Se preveía que el número de cámaras de vigilancia en uso en todo el mundo superase los mil millones en 2021[67]. Las 10 ciudades del mundo con mayor densidad de videovigilancia tienen entre 39 y más de 115 cámaras de vigilancia por cada 1.000 habitantes[68].

31. Además de los sistemas de vigilancia operados por el Estado, algunas empresas han integrado herramientas de vigilancia para uso privado, con funciones específicas para informar sobre incidentes a las autoridades o incluso para concederles acceso directo a sus flujos de datos[69]. Esto amplía enormemente el espacio público bajo vigilancia, al tiempo que socava la transparencia, la supervisión y la rendición de cuentas.

32. En los últimos años, las capacidades de las cámaras de vigilancia han aumentado drásticamente gracias a la incorporación de sofisticadas capacidades de análisis de vídeo. Se calcula que, en 2010, menos del 2 % de las cámaras de red vendidas llevaban incorporado el análisis de vídeo, pero esta proporción había superado el 40 % en 2016, crecimiento que es probable que prosiga[70]. Las funciones de análisis se basan cada vez más en la inteligencia artificial. Las capacidades añadidas para llevar a cabo el reconocimiento facial y la identificación de comportamientos como sospechosos son algunas de las características más problemáticas de los sofisticados sistemas de videovigilancia[71]. Además, el uso de drones con fines de vigilancia se ha normalizado en muchos países, donde se utilizan para vigilar protestas y otro tipo de reuniones[72].

33. Se están llevando cada vez más iniciativas basadas en datos, englobadas en el término general de “ciudades inteligentes”, con el fin de remodelar los espacios urbanos. Los proyectos de ciudades inteligentes se centran en la recopilación y el procesamiento de datos para informar sobre la gestión de las instalaciones de la ciudad, gracias a tecnologías de sensores cada vez con mayores capacidades. Si bien gran parte de los datos recogidos y procesados en esos contextos se refieren a cuestiones como los datos sobre los flujos de tráfico, la contaminación o el ruido, al margen del ámbito de los datos personales, otros datos recogidos pueden vincularse fácilmente a las personas, como las matrículas y los datos de los contadores inteligentes. Además, los datos aparentemente anónimos a menudo pueden desanonimizarse[73], y la infraestructura, como las cámaras instaladas para controlar los flujos de datos sobre el tráfico, puede ser reutilizada para el seguimiento de personas[74].

34. Estas novedades suelen producirse en un contexto de nuevos sistemas de identidad y de ampliación de las bases de datos biométricos. Los sistemas de identidad están vinculados a un extenso almacenamiento central de datos personales en varios países, que incluye información biométrica, como las huellas dactilares, la geometría facial, escaneos del iris y el ADN. Además, las bases de datos suelen estar interconectadas y ponerse a disposición de otros organismos para que realicen búsquedas. Ello hace que la identificación de las personas, dondequiera que se encuentren, resulte cada vez más fácil.

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

[68] Véanse https://www.comparitech.com/vpn-privacy/the-worlds-most-surveilled-cities/ y https://surfshark.com/surveillance-cities.

[69] Véase https://www.accessnow.org/amazon-ring-privacy-review/.

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

[71] Véanse las comunicaciones de Derechos Digitales y de International Network of Civil Liberties Organizations.

[72] Véanse las comunicaciones de Amnistía Internacional y de CIVICUS.

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

[74] Para más información sobre las repercusiones de las ciudades inteligentes en los derechos humanos, véase https://www.amnesty.org/en/latest/research/2019/06/smart-cities-dreams-capable-of-becoming-nightmares/ y https://carrcenter.hks.harvard.edu/files/cchr/files/CCDP_006.pdf.

B. Vigilancia en línea

35. Paralelamente, se ha generalizado la vigilancia del discurso público en línea. Muchas autoridades de todo el mundo están recopilando y analizando los mensajes publicados en medios sociales y las redes privadas y profesionales construidas en plataformas de comunicación de acceso público. Esta información obtenida de los medios sociales abarca desde la investigación de usuarios concretos hasta la recopilación, almacenamiento y análisis de grandes cantidades de datos. Los datos obtenidos pueden incluir: nombres; edades; fotografías y las correspondientes plantillas digitales; direcciones; reacciones a los mensajes de otras personas; contactos sociales y profesionales y redes conexas; datos de localización; intereses; orientación sexual; identificación de género; afiliación y actividades políticas; creencias religiosas e información sanitaria.

36. A menudo, varios tipos de análisis predictivos forman parte de las prácticas de inteligencia de los medios sociales, incluidos los intentos de detectar posibles puntos conflictivos. Sin embargo, estos análisis también pueden utilizarse para evaluar el comportamiento pasado, presente y futuro de las personas y asignar puntuaciones de riesgo relacionadas con la probabilidad de que se conviertan en delincuentes o en amenazas para la seguridad[75]. La información obtenida de los medios sociales también se utiliza para predecir la posibilidad de que se produzcan disturbios sociales[76].

37. Estas actividades pueden servir para múltiples fines legítimos e ilegítimos, desde la investigación de delitos y las actividades de prevención de la delincuencia hasta el estudio de solicitantes de prestaciones sociales, el seguimiento de protestas, la medición del sentimiento público y la elaboración de perfiles de la conducta social de las personas[77].

C. Efectos en los derechos humanos

38. Las tecnologías modernas basadas en los datos están cambiando radicalmente el equilibrio de poder entre la entidad que lleva a cabo la vigilancia y quienes son objeto de esta. Antes de que surgieran la vigilancia automatizada a gran escala y las herramientas de análisis de datos, existían limitaciones prácticas a la vigilancia, que proporcionaban cierto nivel de protección a las personas, incluso en público[78]. Las sofisticadas herramientas digitales hacen que esas protecciones “naturales” del pasado se vuelvan vanas. Hoy en día, un solo funcionario puede supervisar las cuentas de los medios sociales de docenas de personas y, con la ayuda de programas sofisticados y el análisis de los macrodatos, bastan pequeños equipos para observar y elaborar perfiles de miles de cuentas[79].

39. Existen novedades similares que aumentan la eficacia y el alcance de otras medidas de vigilancia de los espacios públicos. Por ejemplo, el auge de la tecnología de reconocimiento facial, junto con otras tecnologías de reconocimiento biométrico, ha transformado fundamentalmente las prácticas tradicionales de vigilancia audiovisual, ya que ha aumentado de forma radical la capacidad de identificar a personas en espacios públicos, incluidas personas que participan en reuniones. La tecnología de reconocimiento facial en directo permite la identificación de personas en tiempo real, así como su vigilancia y seguimiento específicos. La identificación retrospectiva de las personas amplía quizás la diversidad de fuentes de datos, lo que puede tener efectos igualmente invasivos[80] si no se ejerce la máxima moderación.

40. Las consecuencias de la vigilancia pública en los derechos humanos resultan aún más graves porque las fuentes de datos se fusionan cada vez más, por ejemplo, combinando las fuentes de videovigilancia equipadas con reconocimiento facial con los datos de los medios sociales[81] y las bases de datos gubernamentales, incluida información sobre seguridad social,

[75] Véase https://digitalcommons.law.umaryland.edu/jbtl/vol12/iss2/2/, pág. 152.
[76] Véase https://dx.doi.org/10.2139/ssrn.2702426, pág. 1.
[77] Véase https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[78] A/HRC/44/24, párr. 34.
[79] Véase https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media/.
[80] Véase la comunicación de Amnistía Internacional.
[81] Véase la comunicación de International Network of Civil Liberties Organizations.

migración, sospechosos de terrorismo, detenciones o incluso listas de personas señaladas por motivos políticos.

41. Además, los Estados se basan en vastas recopilaciones de datos acumuladas por diversas empresas privadas. En informes anteriores, el Alto Comisionado y los relatores especiales han puesto de relieve la cuestión de los Gobiernos que solicitan acceso a los datos recogidos por los proveedores de servicios de telecomunicaciones e Internet, a menudo en el contexto de las leyes de retención obligatoria de datos[82]. La gama de empresas que reciben este tipo de solicitudes crece sin cesar. Algunos Estados obligan a las empresas a darles acceso directo a los flujos de datos que circulan a través de sus redes. Esos sistemas de acceso directo suscitan gran preocupación, ya que son particularmente propicios a los abusos y tienden a eludir las garantías procesales fundamentales[83].

42. Además, los Estados recurren cada vez más a los servicios de vigilancia que ofrecen las empresas, por ejemplo, adquiriendo información de corredores de datos y otras empresas que recogen y venden datos personales[84]. Tales prácticas pueden eludir restricciones y salvaguardias procesales cruciales, permitiendo a los Estados acceder indirectamente a herramientas que no podrían haber desplegado ellos mismos sin contravenir sus obligaciones en materia de derechos humanos. Por ejemplo, la herramienta de reconocimiento facial elaborada por la empresa Clearview AI ha sido utilizada por miles de organismos encargados de hacer cumplir la ley, pese a haber sido construida extrayendo las fotos de miles de millones de personas de Internet, una intrusión masiva del derecho a la privacidad[85].

43. La vigilancia sistemática de las personas en el espacio público tanto dentro como fuera de Internet, en particular cuando se combina con formas adicionales de analizar y conectar la información obtenida con otras fuentes de datos, constituye una vulneración del derecho a la privacidad y puede tener efectos muy perjudiciales para el disfrute de otros derechos humanos[86]. Puede constituir una amenaza a la libertad de expresión y de reunión pacífica, a la participación y a la democracia, por lo que debería abordarse con la máxima precaución y solo en estricto cumplimiento de los requisitos en materia de derechos humanos. Así debería suceder aunque las actividades vigiladas tengan lugar en público, o en plataformas abiertas de medios sociales, ya que las personas deberían tener un espacio donde no estén expuestas a la observación e intrusión sistemáticas, en particular por parte de las entidades gubernamentales. Como ya ha señalado el Alto Comisionado, la protección del derecho a la privacidad se extiende a los espacios públicos y a la información de acceso público[87]. El Comité de Derechos Humanos ha rechazado la noción de que los datos recogidos en espacios públicos son automáticamente de dominio público y pueden ser de libre acceso[88]. El Tribunal Europeo de Derechos Humanos ha reconocido que la información disponible o perceptible

[82] A/HRC/27/37, párr. 26; A/HRC/39/29, párr. 18; A/HRC/23/40 y A/HRC/23/40/Corr.1, párrs. 65 a 67 y A/69/397, párrs. 53 a 55.

[83] A/HRC/39/29, párr. 19.

[84] Véanse, por ejemplo, https://theintercept.com/2022/06/09/ice-lexisnexis-mass-surveillances y https://www.accessnow.org/cms/assets/uploads/2020/07/Defending-Peaceful-Assembly-Association-Digital-Age.pdf, pág. 25;

[85] Varias autoridades de protección de datos, al determinar que Clearview AI había infringido la ley de protección de datos, impusieron fuertes multas y/o ordenaron que se borraran los datos personales obtenidos, véase https://ico.org.uk/about-the-ico/media-centre/news-and-blogs/2022/05/ico-fines-facial-recognition-database-company-clearview-ai-inc/; véase también 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 y https://www.cnil.fr/fr/reconnaissance-faciale-la-cnil-met-en-demeure-clearview-ai-de-cesser-la-reutilisation-de. Las autoridades de protección de datos sostuvieron que las fuerzas policiales, al utilizar la herramienta, habían violado la ley de protección de datos, véase https://edpb.europa.eu/news/national-news/2021/swedish-dpa-police-unlawfully-used-facial-recognition-app_en y https://edpb.europa.eu/news/national-news/2021/finnish-sa-police-reprimanded-illegal-processing-personal-data-facial_en.

[86] Véase CCPR/C/NGA/CO/2, en el que el Comité de Derechos Humanos expresó su preocupación por la vigilancia de los medios sociales, párr. 40.

[87] A/HRC/39/29, párr. 6.

[88] CCPR/C/COL/CO/7, párr. 32.

públicamente puede entrar en el ámbito del derecho a la privacidad, en particular cuando los datos personales se registran de forma sistemática o permanente[89].

44. Una preocupación particular en materia de vigilancia pública se refiere a la grabación de imágenes fotográficas. La imagen de una persona constituye uno de los atributos fundamentales de su personalidad y revela características únicas que la distinguen de otras personas. El hecho de grabar, analizar y conservar las imágenes faciales de las personas sin su consentimiento constituye una vulneración del derecho a la vida privada. Al desplegar la tecnología de reconocimiento facial en los espacios públicos, que requiere la recopilación y el procesamiento de las imágenes faciales de todas las personas captadas por la cámara, tal vulneración se está produciendo a escala masiva e indiscriminada[90].

45. Además, las medidas de vigilancia pública pueden llevar a la adopción de otras medidas que afectan directamente a personas y comunidades, incluidas medidas coercitivas, y a menudo ambos tipos de medidas se confunden. Se trata, por ejemplo, del aumento de la vigilancia y el control policial de determinados barrios, grupos o personas, lo que a veces da lugar a interrogatorios, arrestos y detenciones de personas. También puede señalarse a algunos grupos y personas como amenazas o riesgos potenciales, por ejemplo, como posibles terroristas o delincuentes, a menudo sin una base sólida, de hecho. Varios Gobiernos utilizan los resultados de diversas medidas de vigilancia pública para identificar a sus críticos o a las personas que no se ajustan a las expectativas sociales, lo que puede dar lugar a actos de acoso, detenciones o a la denegación de servicios esenciales[91].

46. Las operaciones de vigilancia tienden a centrarse de forma desproporcionada en las minorías y las comunidades marginadas[92]. El uso de la inteligencia artificial puede llevar a perpetuar esas pautas de discriminación[93], incluido el uso de tecnologías de reconocimiento facial para la elaboración de perfiles raciales y étnicos[94]. Se ha demostrado que los sistemas de predicción de la actuación policial y de la administración de justicia afectan de forma desproporcionada a las minorías[95].

47. Además, la vigilancia tiene considerables efectos disuasorios en la forma en que las personas ejercen sus derechos, en particular el derecho a la libertad de expresión y de reunión pacífica[96]. Varios estudios ilustran el alcance de estos efectos. Una encuesta realizada en 2015 reveló que el 25 % de los participantes que conocían el caso de Edward Snowden habían

[89] Véase Tribunal Europeo de Derechos Humanos, *Rotaru v. Romania*, párr. 43, sentencia de 4 de mayo de 2000; *Peck v. the United Kingdom*, sentencia de 28 de enero de 2003, párr. 59; *Perry v. the United Kingdom*, sentencia de 17 de julio de 2003, párr. 38 y *Vukota-Bojić v. Switzerland*, sentencia de 18 de enero de 2017, párr. 55.

[90] A/HRC/44/24, párr. 33.

[91] Véase https://privacyinternational.org/explainer/55/social-media-intelligence.

[92] Véanse CERD/C/CHN/CO/14-17 y https://www.brookings.edu/techstream/how-to-reform-police-monitoring-of-social-media.

[93] Véase el documento de sesión sobre la promoción y protección de los derechos humanos y las libertades fundamentales de los africanos y los afrodescendientes frente al uso excesivo de la fuerza y otras violaciones de los derechos humanos por los agentes del orden, párrs. 93 y 94. Puede consultarse en https://www.ohchr.org/es/hr-bodies/hrc/regular-sessions/session47/list-reports.

[94] A/HRC/41/35, párr. 12, y A/HRC/44/57, párr. 39.

[95] Comité para la Eliminación de la Discriminación Racial, recomendación general núm. 36 (2020), relativa a la prevención y la lucha contra la elaboración de perfiles raciales por los agentes del orden, párrs. 33 y 34; A/HRC/44/57, párr. 43; documento de sesión de la Alta Comisionada sobre la promoción y protección de los derechos humanos y las libertades fundamentales de los africanos y los afrodescendientes frente al uso excesivo de la fuerza y otras violaciones de los derechos humanos por los agentes del orden, párr. 93; A/HRC/48/31, párr. 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 y 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, párr. 20; véase, con respecto a las protestas: A/HRC/44/24, párrafos 29, 35 y 52; Tribunal Europeo de Derechos Humanos, *Big Brother Watch and Others v. the United Kingdom*, sentencia de 25 de mayo de 2021 (58170/13, 62322/14 y 24960/15), párr. 495; http://dx.doi.org/10.15779/Z38SS13; https://www.pewresearch.org/wp-content/uploads/sites/9/2015/03/PI_AmericansPrivacyStrategies_0316151.pdf; y https://pen.org/research-resources/global-chilling/.

cambiado el uso que hacían de diversas plataformas tecnológicas[97]. Otro estudio reveló que entre el 34 % y el 61 % de los escritores (dependiendo del país en que se encontraran) habían evitado o al menos considerado evitar ciertos temas en su trabajo por temor a la vigilancia gubernamental[98]. En una encuesta realizada por el Consejo Noruego de Tecnología, el 39 % de los encuestados afirmaron que evitarían utilizar palabras y frases vigiladas por la policía[99]. Como ya ha señalado la Alta Comisionada, estos efectos disuasorios se extienden a las reuniones, incluidas las protestas pacíficas[100].

D. Requisitos en materia de derechos humanos

48. La vigilancia pública conlleva, sin duda, importantes riesgos para los derechos humanos y puede socavar sustancialmente el derecho a la privacidad. Por lo tanto, es esencial que los Estados que recurran a la vigilancia pública evalúen las posibles repercusiones de sus acciones en los derechos humanos y velen estrictamente por el cumplimiento del derecho internacional de los derechos humanos, que exige que cualquier interferencia o restricción de ese tipo esté basada en el derecho, que sea necesaria para alcanzar un fin legítimo y que sea proporcional. Las actuales medidas de vigilancia pública no suelen cumplir esos requisitos.

49. Legalidad: a pesar de las repercusiones de gran alcance de las diversas formas de vigilancia pública, en muchos países faltan marcos legales adecuados aplicables. Con frecuencia no existen leyes de protección de datos o, de existir, son inadecuadas o prevén amplias excepciones para los servicios de aplicación de la ley y de inteligencia[101]. Además, las leyes generales sobre la privacidad de los datos a menudo no proporcionan una orientación detallada ni garantizan limitaciones adecuadas al uso de herramientas de vigilancia específicas. A este respecto, se necesitan instrumentos jurídicos específicos, en particular para la vigilancia realizada en el contexto de la aplicación de la ley y la seguridad nacional[102]. Las leyes y los reglamentos deben establecer limitaciones claras y estrictas al acceso y la fusión de las bases de datos gubernamentales. Lamentablemente, hay pocos indicios de que los Estados estén avanzando hacia la regulación del uso de las técnicas, tecnologías y herramientas de inteligencia de los medios sociales. Aunque las entidades de regulación y de legislación a nivel local, nacional y regional se esfuerzan cada vez más por regular el reconocimiento facial y otras herramientas de vigilancia biométrica[103], la mayoría de las autoridades siguen operando con sistemas de vigilancia biométrica aunque no exista una base legal que sustente dicha actividad.

50. Fines legítimos: no cabe duda de que la vigilancia pública puede ser útil para una gran variedad de fines legítimos, por ejemplo, la protección de la vida o la integridad física de las personas y la seguridad de infraestructuras de importancia fundamental. Lamentablemente, la vigilancia pública suele realizarse con fines que no están permitidos por el derecho internacional de los derechos humanos. Se ha utilizado indebidamente, entre otras cosas, para identificar y rastrear a los disidentes políticos, para realizar perfiles raciales y étnicos, para atacar a las comunidades de personas lesbianas, gais, bisexuales, transgénero e intersexuales y para determinar si las personas se adaptaban a las normas sociales.

---

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

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

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

100 A/HRC/44/24, párrs. 35 y 53.

101 A/HRC/39/29, párr. 34.

102 Los requisitos mínimos aplicables a las leyes de vigilancia ya han sido descritos en informes del Alto Comisionado: véanse A/HRC/27/37 y A/HRC/39/29.

103 Véanse la propuesta de Ley de Inteligencia Artificial de la Unión Europea; las Directrices 05/2022 del Comité Europeo de Protección de Datos sobre el uso de la tecnología de reconocimiento facial en el ámbito de la aplicación de la ley, versión 1.0, que pueden consultarse en https://edpb.europa.eu/our-work-tools/documents/public-consultations/2022/guidelines-052022-use-facial-recognition_es; véanse también la legislación del Estado de Washington, Estados Unidos de América, relativa al uso del reconocimiento facial, que puede consultarse en https://www.securityindustry.org/report/washington-facial-recognition-law-faq/ y las prohibiciones y moratorias adoptadas por las legislaturas locales y regionales.

51. Necesidad y proporcionalidad: aunque la vigilancia pública puede ser permisible, los Estados deben demostrar que las medidas son tanto necesarias como proporcionadas. Sin embargo, la eficacia de las medidas de vigilancia es a menudo dudosa y plantea serias dudas sobre su necesidad o proporcionalidad. Los datos sobre los efectos de la videovigilancia en la seguridad y la prevención de la delincuencia son contradictorios. La mayoría de los estudios apuntan, como mucho, a una modesta reducción de algunos tipos de delitos (como los relacionados con los vehículos y la propiedad) en las zonas controladas por las cámaras de vigilancia, mientras que, en general, los delitos violentos no parecen verse afectados por la presencia de cámaras de vigilancia[104]. Además, una comparación entre numerosos municipios de diversas jurisdicciones muestra una correlación escasa o nula entre el número de cámaras de vigilancia pública y la delincuencia o la seguridad en todo un municipio[105]. En cuanto a la detección automatizada de amenazas, un sistema ampliamente utilizado por las fuerzas policiales para detectar disparos con el fin de identificar posibles escenas de crímenes, se ha demostrado que identifica erróneamente los sonidos como disparos en el 89 % de los casos[106]. Por último, muchos departamentos de policía que habían solicitado utilizar los servicios de actividades policiales predictivas pusieron fin a esas colaboraciones, alegando que su utilidad era limitada[107].

52. La vigilancia general de las personas en los espacios públicos es casi siempre desproporcionada. Las medidas de vigilancia en los espacios públicos deberían ser selectivas y responder a un fin legítimo concreto, como evitar una amenaza específica para la seguridad pública cuya importancia sea tal que compense sus efectos negativos en los derechos humanos. Tales medidas deben ser limitadas y centrarse en lugares y momentos concretos, por ejemplo, cuando haya pruebas que apunten a la probabilidad de que se produzca un delito o de que se planteen amenazas a la seguridad pública. Tampoco deberían permitirse opciones con menor invasión de la privacidad. Es esencial imponer limitaciones estrictas a la duración del almacenamiento de los datos capturados y a los fines asociados para los que se van a utilizar dichos datos. Concretamente, los sistemas de vigilancia biométrica a distancia suscitan gran preocupación en cuanto a su proporcionalidad, dado su carácter altamente invasivo y sus amplias repercusiones en un gran número de personas[108]. En este contexto, la Alta Comisionada ha acogido con satisfacción los recientes esfuerzos por limitar o prohibir el uso de las tecnologías de reconocimiento biométrico a distancia y ha pedido una moratoria para su uso en los espacios públicos, al menos hasta que se establezcan salvaguardias importantes[109]. En caso de utilizarse, estas tecnologías solo deberían desplegarse para responder a situaciones como delitos graves y amenazas serias a la seguridad pública, si se pueden excluir los efectos discriminatorios y se someten a una supervisión adecuada y eficaz, que incluya una autorización independiente y auditorías periódicas independientes de los derechos humanos.

IV. Conclusiones y recomendaciones

53. **El presente informe ofrece una instantánea de varias esferas fundamentales en las que el derecho a la privacidad en el ámbito digital se ve actualmente amenazado. La rápida adopción de las tecnologías digitales plantea una serie de dificultades adicionales que no están abarcadas en este informe, pero a las que cabría prestarles mayor atención. Por ejemplo, la vigilancia masiva encubierta, analizada en anteriores informes del Alto Comisionado[110], sigue siendo un problema grave. Tampoco se comprenden cabalmente**

[104] Véanse https://academicworks.cuny.edu/jj_pubs/256/ y https://doi.org/10.1080/01924036.2021.1879885.

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

[106] Véanse https://www.macarthurjustice.org/blog/shotspotter-is-a-failure-whats-next/ y 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] Véase 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, párrs. 26 y 27 y A/HRC/44/24, párrs. 33 a 38.

[109] A/HRC/48/31, párrs. 27 y 59 d).

[110] Véanse A/HRC/27/37 y A/HRC/39/29.

las consecuencias de los sistemas de identidad digital en los derechos humanos ni los diversos casos en que se utiliza la biometría, pese a que ambas tecnologías están desplegándose en todo el mundo. El seguimiento omnipresente de los usuarios de Internet por parte de innumerables empresas, como anunciantes, instituciones financieras y corredores de datos, requiere mucha más atención en los foros internacionales de derechos humanos. La pandemia de enfermedad por coronavirus (COVID-19) y la vertiginosa variedad de respuestas digitales a la misma podrían ser objeto de un informe en sí mismo. Hay que explorar y comprender más profundamente las formas en que las violaciones y los abusos de la privacidad afectan a las personas marginadas y en situación de vulnerabilidad. Debería hacerse un seguimiento de cerca de los fenómenos emergentes, como el impulso por adoptar de forma generalizada las tecnologías de cadenas de bloques y de realidad aumentada y virtual y el desarrollo de una neurotecnología cada vez más potente.

54. **Sin embargo, aun centrándose en unos pocos acontecimientos de fundamental importancia, el presente informe describe un panorama preocupante acerca de la forma en que el derecho a la privacidad se está viendo constantemente socavado en la era digital. Este análisis no debería entenderse como una negación de los enormes beneficios que las tecnologías digitales están aportando a las sociedades; al contrario, las sociedades deberían abrazar plenamente el progreso tecnológico que empodera a las personas, mejora sus vidas, fortalece la justicia e impulsa la productividad. Pero las múltiples formas en que la vigilancia generalizada amenaza los derechos humanos y el estado de derecho y puede erosionar unas democracias pujantes y pluralistas son profundamente alarmantes. Las características de las modernas tecnologías digitales en red pueden convertirlas en formidables herramientas de control y opresión: cada acción en el espacio digital deja un rastro de datos; la tecnología de computación en la nube facilita la fusión y el análisis de fuentes de datos dispares; la automatización aumenta el posible alcance y eficacia de la vigilancia, y la vigilancia digital es difícil de observar por quienes están siendo objeto de ella. Además, la vigilancia digital está íntimamente ligada a la falta de transparencia en general. El público suele saber muy poco sobre las diversas prácticas de vigilancia que se vinculan íntimamente a muchos aspectos de la vida. Con demasiada frecuencia, los Gobiernos no facilitan información fiable sobre el tipo de sistemas de vigilancia que utilizan y con qué fines, y a menudo no presentan pruebas sobre la eficacia de esos sistemas.**

55. **Las medidas de vigilancia incompatibles con el derecho internacional de los derechos humanos están ya muy extendidas. Incluso cuando la vigilancia tiene fines legítimos, la infraestructura subyacente puede ser fácilmente reutilizada, a menudo con fines para los que no estaba originalmente pensada (lo que se ha dado en llamar "desviación de uso") o a raíz de cambios en el panorama político. Quienes toman las decisiones deben tener esto en cuenta cuando prevean nuevos proyectos que aumenten las facultades de recolección y análisis de datos personales. Se necesita urgentemente celebrar debates públicos sobre los límites de la vigilancia. Sin un debate público dinámico, las sociedades corren el riesgo de encaminarse ciegamente hacia sistemas de vigilancia que permiten a quienes detentan el poder ejercer niveles de control sin precedentes en la vida cotidiana.**

56. **Teniendo presente lo que antecede, el ACNUDH recomienda a los Estados que:**

a) Se aseguren de que cualquier vulneración del derecho a la privacidad, incluida la piratería informática, las restricciones al acceso y el uso de la tecnología de cifrado y la vigilancia del público, cumpla con el derecho internacional de los derechos humanos, incluidos los principios de legalidad, fin legítimo, necesidad y proporcionalidad y no discriminación, y no menoscabe la esencia de ese derecho;

b) Demuestren la diligencia debida en materia de derechos humanos de forma sistemática —incluyendo evaluaciones periódicas de las repercusiones en los derechos humanos— cuando elaboren, desarrollen, compren, desplieguen y pongan en funcionamiento sistemas de vigilancia;

c) Tengan en cuenta, al ejercer la diligencia debida en materia de derechos humanos y evaluar la necesidad y proporcionalidad de los nuevos sistemas y facultades de vigilancia, la totalidad del entorno jurídico y tecnológico en el que están o estarían integrados dichos sistemas o facultades; los Estados también deberían tener en cuenta los riesgos de abuso, de desviación de uso y de reutilización, incluidos los riesgos derivados de futuros cambios políticos;

d) Aprueben y apliquen efectivamente, a través de autoridades independientes, imparciales y dotadas de buenos recursos, una legislación sobre privacidad de datos para los sectores público y privado que cumpla con el derecho internacional de los derechos humanos, incluyendo salvaguardias, supervisión y recursos para proteger efectivamente el derecho a la privacidad;

e) Adopten medidas inmediatas para aumentar de forma efectiva la transparencia del uso de las tecnologías de vigilancia, entre otras cosas informando adecuadamente al público y a las personas y comunidades afectadas y proporcionando periódicamente datos pertinentes para que el público pueda evaluar su eficacia y sus efectos en los derechos humanos;

f) Promuevan el debate público sobre el uso de las tecnologías de vigilancia y garanticen una participación significativa de todas las partes interesadas en las decisiones sobre la adquisición, transferencia, venta, desarrollo, despliegue y uso de las tecnologías de vigilancia, incluida la elaboración de políticas públicas y su aplicación;

g) Apliquen moratorias a la venta y el uso nacional y transnacional de sistemas de vigilancia, como las herramientas de piratería informática y los sistemas biométricos que puedan utilizarse para la identificación o clasificación de personas en lugares públicos, hasta que se establezcan salvaguardias adecuadas para proteger los derechos humanos; tales salvaguardias deberían incluir medidas de control interno y de las exportaciones, de acuerdo con las recomendaciones formuladas en este documento y en informes anteriores al Consejo de Derechos Humanos[111];

h) Garanticen que las víctimas de violaciones de derechos humanos y abusos relacionados con el uso de sistemas de vigilancia tengan acceso a recursos efectivos.

57. **En relación con las cuestiones específicas planteadas en el presente informe, el ACNUDH recomienda a los Estados que:**

Piratería informática

a) Se aseguren de que las autoridades empleen la piratería informática de dispositivos personales solo como último recurso, con la única finalidad de prevenir o investigar un acto específico que suponga una amenaza grave para la seguridad nacional o un delito grave específico, y que tal medida esté dirigida concretamente a la persona sospechosa de haber cometido dichos actos; estas medidas deberían estar sujetas a una estricta supervisión independiente y requerir la aprobación previa de un órgano judicial;

Cifrado

b) Promuevan y protejan el cifrado de alta seguridad y eviten todas las restricciones directas, o indirectas, generales e indiscriminadas del uso del cifrado, como las prohibiciones, la criminalización, la imposición de normas de cifrado mínimas o de requisitos de escaneo general obligatorio del lado del cliente; solo debería interferirse en el cifrado de las comunicaciones privadas de las personas cuando así lo autorice un órgano judicial independiente y en función de cada caso, y solo debería aplicarse esa medida a las personas si es estrictamente necesario para la investigación de delitos graves o la prevención de delitos graves o en caso de amenazas graves para la seguridad pública o la seguridad nacional;

[111] Véanse A/HRC/27/37, A/HRC/39/29, A/HRC/44/24 y A/HRC/48/31.

Vigilancia de los espacios públicos y control de las exportaciones de tecnología de vigilancia

c) Aprueben marcos jurídicos adecuados que regulen la recopilación, el análisis y el intercambio de información de los medios sociales y que definan claramente los motivos permitidos, los requisitos previos, los procedimientos de autorización y los mecanismos de supervisión adecuados;

d) Eviten la vigilancia generalizada de los espacios públicos que afecte a la privacidad y garanticen que todas las medidas de vigilancia pública sean estrictamente necesarias y proporcionadas para el logro de fines legítimos importantes, entre otras formas, limitando rigurosamente su ubicación y tiempo, así como la duración del almacenamiento de los datos, la finalidad de su uso y el acceso a los mismos; los sistemas de reconocimiento biométrico solo deberían utilizarse en los espacios públicos para prevenir o investigar delitos graves o amenazas serias a la seguridad pública y siempre que se apliquen todos los requisitos del derecho internacional de los derechos humanos con respecto a los espacios públicos[112];

e) Establezcan regímenes sólidos y bien adaptados de control de las exportaciones aplicables a las tecnologías de vigilancia, cuyo uso conlleva grandes riesgos para el disfrute de los derechos humanos; los Estados deberían exigir evaluaciones transparentes de los efectos en los derechos humanos que tengan en cuenta las capacidades de las tecnologías en cuestión, así como la situación en el Estado receptor, incluido el cumplimiento de los derechos humanos, la adhesión al estado de derecho, la existencia y aplicación efectiva de leyes aplicables que regulen las actividades de vigilancia y la existencia de mecanismos de supervisión independientes;

f) Velen por que las asociaciones público-privadas, en el suministro y el uso de tecnologías de vigilancia, defiendan e incorporen expresamente las normas de derechos humanos y no den lugar a una renuncia de los Gobiernos a sus responsabilidades en materia de derechos humanos.

[112] Incluidos los requisitos establecidos en A/HRC/44/24, párr. 53 j) (i a v) y A/HRC/48/31, párr. 59 d).