Naciones Unidas A/HRC/27/37

Asamblea General

Distr. general
30 de junio de 2014
Español
Original: inglés

Consejo de Derechos Humanos
27º período de sesiones
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 su resolución 68/167, la Asamblea General solicitó a la Alta Comisionada de las Naciones Unidas para los Derechos Humanos que presentara al Consejo de Derechos Humanos en su 27º período de sesiones y a la Asamblea General en su sexagésimo noveno período de sesiones un informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala, que incluyera opiniones y recomendaciones, para que lo examinaran los Estados Miembros. El presente informe se ha preparado en cumplimiento de esa solicitud. La Oficina del Alto Comisionado también presentará el informe a la Asamblea General en su sexagésimo noveno período de sesiones, de conformidad con la solicitud de la Asamblea.

GE.14-06874 (S) 050814 060814
1406874

Índice

I. Introducción

1. Las tecnologías digitales de la comunicación, como Internet, los teléfonos inteligentes y los dispositivos con acceso a Wi-Fi, forman ya parte de la vida cotidiana. Al mejorar espectacularmente el acceso a la información y la comunicación en tiempo real, las innovaciones en la tecnología de las comunicaciones han impulsado la libertad de expresión, facilitado el debate a nivel mundial y fomentado la participación democrática. Además, estas potentes tecnologías pueden mejorar el disfrute de los derechos humanos dando un mayor eco a la voz de los defensores de los derechos humanos y proporcionándoles nuevas herramientas para documentar y denunciar las violaciones. Como la vida contemporánea tiene lugar cada vez más en línea, la omnipresencia de Internet es un hecho y su utilización con fines íntimos va en aumento.

2. En la era digital, las tecnologías de la comunicación también han aumentado la capacidad de los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos. Como ha señalado el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, los avances tecnológicos entrañan que la eficacia de la vigilancia realizada por el Estado ya no se ve limitada por su magnitud o duración. La disminución de los costos de tecnología y almacenamiento de datos ha eliminado los inconvenientes financieros o prácticos de la vigilancia. El Estado no había tenido nunca la capacidad de que dispone actualmente para realizar actividades de vigilancia simultáneas, invasivas, con objetivos precisos y a gran escala[1]. Es decir, las plataformas tecnológicas de las que depende crecientemente la vida política, económica y social a nivel mundial no solo son vulnerables a la vigilancia en masa, sino que en realidad pueden facilitarla.

3. La divulgación de políticas y prácticas que se aprovechan de la vulnerabilidad de las tecnologías digitales de la comunicación a la vigilancia electrónica y la interceptación en países de todo el mundo ha suscitado honda preocupación. Los ejemplos de actividades de vigilancia digital declaradas y encubiertas en jurisdicciones de todo el mundo se han multiplicado, y la vigilancia en masa por parte de los gobiernos se ha revelado como un hábito peligroso, y no una medida excepcional. Según se ha informado, distintos gobiernos han amenazado con prohibir los servicios de las empresas de telecomunicaciones y de dispositivos inalámbricos a menos que les permitieran un acceso directo al tráfico de las comunicaciones, han intervenido los cables de fibra óptica con fines de vigilancia y han obligado sistemáticamente a las empresas a revelarles información a granel sobre sus clientes y empleados. Además, algunos gobiernos han utilizado supuestamente la vigilancia de las redes de telecomunicaciones para controlar a los miembros de la oposición o a los disidentes políticos. Según ciertas informaciones, las autoridades de algunos Estados registran sistemáticamente todas las conversaciones telefónicas y las conservan para analizarlas, mientras que los gobiernos organizadores de eventos internacionales han vigilado las comunicaciones de los participantes. Las autoridades de un Estado presuntamente exigen que todas las computadoras personales vendidas en el país estén equipadas con un software de filtrado que puede tener otras capacidades de vigilancia. Incluso los grupos no estatales están adquiriendo, según se ha informado, sofisticados equipos de vigilancia digital. Las tecnologías de vigilancia en masa están entrando ahora en el mercado mundial, lo cual aumenta el riesgo de que la vigilancia digital escape a los controles gubernamentales.

4. La preocupación ha aumentado a raíz de las revelaciones publicadas en 2013 y 2014 de que, conjuntamente, el Organismo de Seguridad Nacional de los Estados Unidos de

[1] A/HRC/23/40, párr. 33.

América y el Cuartel General de Comunicaciones del Reino Unido de Gran Bretaña e Irlanda del Norte han creado tecnologías que permiten acceder a gran parte del tráfico mundial en Internet, los registros de llamadas en los Estados Unidos, las libretas de contactos electrónicos de los particulares y enormes volúmenes de otros contenidos digitales de comunicación. Esas tecnologías se han puesto en práctica, según la información publicada, mediante una red transnacional que se basa en las relaciones de inteligencia estratégica de los gobiernos, el control regulatorio de las empresas privadas y contratos comerciales.

5. A raíz de la preocupación expresada por los Estados Miembros y otras partes interesadas por las repercusiones negativas de esas prácticas de vigilancia para los derechos humanos, en diciembre de 2013 la Asamblea General aprobó, sin votación, su resolución 68/167, sobre el derecho a la privacidad en la era digital. En la resolución, que fue copatrocinada por 57 Estados Miembros, la Asamblea afirmó que los derechos de las personas también debían estar protegidos en Internet, y exhortó a todos los Estados a que respetaran y protegiesen el derecho a la privacidad en las comunicaciones digitales. Exhortó además a todos los Estados a que examinaran sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, e hizo hincapié en la necesidad de que los Estados velasen por que se dé cumplimiento pleno y efectivo a sus obligaciones en virtud del derecho internacional de los derechos humanos.

6. También en la resolución 68/167, la Asamblea General solicitó a la Alta Comisionada de las Naciones Unidas para los Derechos Humanos que presentase al Consejo de Derechos Humanos en su 27º período de sesiones y a la Asamblea General en su sexagésimo noveno período de sesiones un informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala, que incluyera opiniones y recomendaciones, para que lo examinasen los Estados Miembros. El presente informe se ha preparado en cumplimiento de esa solicitud. Conforme a lo dispuesto en la resolución 68/167, la Oficina del Alto Comisionado (ACNUDH) también presentará el informe a la Asamblea en su sexagésimo noveno período de sesiones.

II. Antecedentes y metodología

7. Teniendo presente la resolución 68/167, el ACNUDH participó en una serie de eventos y reunió información de muy diversas fuentes. El 24 de febrero de 2014, la Alta Comisionada pronunció el discurso principal de un seminario de expertos sobre "El derecho a la privacidad en la era digital" copatrocinado por Alemania, Austria, el Brasil, Liechtenstein, México, Noruega y Suiza y organizado por la Geneva Academy on International Humanitarian Law and Human Rights.

8. Entre noviembre de 2013 y marzo de 2014, el ACNUDH colaboró con la Universidad de las Naciones Unidas en un proyecto de investigación sobre la aplicación del derecho internacional de los derechos humanos a los regímenes nacionales de control de la vigilancia digital por parte del gobierno. El ACNUDH agradece a la Universidad y reconoce su importante contribución sustantiva a la preparación del presente informe mediante el proyecto de investigación.

9. En el marco de una consulta abierta, el 27 de febrero de 2014, el ACNUDH envió un cuestionario a los Estados Miembros por conducto de sus Misiones Permanentes en Ginebra y en Nueva York; a las organizaciones internacionales y regionales; a las instituciones nacionales de derechos humanos; a las organizaciones no gubernamentales

(ONG); y a entidades empresariales. En su cuestionario, el ACNUDH solicitó aportes sobre las cuestiones abordadas por la Asamblea General en su resolución 68/167. También se creó una página web especial del ACNUDH para publicar el cuestionario y todas las contribuciones y brindar más oportunidades de realizar aportes. Se recibieron contribuciones de 29 Estados Miembros de todas las regiones, 5 organizaciones internacionales o regionales, 3 instituciones nacionales de derechos humanos, 16 ONG y 2 iniciativas del sector privado[2].

10. En muchas de las contribuciones se expusieron detalladamente los marcos legislativos nacionales existentes y otras medidas adoptadas para asegurar el respeto y la protección del derecho a la privacidad en la era digital, así como las iniciativas emprendidas para establecer y poner en práctica garantías procesales y una supervisión efectiva. En algunas de las contribuciones se expusieron los obstáculos encontrados al tratar de hacer efectivo el derecho a la privacidad en la era digital y se sugirieron, entre otras, las siguientes iniciativas a nivel internacional: alentar al Comité de Derechos Humanos a actualizar sus observaciones generales pertinentes, en particular sobre el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos; y la creación por el Consejo de Derechos Humanos de un mandato de los procedimientos especiales sobre el derecho a la privacidad y/o la participación de los titulares de mandatos de los procedimientos especiales pertinentes en iniciativas conjuntas o individuales para abordar las cuestiones relacionadas con el derecho a la privacidad en el contexto de la vigilancia digital y para proporcionar orientación sobre las buenas prácticas.

11. De conformidad con la solicitud formulada en la resolución 68/167 de la Asamblea General, en el presente informe se ofrecen reflexiones y recomendaciones basadas en una evaluación de la información disponible en el momento de su preparación; también se ha utilizado la gran cantidad de material en que se basaron las diversas contribuciones recibidas.

III. Cuestiones relacionadas con el derecho a la privacidad en la era digital

12. Como recuerda la Asamblea General en su resolución 68/167, el derecho internacional de los derechos humanos proporciona un marco universal para evaluar toda injerencia en los derechos individuales a la privacidad. El artículo 12 de la Declaración Universal de Derechos Humanos establece que "nadie será objeto de injerencias arbitrarias en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques a su honra o a su reputación. Toda persona tiene derecho a la protección de la ley contra tales injerencias o ataques". El Pacto Internacional de Derechos Civiles y Políticos, ratificado hasta la fecha por 167 Estados, establece en su artículo 17 que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia, ni de ataques ilegales a su honra y reputación". Afirma además que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques".

13. Otros instrumentos internacionales de derechos humanos contienen disposiciones similares. La legislación a nivel regional y nacional refleja también el derecho de todas las personas al respeto de su vida privada y familiar, su domicilio y su correspondencia, o su derecho al reconocimiento y respeto de su dignidad, su integridad personal o su reputación. Es decir, existe un reconocimiento universal de la importancia fundamental, y la pertinencia

[2] Pueden consultarse todas las contribuciones en: www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx.

perdurable, del derecho a la privacidad y de la necesidad de asegurar su protección, tanto en la legislación como en la práctica.

14. Aunque el mandato del presente informe se centró en el derecho a la privacidad, cabe subrayar que otros derechos también pueden verse afectados por la vigilancia en masa, la interceptación de las comunicaciones digitales y la recopilación de datos personales, por ejemplo el derecho a la libertad de opinión y de expresión, y a buscar, recibir y difundir información; el derecho a la libertad de reunión y de asociación pacíficas; y el derecho a la vida familiar. Todos esos derechos están estrechamente vinculados con el derecho a la privacidad y, cada vez más, se ejercen a través de los medios digitales. Otros derechos, como el derecho a la salud, también pueden verse afectados por las prácticas de vigilancia digital, por ejemplo cuando alguien se abstiene de buscar o comunicar información controvertida relacionada con la salud por temor a perder su anonimato. Hay indicios fidedignos de que las tecnologías digitales han servido para reunir información que ha propiciado actos de tortura y otros malos tratos. La información publicada indica también que los metadatos obtenidos mediante la vigilancia electrónica han sido analizados para determinar la ubicación de objetivos de ataques letales con drones. Esos ataques siguen suscitando gran preocupación en cuanto a su compatibilidad con el derecho internacional de los derechos humanos y con el derecho internacional humanitario, y a la rendición de cuentas por toda violación de los mismos. Los vínculos entre la vigilancia en masa y estos otros efectos en los derechos humanos, aunque quedan fuera del alcance del presente informe, deben ser objeto de un mayor estudio.

A. El derecho a la protección contra las injerencias arbitrarias o ilegales en la vida privada, la familia, el domicilio o la correspondencia

15. Varias contribuciones destacaron que, cuando se realiza en cumplimiento de la ley, incluido el derecho internacional de los derechos humanos, la vigilancia de las comunicaciones electrónicas puede ser una medida necesaria y eficaz para los fines legítimos de las fuerzas del orden o los servicios de inteligencia. Sin embargo, las revelaciones sobre la vigilancia digital en masa plantearon la duda de si esas medidas son compatibles con las normas jurídicas internacionales y si se precisan salvaguardias más sólidas para impedir las violaciones de los derechos humanos. En concreto, las medidas de vigilancia no deben injerirse arbitraria o ilegalmente en la privacidad, la familia, el domicilio o la correspondencia de un individuo; los gobiernos deben tomar medidas específicas para garantizar la protección de la ley contra tales injerencias.

16. Un examen de las diversas contribuciones recibidas pone de manifiesto que para disipar esas dudas es preciso evaluar qué constituye una injerencia en la privacidad en el contexto de las comunicaciones digitales; qué significa la expresión "arbitrarias e ilegales"; y a quién asisten los derechos protegidos por el derecho internacional de los derechos humanos, y dónde. En las siguientes secciones se abordan las cuestiones que se destacaron en diversas contribuciones.

1. Las injerencias en la privacidad

17. Distintos órganos de tratados internacionales y regionales de derechos humanos, tribunales, comisiones y expertos independientes han proporcionado orientaciones pertinentes en relación con el alcance y el contenido del derecho a la privacidad, así como con el significado de las "injerencias" en la privacidad de un individuo. En su Observación general Nº 16, el Comité de Derechos Humanos subrayó que el cumplimiento del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos exige que la integridad y el carácter confidencial de la correspondencia estén protegidos *de jure* y *de facto*.

"La correspondencia debe ser entregada al destinatario sin ser interceptada ni abierta o leída de otro modo."[3]

18. Algunas voces han señalado que, al enviar e intercambiar información personal por medios electrónicos, los usuarios de Internet se avienen conscientemente a entregar voluntariamente información sobre sí mismos y sus relaciones a cambio del acceso digital a bienes, servicios e información. No obstante, cabe dudar seriamente sobre el grado en que los consumidores saben realmente qué datos están compartiendo, cómo y con quién, y qué uso se hará de ellos. Según un informe, "una realidad de los macrodatos es que, una vez que se recopilan los datos, puede ser muy difícil mantener su anonimato. Si bien se están realizando estudios prometedores sobre la posibilidad de censurar la información personal identificable en los grandes conjuntos de datos, se están dedicando muchos más esfuerzos a identificar la procedencia de los datos aparentemente 'anónimos'. La inversión colectiva en la capacidad de exploración de datos es mucho mayor que la inversión en tecnologías que mejoren la privacidad". Por otra parte, los autores del informe señalaron que "centrarse en el control de la recolección y conservación de datos personales, si bien es importante, podría ser ya insuficiente para proteger la privacidad personal", en parte porque "los macrodatos permiten nuevos usos no evidentes e inesperadamente potentes de los datos"[4].

19. En la misma línea, se ha sugerido que la interceptación o la recopilación de datos acerca de una comunicación, en contraposición al contenido de la comunicación, no constituyen en sí mismas una injerencia en la vida privada. Desde el punto de vista del derecho a la privacidad, esa distinción no es convincente. La agregación de la información comúnmente conocida como "metadatos" puede incluso dar una mejor idea del comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona que la información obtenida accediendo al contenido de una comunicación privada. Como observó recientemente el Tribunal de Justicia de la Unión Europea, los metadatos de las comunicaciones, "considerados en su conjunto, pueden permitir extraer conclusiones muy precisas sobre la vida privada de las personas cuyos datos se han conservado"[5]. El reconocimiento de esa evolución ha dado lugar a iniciativas para reformar las políticas y prácticas existentes a fin de asegurar una mayor protección de la privacidad.

20. Por todo ello, toda captura de datos de las comunicaciones es potencialmente una injerencia en la vida privada y, además, la recopilación y conservación de datos de las comunicaciones equivale a una injerencia en la vida privada, independientemente de si posteriormente se consultan o utilizan esos datos. Incluso la mera posibilidad de que pueda captarse información de las comunicaciones crea una injerencia en la vida privada[6] y puede tener un efecto negativo en derechos como los relativos a la libertad de expresión y de asociación. La mera existencia de un programa de vigilancia en masa crea, por lo tanto, una injerencia en la privacidad. Incumbiría al Estado demostrar que tal injerencia no es arbitraria ni ilegal.

---

[3] *Documentos Oficiales de la Asamblea General, cuadragésimo tercer período de sesiones, Suplemento Nº 40* (A/43/40), anexo VI, párr. 8.

[4] Oficina Ejecutiva del Presidente de los Estados Unidos, "Big Data: Seizing Opportunities, Preserving Values", mayo de 2014 (disponible en www.whitehouse.gov/sites/default/files/docs/big_data_privacy_report_may_1_2014.pdf), pág. 54.

[5] Tribunal de Justicia de la Unión Europea, sentencia en los asuntos acumulados C-293/12 y C-594/12, *Digital Rights Ireland y Seitlinger y otros*, sentencia de 8 de abril de 2014, párrs. 26, 27 y 37. Véase también Oficina Ejecutiva del Presidente, "Big Data and Privacy: A Technological Perspective" (disponible en www.whitehouse.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf), pág. 19.

[6] Véase Tribunal Europeo de Derechos Humanos, *Weber and Saravia v. Germany*, párr. 78; *Malone v. UK*, párr. 64.

2. ¿Qué se entiende por "arbitrarias" o "ilegales"?

21. Las injerencias en el derecho de una persona a la privacidad solo están permitidas por el derecho internacional de los derechos humanos si no son arbitrarias ni ilegales. En su Observación general Nº 16, el Comité de Derechos Humanos explicó que el término "ilegales" significaba que no puede producirse injerencia alguna, "salvo en los casos previstos por la ley. La injerencia autorizada por los Estados solo puede tener lugar en virtud de la ley, que a su vez debe conformarse a las disposiciones, propósitos y objetivos del Pacto"[7]. Es decir, las injerencias permitidas por la legislación nacional pueden, no obstante, ser "ilegales" si dicha legislación nacional es contraria a las disposiciones del Pacto Internacional de Derechos Civiles y Políticos. La expresión "injerencias arbitrarias" puede hacerse extensiva también a las injerencias previstas en la ley. El Comité explicó que, con la introducción del concepto de arbitrariedad, "se pretende garantizar que incluso cualquier injerencia prevista en la ley esté en consonancia con las disposiciones, los propósitos y los objetivos del Pacto y sea, en todo caso, razonable en las circunstancias particulares del caso"[8]. El Comité interpretó el concepto de razonabilidad en el sentido de que "cualquier injerencia en la vida privada debe ser proporcional al propósito perseguido y necesaria en las circunstancias particulares del caso"[9].

22. A diferencia de otras disposiciones del Pacto, el artículo 17 no incluye una cláusula con limitaciones explícitas. No obstante, pueden extraerse orientaciones sobre el significado de la expresión calificativa "arbitrarias o ilegales" de los Principios de Siracusa sobre la limitación o suspensión de disposiciones del Pacto Internacional de Derechos Civiles y Políticos[10]; la práctica del Comité de Derechos Humanos reflejada en sus Observaciones generales, en particular las N^{os} 16, 27, 29, 34 y 31, sus conclusiones sobre las comunicaciones individuales[11] y sus observaciones finales[12]; la jurisprudencia regional y nacional[13]; y las opiniones de expertos independientes[14]. Por ejemplo, en su Observación general Nº 31, sobre la índole de la obligación jurídica general impuesta a los Estados partes en el Pacto, el Comité de Derechos Humanos señala que los Estados partes deben abstenerse de violar los derechos reconocidos por el Pacto y que "cualesquiera restricciones a cualquiera de esos derechos debe ser permisible de conformidad con las disposiciones pertinentes del Pacto. Cuando se introducen restricciones, los Estados deben demostrar su necesidad y adoptar únicamente las medidas que resulten proporcionales a la consecución de los legítimos objetivos para lograr una protección constante y eficaz de los derechos del Pacto"[15]. El Comité subrayó además que "en ningún caso se deben aplicar las restricciones o invocarse de una manera que menoscabe la esencia de un derecho del Pacto".

23. Estas fuentes autorizadas apuntan a los principios generales de legalidad, necesidad y proporcionalidad, cuya importancia también se destacó en muchas de las contribuciones recibidas. Para comenzar, toda limitación a los derechos a la privacidad reflejados en el

[7] *Documentos Oficiales de la Asamblea General* (véase la nota 3), párr. 3.
[8] *Ibid.*, párr. 4.
[9] Comunicación Nº 488/1992, *Toonan c. Australia*, párr. 8.3; véanse también las comunicaciones Nº 903/1999, párr. 7.3, y Nº 1482/2006, párrs. 10.1 y 10.2.
[10] Véase E/CN.4/1985/4, anexo.
[11] Por ejemplo, la comunicación Nº 903/1999, 2004, *Van Hulst c. los Países Bajos*.
[12] CCPR/C/USA/CO/4.
[13] Por ejemplo, Tribunal Europeo de Derechos Humanos, *Uzun v. Germany*, 2 de septiembre de 2010, y *Weber and Soravia v. Germany*, párr. 4; y Corte Interamericana de Derechos Humanos, *Escher vs. Brasil*, sentencia, 20 de noviembre de 2009.
[14] Véase A/HRC/13/37 y A/HRC/23/40. Véanse también los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, disponibles en https://es.necessaryandproportionate.org/text.
[15] CCPR/C/21/Rev.1/Add.13, párr. 6.

artículo 17 debe estar prevista en la ley, y la ley debe ser lo suficientemente accesible, clara y precisa para que una persona pueda leerla y saber quién está autorizado a realizar actividades de vigilancia de datos y en qué circunstancias. La limitación debe ser necesaria para alcanzar un objetivo legítimo, así como proporcional al objetivo y la opción menos perturbadora de las disponibles[16]. Por otra parte, debe demostrarse que la limitación impuesta al derecho (una injerencia en la vida privada, por ejemplo, con el fin de proteger la seguridad nacional o el derecho a la vida de otras personas) tiene posibilidades de alcanzar ese objetivo. Es responsabilidad de las autoridades que deseen limitar el derecho demostrar que la limitación está relacionada con un objetivo legítimo. Además, las limitaciones al derecho a la privacidad no deben vaciar el derecho de su esencia y deben ser compatibles con otras normas de derechos humanos, incluida la prohibición de la discriminación. Si la limitación no cumple esos criterios, es ilegal y/o la injerencia en el derecho a la privacidad es arbitraria.

24. Los gobiernos suelen alegar que los programas de vigilancia de las comunicaciones digitales obedecen a motivos de seguridad nacional, en particular los riesgos planteados por el terrorismo. En varias de las contribuciones se indicó que, puesto que las tecnologías de comunicación digital pueden ser, y han sido, utilizadas por particulares con fines delictivos (como el reclutamiento para la comisión de atentados terroristas y el financiamiento de los mismos), la vigilancia legal y específica de las comunicaciones digitales puede constituir una medida necesaria y eficaz para las entidades de inteligencia y/o de aplicación de la ley cuando se lleva a cabo en cumplimiento de la legislación internacional y nacional. La vigilancia por motivos de seguridad nacional o para prevenir atentados terroristas u otros delitos puede ser un "objetivo legítimo" a los efectos de realizar una evaluación desde el punto de vista del artículo 17 del Pacto. Sin embargo, el grado de injerencia debe contraponerse a la necesidad de la medida para lograr ese objetivo y el beneficio real que se obtiene a tal efecto.

25. En relación con la necesidad de una medida, el Comité de Derechos Humanos, en su Observación general Nº 27, sobre el artículo 12 del Pacto Internacional de Derechos Civiles y Políticos, destacó que "las restricciones no deben comprometer la esencia del derecho […]; no se debe invertir la relación entre derecho y restricción, entre norma y excepción"[17]. El Comité explicó además que "no basta con que las restricciones se utilicen para conseguir fines permisibles; deben ser necesarias también para protegerlos". Por otro lado, las medidas deben ser proporcionadas: "el instrumento menos perturbador de los que permitan conseguir el resultado deseado"[18]. Cuando existe un objetivo legítimo y se han establecido las salvaguardias apropiadas, puede permitirse a un Estado realizar actividades de vigilancia bastante perturbadoras; sin embargo, incumbe al gobierno demostrar que la injerencia es necesaria y proporcional al riesgo concreto de que se trate. Así pues, los programas de vigilancia en masa o "a granel" pueden considerarse arbitrarios, aunque persigan un objetivo legítimo y hayan sido aprobados sobre la base de un régimen jurídico accesible. En otras palabras, no es suficiente que las medidas tengan por objeto encontrar determinadas agujas en un pajar; lo importante es el impacto de las medidas en el pajar, en comparación con el riesgo de que se trate; es decir, si la medida es necesaria y proporcionada.

26. La preocupación sobre si el acceso a los datos y su uso se ajustan a objetivos legítimos específicos plantea también dudas sobre la creciente colaboración de los gobiernos con entidades del sector privado para que conserven datos "por si acaso" los necesita el gobierno. La conservación obligatoria de datos de terceros —característica

[16] CCPR/C/21/Rev.1/Add.9, párrs. 11 a 16. Véase también A/HRC/14/46, anexo, práctica 20.

[17] CCPR/C/21/Rev.1/Add.9, párrs. 11 a 16. Véase también Tribunal Europeo de Derechos Humanos, *Handyside v. the United Kingdom*, párr. 48; y *Klass v. Germany*, párr. 42.

[18] CCPR/C/21/Rev.1/Add.9, párrs. 11 a 16.

frecuente de los regímenes de vigilancia de muchos Estados, cuyos gobiernos exigen a las compañías telefónicas y a los proveedores de servicios de Internet que almacenen los metadatos acerca de las comunicaciones y la ubicación de sus clientes para que las fuerzas del orden y los organismos de inteligencia puedan acceder posteriormente a ellos— no parece necesaria ni proporcionada[19].

27. Uno de los factores que deben considerarse al determinar la proporcionalidad es qué se hace con los datos a granel y quién pueden acceder a ellos una vez recopilados. Muchos marcos nacionales carecen de "limitaciones de uso", permitiendo así la recopilación de datos para un objetivo legítimo, pero su uso posterior para otros. La inexistencia de limitaciones de uso efectivas se ha exacerbado desde el 11 de septiembre de 2001, y la línea que separa la justicia penal de la protección de la seguridad nacional se ha difuminado significativamente. El intercambio resultante de datos entre las fuerzas del orden, los organismos de inteligencia y otros órganos del Estado corre el riesgo de violar el artículo 17 del Pacto, ya que las medidas de vigilancia que pueden ser necesarias y proporcionadas para un objetivo legítimo pueden no serlo para otros fines. En un estudio sobre las prácticas nacionales de acceso por el gobierno a datos de terceros se señaló que, "cuando se combina con la mayor facilidad con que los organismos de seguridad nacional y las fuerzas del orden obtienen acceso a datos del sector privado, la ampliación de la libertad para compartir esa información entre los organismos y utilizarla para fines distintos de los que propiciaron su recopilación representa un debilitamiento sustancial de la protección de datos tradicional"[20]. En varios Estados, los regímenes de intercambio de datos han sido anulados por los tribunales por ese motivo. Otros han indicado que ese tipo de limitaciones de uso son una buena práctica para asegurar el cumplimiento efectivo de las obligaciones del Estado en virtud del artículo 17 del Pacto[21], con sanciones significativas por su violación.

B. Protección de la ley

28. El párrafo 2 del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos establece explícitamente que toda persona tiene derecho a la protección de la ley contra las injerencias arbitrarias o ilegales en su vida privada. Ello entraña que cualquier programa de vigilancia de las comunicaciones ha de realizarse sobre la base de una ley a la que el público tenga acceso, que a su vez debe estar en conformidad con el régimen constitucional del propio Estado y el derecho internacional de los derechos humanos[22]. La "accesibilidad" no solo exige que la ley esté publicada, sino que sea suficientemente precisa para que el interesado pueda ajustar su comportamiento a ella, previendo las consecuencias que un determinado acto puede entrañar. El Estado debe asegurarse de que toda injerencia en el derecho a la vida privada, la familia, el domicilio o la correspondencia esté autorizada por leyes que: a) sean de acceso público; b) contengan disposiciones que garanticen que la obtención, el acceso y la utilización de los datos de las comunicaciones obedezcan a objetivos específicos legítimos; c) sean suficientemente precisas y especifiquen en detalle las circunstancias concretas en que dichas injerencias pueden ser autorizadas, los

[19] Véanse las conclusiones del Abogado General Cruz Villalón del Tribunal de Justicia de la Unión Europea en los asuntos acumulados C-293/12 y C-594/12, en las que indica que la Directiva 2006/24/CE (sobre la conservación de datos generados o tratados en relación con la prestación de servicios de comunicaciones electrónicas) es "en su conjunto" incompatible con la Carta de los Derechos Fundamentales de la Unión Europea porque no impone estrictos límites a dicha conservación de datos. Véase también CCPR/C/USA/CO/4, párr. 22.

[20] Fred H. Cate, James X. Dempsey e Ira S. Rubinstein, "Systematic government access to private-sector data", *International Data Privacy Law*, vol. 2, Nº 4, 2012, pág. 198.

[21] Véase A/HRC/14/46, anexo, práctica 23.

[22] Véase *ibid*., anexo.

procedimientos de autorización, las categorías de personas que pueden ser sometidas a vigilancia, el límite de la duración de la vigilancia y los procedimientos para el uso y el almacenamiento de los datos recopilados; y d) proporcionen salvaguardias efectivas contra el uso indebido[23].

29. Por consiguiente, las normas y las interpretaciones secretas —incluso las interpretaciones judiciales secretas— del derecho no cumplen los requisitos necesarios para considerarse "ley"[24]. Lo mismo sucede con las leyes o normas que conceden a las autoridades ejecutivas, como los servicios de seguridad e inteligencia, una facultad discrecional excesiva; el alcance de la facultad discrecional otorgada y la manera de ejercerla deben indicarse (en la propia ley o en directrices vinculantes publicadas) con una claridad razonable. Una ley que sea accesible pero no tenga efectos previsibles tampoco será adecuada. El carácter secreto de determinadas facultades de vigilancia lleva aparejado un mayor riesgo de ejercicio arbitrario de la discrecionalidad, que, a su vez, exige una mayor precisión en la norma por la que se rige el ejercicio de la facultad discrecional, así como una mayor supervisión. Varios Estados exigen también que el marco jurídico se establezca mediante el debate de la legislación primaria en el Parlamento y no mediante la simple aprobación de reglamentos subsidiarios por el Ejecutivo, requisito que contribuye a garantizar que el marco jurídico no solo sea accesible para el público interesado después de su promulgación, sino también durante su elaboración, de conformidad con lo dispuesto en el artículo 25 del Pacto Internacional de Derechos Civiles y Políticos[25].

30. El requisito de la accesibilidad también es pertinente al evaluar la práctica que están empezando a adoptar algunos Estados de externalizar las tareas de vigilancia. Se dispone de información fidedigna que lleva a pensar que algunos gobiernos han desviado sistemáticamente la recopilación y el análisis de datos a jurisdicciones con una menor protección de la privacidad. Al parecer, algunos gobiernos han puesto en marcha una red transnacional de servicios de inteligencia mediante un entramado de lagunas jurídicas que permite coordinar las prácticas de vigilancia para burlar las medidas de protección previstas en los ordenamientos jurídicos internos. Podría decirse que esa práctica no cumple el criterio de la legalidad porque, como se ha señalado en algunas contribuciones al presente informe, hace que el funcionamiento del sistema de vigilancia sea imprevisible para aquellos a quienes se aplica. Esa práctica podría socavar la esencia del derecho protegido por el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y, por lo tanto, estaría prohibida en virtud del artículo 5. Algunos Estados tampoco han adoptado medidas efectivas para proteger a las personas sujetas a su jurisdicción contra las prácticas de vigilancia ilegales de otros Estados o entidades comerciales, en contravención de sus propias obligaciones en materia de derechos humanos.

C. ¿A quién se protege y dónde?

31. La aplicación extraterritorial del Pacto Internacional de Derechos Civiles y Políticos a la vigilancia digital se trató en varias de las contribuciones recibidas. Aunque está claro que algunos aspectos de los programas de vigilancia que han salido a la luz recientemente, por ejemplo, activan las obligaciones territoriales de los Estados que llevan a cabo la vigilancia, se han expresado otras preocupaciones en relación con la vigilancia extraterritorial y la interceptación de las comunicaciones.

[23] CCPR/C/USA/CO/4, párr. 22. Véase también Tribunal Europeo de Derechos Humanos, *Malone v. the United Kingdom*, demanda Nº 8691/79, 2 de agosto de 1984, párrs. 67 y 68; y *Weber and Saravia v. Germany*, demanda Nº 54934/00, 29 de junio de 2006, donde el Tribunal enumera las salvaguardias mínimas que deben establecerse en la legislación.

[24] CCPR/C/USA/CO/4, párr. 22.

[25] Véase también A/HRC/14/46.

32. El artículo 2 del Pacto Internacional de Derechos Civiles y Políticos establece que cada uno de los Estados partes se compromete a respetar y a garantizar a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción los derechos reconocidos en el Pacto, sin distinción alguna de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social. El Comité de Derechos Humanos, en su Observación general Nº 31, señaló que los Estados partes "están obligados por el párrafo 1 del artículo 2 a respetar y garantizar a todos los individuos que se encuentren en su territorio y a todas las personas sometidas a su jurisdicción" los derechos enunciados en el Pacto. "Esto significa que un Estado parte debe respetar y garantizar los derechos establecidos en el Pacto a cualquier persona sometida al poder o al control efectivo de ese Estado incluso si no se encuentra en el territorio del Estado parte"[26]. Esa obligación se hace extensiva a las personas sometidas a su "autoridad"[27].

33. Como se indica incluso en su más antigua jurisprudencia, el Comité de Derechos Humanos se ha guiado por el principio de que un Estado no puede eludir las obligaciones internacionales que le incumben en materia de derechos humanos mediante la adopción de medidas fuera de su territorio que tendría prohibido tomar "en el suyo"[28]. Esa posición está en consonancia con la opinión de la Corte Internacional de Justicia, que ha afirmado que el Pacto Internacional de Derechos Civiles y Políticos "es aplicable con respecto a los actos de un Estado en el ejercicio de su jurisdicción fuera de su propio territorio"[29], así como con los artículos 31 y 32 de la Convención de Viena sobre el Derecho de los Tratados. Las nociones de "poder" y "control efectivo" son indicadores de si un Estado ejerce "jurisdicción" o potestades gubernamentales, cuyo abuso pretenden evitar las normas de protección de los derechos humanos. Los Estados no pueden eludir sus responsabilidades en materia de derechos humanos limitándose a mantener esas potestades fuera del alcance de la ley. Concluir lo contrario no solo supondría socavar la universalidad y la esencia de los derechos protegidos por el derecho internacional de los derechos humanos, sino que también podría crear incentivos estructurales para que los Estados externalicen la vigilancia entre sí.

34. De todo ello se desprende, por lo tanto, que la vigilancia digital puede comprometer las obligaciones de derechos humanos de un Estado si esa vigilancia entraña el ejercicio de su poder o control efectivo en relación con una infraestructura de comunicaciones digitales, dondequiera que esté, por ejemplo mediante escuchas directas o la infiltración en esa infraestructura. Del mismo modo, cuando el Estado ejerce su jurisdicción reguladora sobre un tercero que tiene el control material de los datos, también tendría obligaciones en virtud del Pacto. Si un país trata de hacer valer su jurisdicción en relación con los datos de empresas privadas por el hecho de que hayan sido constituidas en su territorio, las medidas de protección de los derechos humanos deberán hacerse extensivas a aquellas personas cuya privacidad se esté viendo afectada, ya sea en el país de constitución de la empresa o

[26] CCPR/C/21/Rev.1/Add.13, párr. 10.

[27] Véase *Documentos Oficiales de la Asamblea General, trigésimo sexto período de sesiones, Suplemento Nº 40* (A/36/40), anexo XIX, párr. 12.2; véase también anexo XX. Véanse además CCPR/CO/78/ISR, párr. 11; CCPR/CO/72/NET, párr. 8; CCPR/CO/81/BEL, párr. 6; y Comisión Interamericana de Derechos Humanos, *Coard y otros c. los Estados Unidos*, caso 10.951, informe Nº 109/99, 29 de septiembre de 1999, párrs. 37, 39, 41 y 43.

[28] Véase *Documentos Oficiales de la Asamblea General, trigésimo sexto período de sesiones* (véase nota 27), anexo XIX, párrs. 12.2 y 12.3, y anexo XX, párr. 10.3.

[29] Opinión consultiva de la Corte Internacional de Justicia sobre las *Consecuencias jurídicas de la construcción de un muro en el territorio palestino ocupado*, 9 de julio de 2004 (A/ES-10/273 y Corr.1), párrs. 107 a 111. Véase también Corte Internacional de Justicia, *Causa relativa a las actividades armadas en el territorio del Congo (República Democrática del Congo c. Uganda)*, fallo, 2005, pág. 168.

fuera de sus fronteras. Esto se aplica con independencia de que, para empezar, el ejercicio de la jurisdicción sea legal, o de hecho viole la soberanía de otro Estado.

35. Esta conclusión también es importante a la luz del debate actual sobre si los "extranjeros" y los "ciudadanos" deben tener igual acceso a las medidas de protección de la privacidad en los sistemas de supervisión de la vigilancia en aras de la seguridad nacional. Varios ordenamientos jurídicos distinguen entre las obligaciones para con los nacionales o las personas presentes en los territorios del Estado y las obligaciones para con los no nacionales y las personas que están fuera de dicho territorio[30], o establecen menores niveles de protección para las comunicaciones extranjeras o externas. En los casos en que no se sepa con certeza si los datos son extranjeros o nacionales, los servicios de inteligencia a menudo procesan los datos como extranjeros (ya que las comunicaciones digitales suelen cruzar las fronteras en algún momento), permitiendo así que sean recopilados y conservados. El resultado es un nivel de protección de la privacidad sustancialmente inferior —o incluso nulo— para los extranjeros y los no ciudadanos, en comparación con los ciudadanos.

36. El derecho internacional de los derechos humanos es explícito en relación con el principio de no discriminación. El artículo 26 del Pacto Internacional de Derechos Civiles y Políticos dispone que "todas las personas son iguales ante la ley y tienen derecho sin discriminación a igual protección de la ley" y añade que, "a este respecto, la ley prohibirá toda discriminación y garantizará a todas las personas protección igual y efectiva contra cualquier discriminación por motivos de raza, color, sexo, idioma, religión, opiniones políticas o de cualquier otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social". Esas disposiciones han de leerse juntamente con el artículo 17, que establece que "nadie será objeto de injerencias arbitrarias o ilegales en su vida privada" y que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques", así como con el artículo 2, párrafo 1. En este sentido, el Comité de Derechos Humanos ha subrayado la importancia de adoptar "medidas para que toda interferencia en el derecho a la intimidad se ajuste a los principios de legalidad, proporcionalidad y necesidad, con independencia de la nacionalidad o el emplazamiento de las personas cuyas comunicaciones estén bajo vigilancia directa"[31].

D. Garantías procesales y supervisión efectiva

37. El artículo 17, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos establece que toda persona tiene derecho a la protección de la ley contra las injerencias o ataques ilegales o arbitrarios. La "protección de la ley" debe aplicarse mediante garantías procesales efectivas, incluida la creación de instituciones eficaces y dotadas de recursos adecuados. Sin embargo, es evidente que la inexistencia de una supervisión efectiva ha contribuido a la falta de rendición de cuentas por las intrusiones arbitrarias o ilegales en el derecho a la privacidad en el entorno digital. En particular, las salvaguardias internas no acompañadas de una supervisión externa independiente han resultado ineficaces frente a los métodos de vigilancia ilegales o arbitrarios. Aunque esas salvaguardias pueden adoptar muy diversas formas, la participación de todos los poderes del Estado en la supervisión de

[30] Véase, por ejemplo, en los Estados Unidos, la Ley de Vigilancia y Adquisición de Inteligencia Extranjera (Foreign Intelligence Surveillance Act, § 1881a); en el Reino Unido, la Ley de Regulación de las Atribuciones de Investigación (Regulation of Investigatory Powers Act 2000), art. 8.4; en Nueva Zelandia, la Ley del Servicio de Seguridad del Gobierno (Government Security Bureau Act 2003), art. 15A; en Australia, la Ley de los Servicios de Inteligencia (Intelligence Services Act), art. 9; y en el Canadá, la Ley de Defensa Nacional (National Defence Act) art. 273.64, párr. 1.

[31] CCPR/C/USA/CO/4, párr. 22.

los programas de vigilancia, así como de un organismo de supervisión civil independiente, es fundamental para garantizar una protección efectiva de la ley.

38. La participación del poder judicial con arreglo a las normas internacionales relativas a la independencia, la imparcialidad y la transparencia puede contribuir a que el ordenamiento jurídico general cumpla las normas mínimas exigidas por el derecho internacional de los derechos humanos. No obstante, la intervención judicial en la supervisión tampoco debe considerarse una panacea; en varios países, el mandamiento o la revisión judicial de las actividades de vigilancia digital de los servicios de inteligencia y/o los organismos encargados de hacer cumplir la ley han supuesto en la práctica un mero ejercicio de aprobación sumisa. Por consiguiente, la atención se está centrando cada vez más en modelos mixtos de supervisión administrativa, judicial y parlamentaria, aspecto resaltado en varias contribuciones al presente informe. Existe un interés particular en crear puestos encargados de la defensa del "interés público" en el marco de los procesos de autorización de la vigilancia. Dada la creciente importancia del papel desempeñado por terceros, como los proveedores de servicios de Internet, también podría considerarse la posibilidad de permitirles participar en la autorización de las medidas de vigilancia que afecten a sus intereses o impugnar las medidas existentes. La utilidad del asesoramiento, la fiscalización y/o la revisión independientes para asegurar un examen estricto de las medidas impuestas por un régimen jurídico de vigilancia ha sido destacada positivamente en la jurisprudencia en la materia. Las comisiones parlamentarias también pueden desempeñar una función importante; sin embargo, pueden carecer de independencia, recursos o voluntad para detectar los abusos, y pueden verse influidas por grupos de interés. La jurisprudencia a nivel regional ha hecho hincapié en la utilidad de un órgano de supervisión totalmente independiente, en particular para controlar la ejecución de las medidas de vigilancia aprobadas[32]. En 2009, el Relator Especial sobre la promoción y la protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo señaló, por consiguiente, que "no debe haber ningún sistema secreto de vigilancia que no se encuentre sometido al examen de un órgano de supervisión efectivo y todas las injerencias deben ser autorizadas por un órgano independiente"[33].

E. Derecho a un recurso efectivo

39. El Pacto Internacional de Derechos Civiles y Políticos establece que los Estados partes deben garantizar que las víctimas de violaciones de los derechos y libertades reconocidos en el Pacto puedan interponer un recurso efectivo. El artículo 2, párrafo 3 b), dispone además que cada uno de los Estados partes en el Pacto se compromete a garantizar que "la autoridad competente, judicial, administrativa o legislativa, o cualquiera otra autoridad competente prevista por el sistema legal del Estado, decidirá sobre los derechos de toda persona que interponga tal recurso, y desarrollará las posibilidades de recurso judicial". Los Estados también deben garantizar que las autoridades competentes cumplirán toda decisión en que se haya estimado procedente el recurso. Como señaló el Comité de Derechos Humanos en su Observación general Nº 31, el hecho de que un Estado parte no investigue las denuncias de violación puede ser de por sí una vulneración del Pacto[34]. Además, la cesación de la violación constituye un elemento indispensable del derecho a obtener un recurso efectivo.

40. Los recursos efectivos por las violaciones de la privacidad mediante actividades de vigilancia digital pueden tener diversas formas judiciales, legislativas o administrativas,

[32] Véase, por ejemplo, Tribunal Europeo de Derechos Humanos, *Ekimdzhiev v. Bulgaria*, demanda Nº 62540/00, 28 de junio de 2007.

[33] A/HRC/13/37, párr. 62.

[34] CCPR/C/21/Rev.1/Add.13, párr. 15.

aunque suelen compartir ciertas características. En primer lugar, esos recursos deben ser conocidos y accesibles para cualquier persona que afirme de manera defendible que se han violado sus derechos. Por lo tanto, la notificación (de que se ha creado un régimen de vigilancia general o medidas de vigilancia específicas) y la legitimación (para impugnar tales medidas) se convierten en cuestiones fundamentales para determinar el acceso a un recurso efectivo. Los Estados adoptan diferentes enfoques de la notificación: mientras que algunos requieren la notificación *a posteriori* a las personas objeto de vigilancia, una vez que concluyen las investigaciones, muchos regímenes no prevén la notificación. Algunos también requieren formalmente la notificación en los asuntos penales; sin embargo, en la práctica, esta obligación parece ignorarse frecuentemente. También existen diversos enfoques nacionales de la cuestión de la legitimación de una persona para iniciar una impugnación judicial. El Tribunal Europeo de Derechos Humanos dictaminó que, si bien la existencia de un régimen de vigilancia podía resultar una injerencia en la privacidad, la afirmación de que dicha injerencia constituía una violación de derechos solo era defendible ante los tribunales si existía una "probabilidad razonable" de que la persona en cuestión hubiera sido realmente objeto de vigilancia ilegal[35].

41. En segundo lugar, los recursos efectivos deben dar lugar a una investigación inmediata, exhaustiva e imparcial de las presuntas violaciones. Esto puede conseguirse mediante la creación de un "organismo de control independiente y contar con garantías suficientes de debido proceso y supervisión judicial, dentro de las limitaciones permisibles en una sociedad democrática"[36]. En tercer lugar, para que los recursos sean efectivos, deben ser suficientes para poner fin a las violaciones en curso, por ejemplo ordenando la eliminación de los datos u otra reparación[37]. Esos organismos de control deben tener "un acceso pleno y sin trabas a toda la información pertinente y dispone[r] de los recursos y servicios técnicos necesarios para realizar las investigaciones, y de la capacidad de dictar órdenes de obligado cumplimiento"[38]. En cuarto lugar, cuando las violaciones de derechos humanos alcanzan al nivel de violaciones graves, los recursos no judiciales no son suficientes, ya que se requiere un proceso penal[39].

IV. ¿Qué papel para las empresas?

42. Hay numerosas pruebas de que los gobiernos recurren cada vez más al sector privado para que realice y facilite las actividades de vigilancia digital. Gobiernos de todos los continentes han utilizado tanto mecanismos legales formales como métodos encubiertos para tener acceso a los contenidos, así como a los metadatos. Ese proceso es cada vez más formalizado: al trasladarse la prestación de servicios de telecomunicaciones del sector

[35] Véase *Esbester v. the United Kingdom*, demanda Nº 18601/91, decisión de la Comisión de 2 de abril de 1993; *Redgrave v. the United Kingdom*, demanda Nº 202711/92, decisión de la Comisión de 1 de septiembre de 1993; y *Matthews v. the United Kingdom*, demanda Nº 28576/95, decisión de la Comisión de 16 de octubre de 1996.

[36] "Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión", formulada por el Relator Especial sobre el derecho a la libertad de opinión y de expresión y la Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos, junio de 2013 (disponible en www.oas.org/es/cidh/expresion/showarticle.asp?artID=927&lID=2), párr. 9.

[37] Véase, por ejemplo, Tribunal Europeo de Derechos Humanos, *Segersted-Wiber and others v. Sweden*, demanda Nº 62332/00, 6 de junio de 2006. Véase también CCPR/C/21/Rev.1/Add.13, párrs. 15 a 17.

[38] A/HRC/14/46.

[39] Principios y directrices básicos sobre el derecho de las víctimas de violaciones manifiestas de las normas internacionales de derechos humanos y de violaciones graves del derecho internacional humanitario a interponer recursos y obtener reparaciones (resolución 60/147 de la Asamblea General, anexo).

público al sector privado, se ha producido una "delegación de las responsabilidades policiales y cuasijudiciales a los intermediarios de Internet disfrazada de 'autorregulación' o 'cooperación'"[40]. La promulgación de leyes que obligan a las empresas a preparar sus redes para la interceptación es motivo de especial preocupación, en particular porque crea un ambiente que facilita las medidas de vigilancia exhaustiva.

43. Un Estado puede tener motivos legítimos para exigir a una empresa de tecnología de la información y las comunicaciones que le proporcione datos de sus usuarios; sin embargo, cuando una empresa suministra datos o información de sus usuarios a un Estado en respuesta a una solicitud que contraviene el derecho a la privacidad establecido en el derecho internacional, proporciona tecnología o equipos de vigilancia en masa a un Estado sin salvaguardias adecuadas o cuando se da a dicha información otro uso contrario a los derechos humanos, la empresa en cuestión puede ser cómplice o estar involucrada de otra manera en violaciones de los derechos humanos. Los Principios Rectores sobre las empresas y los derechos humanos, aprobados por el Consejo de Derechos Humanos en 2011, proporcionan un marco internacional para prevenir y combatir los efectos adversos vinculados con las actividades empresariales en los derechos humanos. La responsabilidad de respetar los derechos humanos se aplica a todas las operaciones de la empresa en todo el mundo, independientemente de la ubicación de sus usuarios, y existe independientemente de si el Estado cumple con sus obligaciones de derechos humanos.

44. Se han hecho importantes esfuerzos multipartitos para aclarar la aplicación de los Principios Rectores al sector de la tecnología de la información y las comunicaciones. Por ejemplo, las empresas que proporcionan contenidos o servicios de Internet, o suministran la tecnología y los equipos que hacen posible las comunicaciones digitales, deberían formular una declaración de política explícita en la que expongan su compromiso de respetar los derechos humanos en todas las actividades de la empresa. También deberían contar con políticas adecuadas de diligencia debida para detectar, evaluar, prevenir y mitigar todo impacto negativo. Las empresas deberían evaluar si sus condiciones de servicio, o sus políticas de recopilación e intercambio de datos de sus clientes, pueden dar lugar a un impacto negativo en los derechos humanos de sus usuarios, y de qué manera pueden hacerlo.

45. Cuando los gobiernos exigen a las empresas que les proporcionen acceso a los datos en contravención de las normas internacionales de derechos humanos, las empresas deben tratar de honrar los principios de derechos humanos en la medida de lo posible, y ser capaces de demostrar sus iniciativas en curso para hacerlo. Ello puede entrañar interpretar las demandas del gobierno de la manera más restringida posible, pedir aclaraciones a un gobierno en relación con el alcance y el fundamento jurídico de la demanda, requerir una orden judicial antes de acceder a las peticiones de datos del gobierno, y comunicar de forma transparente a sus usuarios los riesgos y la aceptación de las demandas del gobierno. Existen ejemplos positivos del sector en ese sentido, tanto por parte de empresas individuales como de iniciativas multipartitas.

46. Una parte fundamental de la diligencia debida en materia de derechos humanos que se define en los Principios Rectores es la realización de consultas verdaderas con las partes afectadas. En el contexto de las empresas de tecnología de la información y las comunicaciones, ello incluye también informar transparentemente a los usuarios de la manera en que sus datos son recopilados, almacenados, usados y potencialmente compartidos con otros, de modo que sean capaces de plantear sus preocupaciones y de tomar decisiones con conocimiento de causa. Los Principios Rectores aclaran que, cuando las empresas detectan que han causado o contribuido a un impacto negativo en los derechos

[40] Véase European Digital Rights, "The Slide from 'Self-Regulation' to Corporate Censorship", Bruselas, enero de 2011, disponible en www.edri.org/files/EDRI_selfreg_final_20110124.pdf.

humanos, tienen la obligación de asegurar la reparación proporcionándola directamente o cooperando con procesos legítimos de reparación. Para permitir que se proporcione una reparación a la mayor brevedad, las empresas deberían establecer mecanismos de queja allá donde operen. Dichos mecanismos pueden ser particularmente importantes en los países en que los derechos no estén suficientemente protegidos o en que no se pueda acceder a recursos judiciales o de otra índole. Además de elementos como la indemnización y el resarcimiento, la reparación debería incluir información sobre los datos que se han facilitado a las autoridades estatales, y sobre la manera en que se han facilitado.

V. Conclusiones y recomendaciones

47. **El derecho internacional de los derechos humanos proporciona un marco claro y universal para la promoción y la protección del derecho a la privacidad, también en el contexto de la vigilancia nacional y extraterritorial, la interceptación de las comunicaciones digitales y la recopilación de datos personales. Sin embargo, las prácticas en muchos Estados han puesto de manifiesto una carencia de leyes nacionales adecuadas y/o de aplicación de las mismas, insuficientes garantías procesales y capacidades de supervisión ineficaces, elementos que han contribuido a la falta de rendición de cuentas por las injerencias arbitrarias o ilegales en el derecho a la privacidad.**

48. **Al estudiar las significativas lagunas en la efectividad del derecho a la privacidad, cabe formular dos observaciones. La primera es que sigue saliendo a la luz información sobre las políticas y prácticas de vigilancia nacionales y extraterritoriales. Se están realizando investigaciones con el fin de reunir información sobre la vigilancia electrónica y la recopilación y el almacenamiento de datos personales, así como para evaluar su impacto en los derechos humanos. Distintos tribunales nacionales y regionales están examinando la legalidad de las políticas y medidas de vigilancia electrónica. Toda evaluación de la compatibilidad de las políticas y prácticas de vigilancia con el derecho internacional de los derechos humanos debe adaptarse necesariamente al carácter evolutivo de la cuestión. La segunda observación, que está relacionada con la primera, se refiere a la preocupante falta de transparencia gubernamental asociada a las políticas, leyes y prácticas de vigilancia, que dificulta todo intento de evaluar su compatibilidad con el derecho internacional de los derechos humanos y asegurar la rendición de cuentas.**

49. **Para abordar efectivamente los desafíos relacionados con el derecho a la privacidad en el contexto de las tecnologías modernas de comunicación será necesario un compromiso multisectorial, concertado y constante. Este debería incluir un diálogo en el que participen todas las partes interesadas, incluidos los Estados Miembros, la sociedad civil, las comunidades científica y técnica, el sector empresarial, los docentes universitarios y los expertos en derechos humanos. A medida que sigan evolucionando las tecnologías de las comunicaciones, será fundamental disponer de una función rectora para asegurar que dichas tecnologías se utilicen para materializar su potencial de mejora del disfrute de los derechos humanos consagrados en el marco jurídico internacional.**

50. **Teniendo presentes estas observaciones, hay una necesidad clara y acuciante de supervisión para asegurar que toda política o práctica de vigilancia sea compatible con el derecho internacional de los derechos humanos, incluido el derecho a la privacidad, mediante el establecimiento de salvaguardias eficaces contra los abusos. Como medida inmediata, los Estados deberían revisar sus propias leyes, políticas y prácticas nacionales para garantizar su plena conformidad con el derecho internacional de los derechos humanos. Si detectan deficiencias, deberían tomar**

medidas para colmarlas, en particular adoptando un marco legislativo claro, preciso, accesible, integral y no discriminatorio. Deberían tomarse medidas para establecer regímenes y prácticas de supervisión efectiva e independiente, prestando atención al derecho de las víctimas a un recurso efectivo.

51. **La promoción y la protección del derecho a la privacidad en la era digital presentan una serie de importantes desafíos prácticos. Sobre la base del examen inicial de algunos de esos desafíos en el presente informe, es preciso intensificar el debate y realizar un estudio a fondo sobre las cuestiones relativas a la protección efectiva de la ley, las garantías procesales, la supervisión efectiva y los recursos. Un análisis en profundidad de esas cuestiones proporcionaría una mayor orientación práctica, basada en el derecho internacional de los derechos humanos, sobre los principios de necesidad, proporcionalidad y legitimidad en relación con las prácticas de vigilancia; sobre las medidas de supervisión efectiva, independiente e imparcial; y sobre los recursos. También ayudaría a las empresas a cumplir su obligación de respetar los derechos humanos, teniendo en cuenta las salvaguardias en materia de diligencia debida y gestión de los riesgos, así como su papel en cuanto a los recursos efectivos.**