Naciones Unidas A/HRC/39/29

Asamblea General

Distr. general
3 de agosto de 2018
Español
Original: inglés

Consejo de Derechos Humanos
39º 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 del Alto Comisionado de las Naciones Unidas para los Derechos Humanos

Resumen

Este informe se presenta de conformidad con la resolución 34/7, en la que el Consejo de Derechos Humanos pidió al Alto Comisionado de las Naciones Unidas para los Derechos Humanos que preparase un informe en el que se determinasen y aclarasen los principios, las normas y las mejores prácticas en relación con la promoción y la protección del derecho a la privacidad en la era digital, incluida la responsabilidad de las empresas en ese sentido, y que lo presentase al Consejo en su 39º período de sesiones.

GE.18-12799 (S) 220818 290818
1812799

I. Introducción

1. La necesidad de hacer frente a los desafíos que plantea el mundo digital para el derecho a la privacidad nunca ha sido tan acuciante. Impulsadas principalmente por el sector privado, las tecnologías digitales que utilizan constantemente datos sobre la vida de las personas están penetrando progresivamente en el tejido social, cultural, económico y político de las sociedades modernas. Las tecnologías que emplean un gran volumen de datos, como los macrodatos y la inteligencia artificial, son cada vez más poderosas y amenazan con crear un entorno digital intrusivo en el que tanto los Estados como las empresas pueden llevar a cabo actividades de vigilancia, análisis y predicción e incluso manipular el comportamiento de la población en una medida sin precedentes. Es innegable que las tecnologías basadas en datos pueden destinarse a usos altamente beneficiosos, pero estos avances tecnológicos plantean riesgos muy importantes para la dignidad humana, la autonomía y la vida privada, así como para el ejercicio de los derechos humanos en general, si no se gestionan con sumo cuidado.

2. Los agentes internacionales y regionales son cada vez más conscientes de los desafíos y están empezando a actuar en consecuencia. El Consejo de Derechos Humanos creó el mandato del Relator Especial sobre el derecho a la privacidad en julio de 2015. El Consejo de Derechos Humanos y la Asamblea General han expresado en numerosas resoluciones su preocupación por los riesgos para la privacidad que resultan de las medidas de vigilancia de los Estados y de las prácticas de las empresas[1]. A nivel regional, se han adoptado varias medidas para reforzar la protección de la privacidad de los datos, como el Reglamento general de protección de datos de la Unión Europea, que ha entrado en vigor recientemente y ha tenido repercusiones a nivel mundial; el protocolo del Consejo de Europa por el que se actualiza y moderniza el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal y las directrices sobre protección de datos personales para África de la Comisión de la Unión Africana. Al mismo tiempo, muchos gobiernos han aprobado leyes o propuesto legislación para ampliar sus facultades de vigilancia, a menudo en contravención de las normas internacionales de derechos humanos aplicables[2].

3. En el presente informe se ofrece orientación sobre cómo abordar algunos de los desafíos apremiantes que afectan al derecho a la privacidad en la era digital. Se presenta un breve resumen del marco jurídico internacional y un análisis de las principales tendencias actuales. A continuación, se examinan las obligaciones de los Estados y la responsabilidad de las empresas, incluido un examen de las salvaguardias y los mecanismos de supervisión adecuados. En el último capítulo se aporta información sobre los mecanismos de reparación que pueden ofrecerse ante vulneraciones y violaciones de la privacidad.

4. Este informe se basa en el informe presentado por el Alto Comisionado en 2014 sobre el derecho a la privacidad en la era digital (A/HRC/27/37) y en las presentaciones y los debates que tuvieron lugar en el taller de expertos celebrado en Ginebra en febrero de 2018[3]. También se basa en 63 comunicaciones escritas presentadas por una amplia gama de partes interesadas[4].

[1] Véanse, por ejemplo, las resoluciones 68/167, 69/166 y 71/199 de la Asamblea General y las resoluciones 28/16 y 34/7 y la decisión 25/117 del Consejo de Derechos Humanos.

[2] Véase, por ejemplo, Anja Seibert-Fohr, “Digital surveillance, metadata and foreign intelligence cooperation: unpacking the international right to privacy” (abril de 2018). Puede consultarse en: https://ssrn.com/abstract=3168711; https://csrcl.huji.ac.il/people/line-surveillance-case-law-un-human-rights-committee and www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyin DigitalAge/SR_right_privacy.pdf.

[3] Véase www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgePrivacyWorkhop.aspx. La transmisión web puede consultarse en: http://webtv.un.org/search/part-1.1-un-expert-workshop-on-the-right-to-privacy-in-the-digital-age/5734527899001/?term=2018-02-19&sort=date&page=2.

[4] Todas las comunicaciones pueden consultarse en: www.ohchr.org/EN/Issues/DigitalAge/Pages/ReportDigitalAge.aspx.

II. Comprender el derecho a la privacidad en la era digital

5. El derecho a la vida privada es un derecho humano fundamental reconocido en el artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y otros muchos instrumentos internacionales y regionales de derechos humanos[5] [6]. La privacidad puede entenderse como la presunción de que el individuo debe tener una esfera de desarrollo autónomo, interacción y libertad, una "esfera privada" con o sin relación con otras y libre de la intervención del Estado y de la intervención excesiva no solicitada de otros individuos no invitados (véanse, por ejemplo, A/HRC/13/37, párr. 11, y A/HRC/23/40, párrs. 22 y 42). En el entorno digital, la privacidad de la información, que abarca la información que existe o puede obtenerse acerca de una persona y de su vida y las decisiones basadas en esa información, tiene especial importancia.

6. La protección del derecho a la privacidad es amplia, ya que no solo abarca la información sustantiva contenida en las comunicaciones, sino también los metadatos, puesto que, al analizarse y reunirse, estos pueden "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" (véase A/HRC/27/37, párr. 19). La protección del derecho a la privacidad no se limita a los espacios privados, aislados, como el domicilio de una persona, sino que se extiende a los espacios públicos y a la información de acceso público (véase CCPR/C/COL/CO/7, párr. 32). Por ejemplo, el derecho a la vida privada entra en juego cuando un Gobierno vigila un espacio público, como un mercado o una estación de ferrocarril y, por lo tanto, observa a las personas. Asimismo, el derecho a la vida privada también se ve afectado cuando se reúne y analiza la información sobre una persona que se ha hecho pública en las redes sociales[7]. El intercambio público de información no implica que la información sustantiva quede desprotegida[8].

7. El derecho a la privacidad no solo se ve comprometido cuando la información sobre una persona es examinada o utilizada por un ser humano o un algoritmo[9]. El simple hecho que se generen y reúnan datos relativos a la identidad, la familia o la vida de una persona ya afecta a su derecho a la privacidad, pues a través de esas acciones, la persona pierde en cierta medida el control sobre una información que podría poner en riesgo su vida privada (véase A/HRC/27/37, párr. 20)[10]. Además, la mera existencia de sistemas secretos de vigilancia interfiere con el derecho a la privacidad *(ibid.)*[11].

8. El derecho a la vida privada se aplica por igual a todas las personas. Las diferencias en cuanto a su protección por motivos de nacionalidad o de otra índole son incompatibles con el derecho a la igualdad y a la no discriminación consagrado en el artículo 26 del Pacto Internacional de Derechos Civiles y Políticos.

[5] Véase, por ejemplo, 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; y el artículo 22 de la Convención sobre los Derechos de las Personas con Discapacidad.

[6] Véase, por ejemplo, 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 Europeo de Derechos Humanos.

[7] Véase la comunicación de Privacy International para el presente informe.

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

[9] Véase Paul Bernal, "Data gathering, surveillance and human rights: recasting the debate", *Journal of Cyber Policy*, vol. 1, núm. 2 (2016).

[10] Véanse también Tribunal Europeo de Derechos Humanos, *Rotaru c. Rumania*, demanda núm. 28341/95, sentencia de 4 de mayo de 2000, y *Kopp c. Suiza*, demanda núm. 23224/94, sentencia de 25 de marzo de 1998.

[11] Véanse también Tribunal Europeo de Derechos Humanos, *Roman Zakharov c. Rusia*, demanda núm. 47143/06, sentencia de 4 de diciembre de 2015.

9. 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 parte, incluso si no se encuentra en el territorio del Estado parte[12]. El derecho de los derechos humanos se aplica en los casos en que un Estado ejerce su poder o control efectivo sobre la infraestructura de las comunicaciones digitales, dondequiera que se encuentren, por ejemplo a través de escuchas directas o de la infiltración en una infraestructura de comunicaciones situada fuera de su territorio. Asimismo, cuando un Estado ejerce su jurisdicción reguladora sobre un tercero que controla la información sobre una persona (por ejemplo, un proveedor de servicios en la nube), ese Estado también deberá hacer extensivas las medidas de protección de los derechos humanos a aquellas personas cuya privacidad se esté viendo afectada por el acceso a esa información y su utilización (véase A/HRC/27/37, párr. 34).

10. De conformidad con el artículo 17 del Pacto, las injerencias solo serán admisibles si no son arbitrarias o ilegales. Los mecanismos de derechos humanos han interpretado sistemáticamente que esas palabras apuntan a los principios generales de legalidad, necesidad y proporcionalidad (véase A/HRC/27/37, párrs. 21 a 27)[13]. Con arreglo a esos principios, la injerencia de los Estados en el derecho a la privacidad solo puede hacerse en la medida prevista por la ley, y en la legislación pertinente se deben especificar con detalle las circunstancias precisas en que podrán autorizarse esas injerencias[14]. La injerencia no solo es ilegal y arbitraria cuando no está prevista en la ley, sino también cuando una ley o una injerencia concreta es incompatible con las disposiciones, los propósitos y los objetivos del Pacto[15]. Una limitación solo puede ser legal y no arbitraria si persigue un fin legítimo (véase A/HRC/29/32, párr. 33). La limitación debe ser necesaria y proporcional a ese fin legítimo, y debe ser la menos intrusiva de las opciones disponibles. Además, las limitaciones del derecho a la privacidad no deben comprometer la esencia del derecho (véase A/69/397, párr. 51).

11. El derecho a la privacidad es fundamental para el goce y el ejercicio de los derechos humanos dentro y fuera de Internet. Constituye uno de los fundamentos de la sociedad democrática y tiene un papel clave en la realización de una amplia gama de derechos humanos, que van desde la libertad de expresión (véanse A/HRC/23/40 y A/HRC/29/32, párr. 15) y la libertad de asociación y reunión (véanse A/HRC/31/66, párrs. 73 a 78 y A/72/135, párrs. 47 a 50) a la prohibición de la discriminación, entre otros[16]. La injerencia en el derecho a la privacidad puede tener repercusiones desproporcionadas en determinadas personas o grupos, agravando así la desigualdad y la discriminación[17]. La reglamentación excesiva de la privacidad también puede imponer limitaciones indebidas a otros derechos, en particular a la libertad de expresión cuando, por ejemplo, una reglamentación desproporcionada interfiere con la difusión de noticias legítimas, la expresión artística o la investigación científica. Por falta de espacio, la relación entre el derecho a la privacidad y los demás derechos humanos, sus efectos discriminatorios sobre personas y grupos específicos, y los enfoques para la protección de estos últimos, no pueden examinarse en el presente informe.

[12] Véase la observación general núm. 31 (2004) del Comité de Derechos Humanos sobre la índole de la obligación jurídica general impuesta a los Estados partes en el Pacto, párr. 10.

[13] Véase también la resolución 34/7 del Consejo de Derechos Humanos, párr. 2.

[14] Véase la observación general núm. 16 (1988) del Comité de Derechos Humanos sobre el derecho a la intimidad, párrs. 3 y 8.

[15] *Ibid*., párr. 4.

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

[17] Véanse la resolución 71/199, párr. 5 g), de la Asamblea General; la resolución 34/7, párr. 5 g), del Consejo de Derechos Humanos; y la comunicación de *International Network of Civil Liberties Organizations* para el presente informe.

III. Injerencias en la privacidad: tendencias y preocupaciones

A. Uso creciente de datos personales por los Gobiernos y las empresas

Aumento de la huella digital

12. Tanto los Estados como las empresas reúnen y utilizan una cantidad cada vez mayor de datos relacionados con la vida privada de las personas. Las computadoras personales, los teléfonos inteligentes, los relojes inteligentes, los medidores de actividad física y otros dispositivos portátiles recopilan inmensos flujos de datos sobre miles de millones de personas. Además, un número cada vez mayor de dispositivos y sensores interconectados instalados en los llamados hogares inteligentes y ciudades inteligentes añaden datos adicionales. La información que se reúne y utiliza es enorme en alcance y profundidad, y abarca desde identificadores de dispositivos, direcciones de correo electrónico y números de teléfono hasta datos biométricos, médicos y financieros y pautas de conducta. Muchas de esas actividades se realizan sin el conocimiento de las personas afectadas y sin su consentimiento válido.

Intercambio y fusión de datos

13. Las empresas y los Estados intercambian y fusionan constantemente datos personales procedentes de diversas fuentes y bases de datos, y los corredores de datos tienen un papel fundamental en el proceso. Como resultado, las personas se encuentran en una posición de indefensión, ya que resulta prácticamente imposible llevar un seguimiento de quién tiene información sobre ellas y de qué tipo de información se trata, y aún más controlar las múltiples formas en que puede ser utilizada.

Datos biométricos

14. Los Estados y las empresas cada vez hacen más uso de sistemas basados en la recopilación y el uso de datos biométricos, como el ADN, la geometría facial, la voz, los patrones de la retina o el iris y las huellas dactilares. Algunos países han creado enormes bases de datos centralizadas que almacenan ese tipo de información para una amplia variedad de fines, desde la seguridad nacional y la investigación penal hasta la identificación de personas con miras a la prestación de servicios esenciales, como servicios sociales, financieros o educativos. Las autoridades estatales de todo el mundo instalan en las ciudades, las estaciones de tren o los aeropuertos cámaras de televisión de circuito cerrado que utilizan el reconocimiento facial para identificar y caracterizar automáticamente a las personas. Las tecnologías biométricas se utilizan cada vez más para el control de la migración, tanto en las fronteras como dentro de los países. La creación de bases de datos de información biométrica a gran escala suscita graves preocupaciones por sus consecuencias para los derechos humanos. Estos son datos particularmente delicados, ya que, por definición, están indisociablemente vinculados a una persona concreta y a su vida, y pueden ser objeto de vulneraciones graves. Por ejemplo, el robo de la identidad a través de los datos biométricos es muy difícil de reparar y puede afectar gravemente a los derechos de una persona. Además, esos datos pueden utilizarse para fines distintos de aquellos para los que se recopilaron, como el seguimiento y la vigilancia ilegales de personas. Teniendo en cuenta esos riesgos, al recopilar datos biométricos se debería prestar especial atención a los principios de necesidad y proporcionalidad. En este contexto, resulta preocupante que algunos Estados hayan emprendido enormes proyectos basados en datos biométricos sin contar con las garantías jurídicas y procesales necesarias.

Aumento de la capacidad de análisis

15. La capacidad de análisis de la tecnología basada en datos sigue aumentando exponencialmente. El análisis de macrodatos y la inteligencia artificial permiten a los Estados y las empresas obtener información cada vez más específica sobre la vida de las personas, hacer deducciones sobre sus características físicas y mentales y crear perfiles de

personalidad detallados. Muchos de los sistemas utilizados por los gobiernos y las empresas han sido creados con ese fin preciso (obtener la mayor cantidad posible de información sobre las personas a fin de analizarlas, establecer sus perfiles, evaluarlas, clasificarlas y, en última instancia, adoptar decisiones, a menudo automatizadas, acerca de ellas).

16. El entorno resultante entraña riesgos para las personas y las sociedades que no deben subestimarse. Por ejemplo, en los últimos años se han registrado filtraciones de datos de gran alcance que han expuesto a las personas afectadas al robo de su identidad y a la divulgación de información privada. Se ha señalado una relación entre la recopilación y el análisis ilegales de datos y las campañas de captación de votantes. Los perfiles, la "puntuación" y la "clasificación" de las personas pueden servir para evaluar si una persona puede optar a seguros de atención médica o de otro tipo y a servicios financieros, entre otras prestaciones. La adopción de decisiones opacas basadas en datos en casos de gran importancia, por ejemplo, procedimientos de sentencia y evaluaciones sobre el riesgo de reincidencia, puede poner en riesgo el respeto de las garantías procesales. El afán de identificar a personas que puedan representar un riesgo para la seguridad en el contexto de las actuaciones policiales predictivas plantea preocupaciones relacionadas con la transparencia, la generalización, la rendición de cuentas y la posibilidad de generar discriminación[18].

B. Vigilancia e interceptación de las comunicaciones por los Estados

Vigilancia a gran escala

17. Muchos Estados siguen llevando a cabo actividades secretas de vigilancia e interceptación de las comunicaciones a gran escala, y recopilando, almacenando y analizando datos de todos los usuarios en una amplia gama de medios de comunicación (por ejemplo, correos electrónicos, llamadas telefónicas y de vídeo, mensajes de texto y sitios web visitados). Aunque algunos Estados afirman que esa vigilancia en masa e indiscriminada es necesaria para proteger la seguridad nacional, esta práctica "no es permisible en virtud del derecho internacional de los derechos humanos, ya que no sería posible realizar un análisis individualizado de la necesidad y la proporcionalidad en el contexto de esas medidas" (véase A/HRC/33/29, párr. 58)[19]. El Tribunal Europeo de Derechos Humanos ha señalado que "un sistema de vigilancia secreta creado para proteger la seguridad nacional puede socavar o incluso destruir la democracia con el pretexto de defenderla"[20].

Acceso a los datos de los usuarios de las empresas

18. Los Estados suelen recurrir a las empresas para recopilar e interceptar datos personales. Por ejemplo, algunos Estados obligan a los proveedores de servicios de telecomunicaciones e Internet a darles acceso directo a los flujos de datos que circulan a través de sus redes. Esos sistemas de acceso directo suscitan una gran preocupación, ya que son particularmente propicios a los abusos y tienden a eludir las garantías procesales fundamentales[21]. Algunos Estados también solicitan acceso a las enormes cantidades de información recopilada y almacenada por proveedores de servicios de telecomunicaciones e Internet. Los Estados siguen imponiendo a las empresas de telecomunicaciones y los proveedores de servicios de Internet la obligación vinculante de conservar los datos de las comunicaciones durante largos períodos de tiempo[22]. Muchas leyes de ese tipo obligan a las empresas a recopilar y almacenar de manera indiscriminada la totalidad de los datos de tráfico de todos los abonados y usuarios en todos los medios de comunicación electrónica. Estas disposiciones limitan la capacidad de las personas de comunicarse de forma anónima,

[18] Véase Ajay Sandhu, "Data driven policing: highlighting some risks associated with predicting crime", Human Rights Centre, Universidad de Essex.

[19] Véase A/HRC/27/37, párr. 25.

[20] Véase *Roman Zakharov c. Rusia*, párr. 232.

[21] Véase *Roman Zakharov c. Rusia*, párr. 270.

[22] Véase CCPR/C/ZAF/CO/1, párrs. 42 y 43, y CCPR/C/PAK/CO/1, párrs. 35 y 36.

implican riesgos de abuso y pueden facilitar la divulgación de información a terceros, incluidos delincuentes, opositores políticos o empresas competidoras mediante piratería u otras filtraciones de datos. Esas leyes exceden los límites de lo que puede considerarse necesario y proporcional[23].

Piratería informática

19. Los Gobiernos parecen recurrir cada vez más a programas informáticos de interceptación maliciosa que se infiltran en los dispositivos digitales de las personas. Este tipo de piratería informática permite la interceptación y recopilación indiscriminada de todo tipo de comunicaciones y datos, cifrados o no, así como el acceso remoto y secreto a los dispositivos personales y los datos almacenados en ellos, lo que facilita la vigilancia en tiempo real y la manipulación de los datos contenidos en esos dispositivos[24]. Esto comporta riesgos que no solo afectan al derecho a la intimidad, sino también a los derechos a la equidad procesal respecto del uso de estas pruebas en las actuaciones judiciales (véase A/HRC/23/40, párr. 62). La piratería informática también plantea problemas importantes de extraterritorialidad, ya que puede afectar a personas en distintas jurisdicciones[25]. Además, esa piratería se basa en explotar las vulnerabilidades de los sistemas de tecnología de la información y las comunicaciones (TIC) y, por lo tanto, contribuye a las amenazas a la seguridad que afectan a millones de usuarios.

Intentos de debilitar el cifrado y el anonimato

20. Los intentos reiterados de los Estados de debilitar la tecnología de cifrado y limitar el acceso a las herramientas de anonimato también suponen una amenaza para la seguridad y la confidencialidad de las comunicaciones y otras actividades en línea. Algunos Estados piden que se introduzcan puertas traseras obligatorias en las comunicaciones cifradas, exigen a los proveedores de servicios de comunicaciones cifradas que proporcionen copias de las claves de cifrado (véase A/HRC/29/32, párrs. 38 a 45) o incluso prohíben o bloquean ciertas aplicaciones de comunicación segura, en particular servicios de mensajería cifrada y redes virtuales privadas y anónimas. El cifrado y el anonimato brindan a los individuos y a los grupos una zona de vida privada en línea para sostener opiniones y ejercer la libertad de expresión sin injerencia o ataques arbitrarios o ilegales (A/HRC/29/32)[26]. Las herramientas de cifrado y anonimato son muy utilizadas en todo el mundo, en particular por los defensores de los derechos humanos, la sociedad civil, los periodistas, los denunciantes de irregularidades y los disidentes políticos que son objeto de persecución y acoso. Al debilitarlas, se atenta contra la vida privada de todos los usuarios, que quedan expuestos a las injerencias ilícitas no solo de los Estados, sino también de agentes no estatales, incluidas las redes delictivas[27]. Ese efecto generalizado e indiscriminado no es compatible con el principio de proporcionalidad (véase A/HRC/29/32, párr. 36).

Intercambio de información de inteligencia

21. Los Gobiernos de todo el mundo suelen intercambiar información sobre personas sin sujeción a un marco jurídico ni a una supervisión adecuada[28]. El intercambio de inteligencia

[23] Véanse, por ejemplo, los asuntos acumulados núms. C-203/15 y C-698/15, *Tele2 Sverige AB c. Swedish Post* y *Telecom Authority* y *Secretary of State for the Home Department c. Watson*, sentencia de 21 de diciembre de 2016, párr. 107; CCPR/C/ZAF/CO/1, párrs. 42 y 43; y CCPR/C/CMR/CO/5, párrs. 39 y 40.

[24] Véase Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, "Encryption and anonymity follow-up report" (junio de 2018).

[25] Véase la comunicación de Privacy International.

[26] Véase también UCI Law International Justice Clinic, "Selected references: unofficial companion to report of the Special Rapporteur (A/HRC/29/32) on encryption, anonymity and the freedom of expression"; Amnistía Internacional, "Encryption. A matter of human rights" (marzo de 2016); y Wolfgang Schulz y Joris van Hoboken, "Human rights and encryption", Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura (2016).

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

[28] Véase Privacy International, *Secret Global Surveillance Networks: Intelligence Sharing between Governments and the Need for Safeguards* (abril de 2018), y www.ohchr.org/Documents/Issues/DigitalAge/ReportPrivacyinDigitalAge/SRCT.pdf.

plantea el grave riesgo de que un Estado pueda utilizar ese enfoque para eludir las limitaciones jurídicas internas sirviéndose de terceros para obtener y después compartir información. Esa práctica no cumpliría el criterio de la legalidad y podría socavar la esencia del derecho a la privacidad (véase A/HRC/27/37, párr. 30). La amenaza para la protección de los derechos humanos es particularmente grave cuando se comparte información de inteligencia con Estados que cuentan con un estado de derecho deficiente o un historial de violaciones sistemáticas de los derechos humanos. La información que un Estado recibe de otro puede haber sido obtenida por medios contrarios al derecho internacional, como la tortura y otros tratos o penas crueles, inhumanos o degradantes. Los riesgos para los derechos humanos que resultan del intercambio de información de inteligencia se ven agravados por la actual falta de transparencia, rendición de cuentas y supervisión de los acuerdos de intercambio de información (véanse A/69/397, párr. 44, CCPR/C/GBR/CO/7, párr. 24, y CCPR/C/SWE/CO/7, párr. 36). Excepto en contadas ocasiones, la legislación no prevé un marco reglamentario adecuado para el intercambio de inteligencia que cumpla con el principio de legalidad consagrado en el derecho internacional de los derechos humanos[29].

Acceso transfronterizo a los datos de las empresas

22. En los últimos tiempos se han realizado esfuerzos por crear mecanismos jurídicos que faciliten el acceso de los Estados a la información personal almacenada en los servidores de las empresas en el extranjero. La obtención de pruebas en el marco de las investigaciones penales constituye, sin duda, un objetivo importante y legítimo. No obstante, ese acceso puede resultar en el debilitamiento o la elusión de las garantías procesales, como el requisito de autorización por un órgano independiente y el establecimiento de mecanismos de supervisión adecuados. Las solicitudes de datos transfronterizas también pueden tener efectos negativos en el acceso de las personas a procedimientos de apelación y mecanismos de reparación. Resulta particularmente preocupante que los Estados en los que el estado de derecho es deficiente o tienen un historial problemático de derechos humanos puedan obtener acceso a información personal sensible sin una protección adecuada frente a las vulneraciones de los derechos humanos.

IV. Responsabilidades de los Estados

A. Responsabilidad de los Estados de respetar y obligación de proteger el derecho a la privacidad en la era digital

23. El artículo 2, párrafo 1, del Pacto Internacional de Derechos Civiles y Políticos dispone que los Estados se comprometen a “respetar y garantizar” a todos los individuos que se encuentren en su territorio y estén sujetos a su jurisdicción los derechos reconocidos en el Pacto, sin discriminación alguna. Los Estados partes deben abstenerse de violar los derechos reconocidos por el Pacto y cualesquiera restricciones a cualquiera de esos derechos debe ser permisible de conformidad con las disposiciones pertinentes del Pacto[30]. Sin embargo, las obligaciones de los Estados van más allá del deber de respetar y también incluyen medidas “positivas” para proteger el disfrute de los derechos. En el contexto del derecho a la privacidad, eso implica el deber de adoptar medidas legislativas y de otra índole para hacer efectivas la prohibición de injerencias y ataques arbitrarios o ilegales, provengan de las autoridades estatales o de personas físicas o jurídicas[31].

24. El deber de proteger se refleja en el primer pilar de los Principios Rectores sobre las Empresas y los Derechos Humanos, titulado “El deber del Estado de proteger los derechos humanos”, en el que se explica en detalle lo que implica el deber de los Estados de prestar protección frente a las consecuencias negativas de las actividades de las empresas sobre los derechos humanos. El primero de los Principios Rectores exige que se adopten las medidas apropiadas para prevenir, investigar, castigar y reparar las violaciones de los derechos

[29] Véase la comunicación de Privacy International.

[30] Véase Comité de Derechos Humanos, observación general núm. 31, párr. 6.

[31] Véase Comité de Derechos Humanos, observaciones generales núm. 16, párrs. 1 y 9, y núm. 31, párr. 8.

humanos mediante políticas adecuadas, actividades de reglamentación y sometimiento a la justicia. En los demás principios se presentan las diferentes esferas jurídicas y normativas en las que los Estados deben adoptar "una combinación inteligente de medidas" —nacionales e internacionales, obligatorias y facultativas— para promover el respeto de los derechos humanos por las empresas[32]. Un ejemplo de la aplicación del enfoque presentado en los Principios Rectores en relación con el sector de las TIC son las orientaciones sectoriales elaboradas en el ámbito de la Unión Europea, centradas en el modo en que las empresas de TIC deberían abordar cualquier efecto perjudicial de sus actividades.

25. El deber de los Estados de proteger contra las vulneraciones del derecho a la vida privada por parte de las empresas y otros terceros constituidos o domiciliados en su jurisdicción tiene efectos extraterritoriales. Por ejemplo, los regímenes de control de las exportaciones aplicados por los Estados a la tecnología de vigilancia deberían prever la evaluación del marco jurídico que rige el uso de la tecnología en el país de destino, el historial de derechos humanos del usuario final previsto y las salvaguardias y procedimientos de supervisión vigentes para el uso de las facultades de vigilancia. Los acuerdos de concesión de licencias de exportación deberían exigir garantías de derechos humanos. Además, los Estados tienen el deber de proteger a las personas que se encuentran en su jurisdicción frente a las injerencias extraterritoriales en su derecho a la intimidad, como los medios de interceptación de comunicaciones o la piratería informática.

B. Responsabilidad del Estado de establecer salvaguardias adecuadas y una supervisión eficaz

26. El disfrute del derecho a la privacidad depende en gran medida de la existencia de un marco jurídico, reglamentario e institucional que prevea salvaguardias adecuadas, en particular mecanismos de supervisión eficaces. En una época en la que los Estados y las empresas pueden acceder a una gran cantidad de datos personales y las personas tienen un conocimiento limitado del uso que se da a la información sobre ellas y sus vidas, resulta fundamental centrarse en la adopción de medidas que mitiguen las consecuencias que esas asimetrías de poder e información tienen sobre los derechos humanos.

1. Marco general de protección contra injerencias indebidas

27. El marco de protección de la privacidad de un Estado debe basarse en leyes que establezcan las normas para el tratamiento de la información personal, tanto por los Estados como por agentes privados[33]. Aunque los Estados tienen un margen de discrecionalidad para definir la combinación inteligente de medidas que rigen el uso de la información personal por las empresas, el artículo 17, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos prevé la obligación de brindar a las personas la protección de la ley. La interconexión creciente del tratamiento de datos públicos y privados y el historial de uso indebido de información personal a gran escala y de manera recurrente por algunas empresas confirman que es necesario adoptar medidas legislativas para lograr un nivel adecuado de protección de la privacidad[34].

28. Cada vez existe un mayor consenso mundial acerca de la necesidad de unas normas mínimas que rijan el tratamiento de los datos personales por los Estados, las empresas y otros agentes del sector privado. Entre los instrumentos y directrices internacionales que reflejan estos avances están los Principios Rectores sobre la reglamentación de los ficheros

[32] Véase el comentario del principio 2.

[33] Véanse la observación general núm. 16, párr. 9, del Comité de Derechos Humanos, A/HRC/13/37, párr. 61, y A/HRC/17/27, párr. 56. Para un panorama general de la legislación sobre protección de datos, véase la comunicación de Graham Greenleaf, Universidad de Nueva Gales del Sur, para el presente informe. En el presente informe, se entiende que el "tratamiento" comprende cualquier operación que se realice en relación con los datos personales, lo que incluye la recopilación, la conservación, el uso, la modificación, la eliminación, la divulgación, la transferencia y la combinación.

[34] Véanse las resoluciones 34/7, párr. 5 f), y 38/7, párr. 17, del Consejo de Derechos Humanos.

computadorizados de datos personales de 1990; el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal del Consejo de Europa, de 1981, y su versión actualizada, que prevé un alto grado de protección a nivel mundial[35]; las Directrices sobre Privacidad de la Organización de Cooperación y Desarrollo Económicos, de 1980, actualizadas en 2013; la Convención de la Unión Africana sobre Ciberseguridad y Protección de Datos Personales (Convención de Malabo), de 2014; la resolución de Madrid de la Conferencia Internacional de Autoridades de Protección de Datos y Privacidad; y el Marco de Privacidad del Foro de Cooperación Económica Asia Pacífico, de 2015, entre otros. Esas normas, en particular el Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal, han servido de base para la elaboración de los marcos de protección de datos de muchos Estados y pueden utilizarse para el diseño de instrumentos de política adecuados[36].

29. Los instrumentos y directrices mencionados contienen una serie de principios, derechos y obligaciones fundamentales que garantizan un nivel mínimo de protección de los datos personales. En primer lugar, el tratamiento de los datos personales debe ser justo, legítimo y transparente. Las personas cuyos datos personales se están tratando deberían ser informadas sobre el tratamiento de datos, sus circunstancias, su carácter y su alcance, entre otras cosas mediante políticas transparentes de protección de datos. Para prevenir el uso arbitrario de la información personal, el tratamiento de datos personales debería basarse en el consentimiento libre, específico, informado y sin ambigüedades de las personas interesadas, o en otro fundamento legítimo previsto en la ley[37]. El tratamiento de datos personales debe ser necesario y proporcional a un fin legítimo que la entidad que trata los datos debe especificar. Por consiguiente, la cantidad y el tipo de datos y el período de conservación deben ser limitados, los datos deben ser precisos y, en la medida de lo posible, deben utilizarse técnicas de anonimato y seudonimización. Deben evitarse los cambios de finalidad sin el consentimiento de la persona interesada, y cuando se produzcan, han de limitarse a fines compatibles con el señalado en un inicio. Dado que los datos personales son susceptibles de divulgación, modificación o eliminación no autorizadas, es esencial que se adopten medidas de seguridad adecuadas. Además, las entidades que tratan datos personales deben hacerse responsables del cumplimiento de las disposiciones aplicables del marco jurídico y normativo para el tratamiento de datos. Por último, los datos sensibles deben gozar de un nivel particularmente elevado de protección[38].

30. En todos los instrumentos y directrices mencionados se reconoce que las personas cuyos datos se están tratando deben gozar de ciertos derechos. Como mínimo, las personas afectadas tienen derecho a saber que sus datos personales se han conservado y tratado, a acceder a los datos almacenados, a rectificar los datos inexactos u obsoletos y a suprimir o corregir los datos almacenados de manera ilícita o innecesaria. En los instrumentos más recientes se han añadido derechos adicionales importantes, en particular, el derecho de oposición al tratamiento de datos personales, al menos en los casos en que la entidad que trata los datos no demuestre que existen motivos legítimos e imperativos para su tratamiento[39]. Los Estados deben centrarse de manera particular en brindar una protección sólida frente a la injerencia en el derecho a la privacidad mediante la elaboración de perfiles y la toma de decisiones automatizada. Los derechos anteriormente descritos también deben aplicarse a la información obtenida, inferida y predicha por medios automáticos, en la

[35] Además de los 47 Estados miembros del Consejo de Europa, la Convención ha sido ratificada por Mauricio, el Senegal, Túnez y el Uruguay, y otros Estados han iniciado ya el proceso de adhesión.

[36] Para obtener orientación detallada, véase: https://privacyinternational.org/advocacy-briefing/2165/guide-policy-engagement-data-protection y Access Now, “Creating a data protection framework: a do’s and don’ts guide for lawmakers. Lessons from the EU general data protection regulation” (2018).

[37] Véase el artículo 5, párrafo 2, de la versión actualizada del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal; el artículo 13, párrafo 1, de la Convención de Malabo; y el principio 12 de la resolución de Madrid.

[38] Véase el artículo 6 de la versión actualizada del Convenio para la Protección de las Personas con respecto al Tratamiento Automatizado de Datos de Carácter Personal.

[39] *Ibid*., artículo 9, párrafo 1 d). Véase también el artículo 21 del Reglamento general de protección de datos y el artículo 18, párrafo 1, de la Convención de Malabo.

medida en que esa información pueda ser considerada personal. Es importante que el marco jurídico garantice que esos derechos no limiten indebidamente el derecho a la libertad de expresión, incluido el tratamiento de datos personales para fines periodísticos, artísticos y académicos.

31. Los marcos para la protección de datos también deben imponer ciertas obligaciones a las entidades que tratan datos personales. Estas obligaciones incluyen determinados aspectos de organización, como el establecimiento de un mecanismo de supervisión interna, pero también medidas obligatorias, como la notificación de las filtraciones de datos y la evaluación del impacto de sus actividades en la privacidad. En un entorno tecnológico cada vez más complejo, estas evaluaciones tienen un papel fundamental en la prevención y mitigación de las vulneraciones de la vida privada[40]. Además, los requisitos relativos al diseño de los productos y servicios, como la protección de la privacidad desde el diseño[41] y la protección de la privacidad por defecto[42], son herramientas esenciales para la salvaguarda del derecho a la privacidad.

32. En un mundo globalizado, las transferencias de datos, en particular de grandes cantidades de datos personales, son una práctica común que resulta necesaria para el funcionamiento de muchos servicios. Los Estados deben velar por que esas transferencias no conlleven o faciliten la injerencia indebida en el derecho a la privacidad. Al mismo tiempo, deben evitar los requisitos estrictos de localización de datos que obligan a todas las entidades que tratan los datos a almacenar toda la información personal en el territorio del país en cuestión (véase A/HRC/32/38, párr. 61). En lugar de eso, los Estados deben centrarse en encontrar formas de garantizar que los datos personales transferidos a otro Estado estén protegidos, como mínimo, en la medida exigida por el derecho internacional de los derechos humanos.

33. Los Estados deben establecer órganos de supervisión independientes para el tratamiento de datos personales. Esos órganos son fundamentales para proteger los derechos humanos de las personas frente el recurso excesivo a las prácticas de tratamiento de datos personales. La autoridad de supervisión debe contar con una base jurídica que establezca claramente su mandato, sus atribuciones y su independencia. Los órganos de supervisión deben contar con los recursos técnicos, financieros y humanos necesarios para supervisar eficazmente las actividades de tratamiento de datos de los Estados y las empresas, y para hacer cumplir los requisitos legales en esa esfera. Además, deben tener la autoridad jurídica necesaria para desempeñar sus funciones, en particular para imponer sanciones proporcionales a las violaciones o abusos cometidos[43].

2. Salvaguardias de procedimiento y supervisión de la vigilancia y la interceptación de las comunicaciones

Salvaguardias

34. Aunque todos los tipos de actividades de vigilancia deben realizarse sobre la base de una ley (véase A/HRC/27/37, párr. 28), el Relator Especial sobre el derecho a la privacidad ha señalado que existe una falta generalizada de legislación en esa esfera. Cabe señalar que, en muchas jurisdicciones, los servicios de inteligencia y los organismos encargados de hacer cumplir la ley quedan fuera del ámbito de aplicación de las leyes de protección de datos. En virtud de los principios de necesidad y proporcionalidad, esas excepciones deberían limitarse a fin garantizar un nivel adecuado de protección de los datos en todos los poderes del Estado. La legislación específica sobre vigilancia debería cumplir los criterios mínimos que se presentan a continuación.

[40] Para un análisis exhaustivo de diversos enfoques de las evaluaciones del impacto en la privacidad, véase David Wright y Paul de Hert, eds., *Privacy Impact Assessment* (Nueva York, Springer, 2012).

[41] Implica que la protección de la vida privada debe integrarse desde el primer momento cuando se diseña un sistema.

[42] Requiere que un sistema aplique por defecto parámetros de protección de la privacidad.

[43] Véase, por ejemplo, https://ico.org.uk/action-weve-taken/investigation-into-data-analytics-for-political-purposes/.

35. La legislación debe ser de acceso público. Las normas y las interpretaciones secretas del derecho no cumplen los requisitos necesarios para considerarse "ley" (*ibid*., párr. 29). Las leyes deben ser suficientemente precisas. La discrecionalidad otorgada a los poderes ejecutivo y judicial y la manera de ejercer esa discrecionalidad se debe circunscribir con claridad razonable (véase A/69/397, párr. 35)[44]. Para ese fin, es necesario describir la naturaleza del delito y las categorías de personas que pueden ser objeto de vigilancia. Las justificaciones imprecisas y excesivamente amplias, como las referencias vagas a la "seguridad nacional", no pueden considerarse disposiciones suficientemente claras. La vigilancia debe basarse en sospechas razonables, y toda decisión que la autorice debe ser suficientemente específica[45]. La ley debe asignar de manera estricta las competencias necesarias para llevar a cabo actividades de vigilancia y acceder a los resultados de estas a autoridades concretas.

36. En lo que respecta a su alcance, el marco jurídico de la vigilancia debe abarcar las solicitudes presentadas por los Estados a las empresas. También debe abarcar el acceso a información conservada extraterritorialmente o el intercambio de información con otros Estados. Debe establecerse por ley una estructura para garantizar la rendición de cuentas y la transparencia en los organismos públicos que realizan actividades de vigilancia.

37. Las facultades de vigilancia secreta solo pueden justificarse en la medida en que sean estrictamente necesarias para lograr un objetivo legítimo y cumplan el requisito de proporcionalidad (véase A/HRC/23/40, párr. 83 b))[46]. Las medidas de vigilancia secretas deben limitarse a prevenir o investigar los delitos o amenazas más graves. La duración de la vigilancia debe limitarse al mínimo estrictamente necesario para lograr el objetivo especificado. Debe haber normas rigurosas para utilizar y almacenar los datos obtenidos, y las circunstancias en que hay que eliminar los datos recopilados y almacenados deben definirse claramente[47]. El intercambio de inteligencia debe estar sujeto a los mismos principios de legalidad, estricta necesidad y proporcionalidad.

38. Al valorar la posibilidad de utilizar medidas de piratería selectivas, los Gobiernos deben ser sumamente cautelosos y recurrir a ellas únicamente en circunstancias excepcionales para investigar y prevenir los delitos o amenazas más graves, y contar con la participación del poder judicial (véase CCPR/C/ITA/CO/6, párr. 37)[48]. El diseño de las operaciones de piratería debe tener un enfoque estricto, de modo que el acceso a la información se limite a objetivos y tipos de información concretos. Los Estados deben abstenerse de obligar a las entidades privadas a que presten asistencia en las operaciones de piratería, lo que afecta la seguridad de sus propios productos y servicios. El descifrado obligado solo puede ser admisible cuando se aplique de forma selectiva y en función de cada caso y cuando esté sujeto a la orden de un juez y a la protección del derecho a las debidas garantías procesales (véase A/HRC/29/32, párr. 60).

Autorización y supervisión independientes[49]

39. Las medidas de vigilancia, incluidas las peticiones de datos sobre comunicaciones a las empresas y el intercambio de inteligencia, deben ser autorizadas, examinadas y supervisadas por órganos independientes en todas las etapas, entre otras cuando se emite la orden inicial, mientras se están aplicando las medidas y una vez estas han concluido (véase CCPR/C/FRA/CO/5, párr. 5)[50]. El órgano independiente que autoriza las medidas de vigilancia concretas, preferiblemente una autoridad judicial, debe asegurarse de que existen pruebas claras de una amenaza lo suficientemente importante y de que la propuesta de

[44] Véase también *Roman Zakharov c. Rusia*, párr. 230.

[45] *Ibid*., párrs. 248 y 260.

[46] Véase también *Szabo y Vissy c. Hungría*, párr. 73.

[47] Véase *Roman Zakharov c. Rusia*, párr. 231.

[48] Véanse también Access Now, "A human rights response to government hacking" (septiembre de 2016) y Privacy International, "Government hacking and surveillance: 10 necessary safeguards".

[49] Véase A/HRC/34/60 y Agencia de los Derechos Fundamentales de la Unión Europea, *Surveillance by Intelligence Services: Fundamental Rights Safeguards and Remedies in the EU. Volume II: Field Perspectives and Legal Update*, (Luxemburgo, Oficina de Publicaciones de la Unión Europea, 2017).

[50] Véase *Roman Zakharov c. Rusia*, párr. 233.

vigilancia tiene un fin específico y es estrictamente necesaria y proporcional, y autorizar (o rechazar) *ex ante* las medidas de vigilancia.

40. Los marcos de supervisión pueden estar compuestos por una combinación de medidas de supervisión administrativa, judicial y/o parlamentaria[51]. Los órganos de supervisión deben ser independientes de las autoridades que llevan a cabo la vigilancia y disponer de conocimientos técnicos, competencias y recursos pertinentes y adecuados. La autorización y la supervisión deben estar a cargo de distintas instituciones. Los organismos de supervisión independientes deben investigar y supervisar de forma proactiva las actividades de las entidades que realizan la vigilancia, tener acceso a los resultados de la vigilancia y llevar a cabo exámenes periódicos de las capacidades de vigilancia y los avances tecnológicos. Los organismos que llevan a cabo la vigilancia deben tener la obligación de facilitar toda la información necesaria para una supervisión eficaz cuando se les solicite y de presentar informes periódicos a los órganos de supervisión, así como de llevar registros de todas las medidas de vigilancia adoptadas[52]. Los procesos de supervisión también deben ser transparentes y estar sujetos a escrutinio público adecuado, y las decisiones de los órganos de supervisión deben poder ser objeto de recurso o de revisión independiente. En ausencia de un proceso contradictorio, es particularmente importante que los órganos de supervisión estén expuestos a puntos de vista divergentes, por ejemplo a través de consultas con expertos y diversas partes interesadas (véase por ejemplo A/HRC/34/60, párr. 36), es esencial que se introduzcan "puntos de fricción" (cuestionamientos constantes de sus enfoques e interpretaciones)[53].

Principio de transparencia

41. Las autoridades estatales y los órganos de supervisión también deberían informar al público de las leyes, políticas y prácticas vigentes en materia de vigilancia e interceptación de las comunicaciones y otras formas de tratamiento de los datos personales, ya que el debate y el escrutinio público son esenciales para comprender las ventajas y limitaciones de las técnicas de vigilancia (véase A/HRC/13/37, párr. 55). Las personas que han sido sometidas a vigilancia deben ser informadas, y se les debe explicar *a posteriori* la injerencia en su derecho a la intimidad. Esas personas también deberían tener derecho a modificar o eliminar información personal no pertinente, siempre y cuando esa información ya no sea necesaria para llevar a cabo una investigación en curso o pendiente (véase A/HRC/34/60, párr. 38).

V. Responsabilidades de las empresas

42. En el segundo pilar de los Principios Rectores sobre las Empresas y los Derechos Humanos se presenta un plan oficial aplicable a todas las empresas, independientemente de su tamaño, sector, contexto operacional, propietario y estructura, para prevenir y abordar todas las consecuencias negativas de sus actividades sobre los derechos humanos, incluido el derecho a la privacidad[54]. Se señala la responsabilidad de las empresas de respetar todos los derechos humanos internacionalmente reconocidos, lo que significa que deben abstenerse de infringir los derechos humanos de terceros y hacer frente a las consecuencias negativas sobre los derechos humanos en las que tengan alguna participación[55]. La responsabilidad de respetar los derechos humanos abarca todas las actividades y relaciones comerciales de una empresa. Resulta particularmente importante su aplicación al espacio digital, con independencia del lugar en que se encuentren las personas afectadas. La responsabilidad de respetar existe independientemente de que el Estado cumpla con sus propias obligaciones de derechos humanos.

[51] Véase la resolución 71/199, de la Asamblea General, párr. 5 d).

[52] Véase Tribunal Europeo de Derechos Humanos, *Kennedy c. el Reino Unido*, demanda núm. 26839/05, sentencia de 18 de mayo 2010, párr. 165, y *Roman Zakharov c. Rusia*, párr. 272.

[53] Véase Human Rights, Big Data and Technology Project, Human Rights Centre, Universidad de Essex, comunicación para el presente informe.

[54] Los Principios Rectores recibieron el apoyo unánime del Consejo de Derechos Humanos en su resolución 17/4.

[55] Principio rector 11.

43. La responsabilidad de respetar los derechos humanos exige que las empresas: a) eviten que sus propias actividades provoquen consecuencias negativas sobre los derechos humanos; b) eviten que sus propias actividades contribuyan a provocar consecuencias negativas, ya sea directamente o a través de una entidad externa (Gobierno, empresas u otras); y c) traten de prevenir o mitigar las consecuencias negativas sobre los derechos humanos directamente relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlo[56]. Por ejemplo, una empresa que facilite datos sobre sus usuarios a un Gobierno que posteriormente los utilice para localizar y enjuiciar a disidentes políticos habrá contribuido a esas violaciones de los derechos humanos, incluido el derecho a la privacidad. Las empresas que fabriquen y vendan tecnologías que se utilicen en injerencias ilegales o arbitrarias también estarán contribuyendo a provocar consecuencias negativas sobre los derechos humanos.

44. Si existe un conflicto de exigencias entre el respeto del derecho internacional de los derechos humanos y las obligaciones previstas en la legislación nacional, las empresas deben esforzarse por ajustarse al derecho internacional de los derechos humanos en la medida de lo posible y por mitigar al máximo los efectos negativos de sus actividades, por ejemplo, haciendo una interpretación lo más restrictiva posible de las exigencias de los Gobiernos[57].

45. La responsabilidad de respetar los derechos humanos exige a las empresas que cuenten con políticas y procedimientos apropiados en función de su tamaño y circunstancias, a saber:

a) Que hagan público un compromiso político aprobado al más alto nivel directivo e incluyan la responsabilidad de respetar los derechos humanos en todas las políticas y los procedimientos operacionales[58];

b) Que procedan con la debida diligencia en materia de derechos humanos, lo que implica:

i) Realizar evaluaciones del impacto de sus actividades para identificar y evaluar las consecuencias negativas reales o potenciales que puedan tener sobre los derechos humanos;

ii) Integrar esas evaluaciones y tomar las medidas oportunas para prevenir y mitigar las consecuencias negativas sobre los derechos humanos que se hayan identificado;

iii) Hacer un seguimiento de la eficacia de sus esfuerzos;

iv) Informar oficialmente de cómo han abordado las consecuencias de sus actividades sobre los derechos humanos[59];

c) Reparar o contribuir a reparar los abusos cuando la empresa determine que ha provocado o contribuido a provocar consecuencias negativas[60].

46. De acuerdo con los Principios Rectores, todas las empresas tienen la responsabilidad de aplicar la debida diligencia en materia de derechos humanos al identificar y evaluar las consecuencias de sus actividades. Por ejemplo, como parte de la debida diligencia, las empresas que venden tecnología de vigilancia deben llevar a cabo una rigurosa evaluación del impacto sobre los derechos humanos antes de realizar cualquier transacción. Para mitigar el riesgo, es necesario que en los acuerdos contractuales se establezcan garantías claras del uso final mediante salvaguardias firmes de los derechos humanos que impidan la utilización arbitraria o ilegal de la tecnología y exámenes periódicos de la utilización de la

[56] Principio rector 13. Véase también ACNUDH, “La responsabilidad de las empresas de respetar los derechos humanos: Guía para la interpretación” (2012).
[57] Principio rector 23.
[58] Principio rector 16.
[59] Principios rectores 17 a 21.
[60] Principio rector 22 y sección VI del presente informe.

tecnología por los Estados[61]. Las empresas que recopilan y conservan datos de sus usuarios deben evaluar los riesgos para la privacidad asociados a las potenciales peticiones de esos datos por parte de los Estados, en particular el entorno jurídico e institucional de los Estados en cuestión. Deben prever procedimientos y salvaguardias apropiados para prevenir y mitigar las posibles vulneraciones de la privacidad y otros derechos humanos. También es necesario llevar a cabo evaluaciones del impacto sobre los derechos humanos a la hora de aprobar las condiciones de servicio y las opciones de diseño e ingeniería que afectan a la seguridad y la privacidad y de adoptar decisiones relativas a la prestación o rescisión de los servicios en un mercado determinado (véase A/HRC/32/38, párr. 11).

47. Como parte del proceso de diligencia debida en materia de derechos humanos, los Principios Rectores establecen que las empresas deben explicar la manera en que abordan las consecuencias de sus actividades sobre los derechos humanos y estar preparadas para comunicarlas externamente, sobre todo cuando los afectados o sus representantes planteen sus inquietudes[62]. En el entorno digital, esto implica divulgar cuáles son los datos personales que se recopilan, durante cuánto tiempo se almacenan, con qué fin, cómo se utilizan y con quién y en qué circunstancias se comparten. Esto incluye las peticiones de los Estados para acceder a los datos de los usuarios. En los casos en que las leyes y los reglamentos nacionales obstaculicen la presentación de esa información, las empresas deben recurrir en la mayor medida posible a cualquier influencia que puedan tener, y se les alienta a defender su derecho a divulgar esa información.

48. Como parte de la puesta en práctica de los compromisos políticos contraídos en virtud de los Principios Rectores, el sector de las TIC ha elaborado directrices para la aplicación de políticas de derechos humanos. Entre esas iniciativas están los Principios de Libertad de Expresión y Privacidad de Global Network Initiative (Principios de la GNI)[63] y los Principios Rectores del Grupo de Diálogo de la Industria de las Telecomunicaciones[64]. Por ejemplo, los Principios de la GNI declaran expresamente que las empresas participantes "emplearán protección con respecto a la información personal" y "respetarán y trabajarán para proteger los derechos de privacidad de los usuarios cuando se enfrenten a demandas del Gobierno, leyes o regulaciones que comprometan la privacidad en forma inconsistente con las leyes y estándares internacionalmente reconocidos".

49. El Índice de Responsabilidad Empresarial de Ranking Digital Rights Corporate evalúa una serie de empresas de Internet, telefonía móvil y telecomunicaciones centrándose específicamente en sus compromisos de divulgación y sus políticas en lo que respecta a la libertad de expresión y la privacidad[65]. Este podría ser un instrumento útil para pedir responsabilidades a las empresas por el impacto de sus actividades en los derechos de los usuarios.

VI. Mecanismos de reparación

50. Las víctimas de vulneraciones o violaciones de la privacidad cometidas por los Estados o las empresas deben tener acceso a mecanismos de reparación eficaces. Los Estados no solo tienen la obligación de velar por la rendición de cuentas y la reparación ante las violaciones de los derechos humanos perpetradas por agentes estatales, sino que también deben adoptar las medidas apropiadas para garantizar que las víctimas de violaciones de los derechos humanos relacionadas con empresas tengan acceso a mecanismos de reparación eficaces (véase el pilar III de los Principios Rectores sobre las Empresas y los Derechos Humanos). Según la naturaleza de cada caso o situación, las víctimas deben tener acceso a reparación a través de mecanismos de reclamación judiciales

[61] Véase Privacy International, comunicación presentada al Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión (enero de 2016). Puede consultarse en: www.ohchr.org/Documents/Issues/Expression/PrivateSector/PrivacyInternational.pdf.

[62] Principio rector 21.

[63] Puede consultarse en: https://globalnetworkinitiative.org/gni-principles/. Véase también Global Network Initiative, comunicación para el presente informe.

[64] Puede consultarse en: www.telecomindustrydialogue.org/about/guiding-principles/.

[65] Véase https://rankingdigitalrights.org/index2018/.

o extrajudiciales eficaces (A/HRC/32/19, Corr.1 y Add.1 y A/HRC/38/20 y Add.1). Entre los mecanismos estatales extrajudiciales competentes en la esfera de las TIC están las autoridades independientes con facultades para supervisar las prácticas del Estado y el sector privado en la esfera de la protección de datos, como los organismos de protección de la privacidad y los organismos de protección de datos.

51. Con arreglo a los Principios Rectores, si las empresas determinan que han provocado o contribuido a provocar consecuencias negativas sobre los derechos humanos deben repararlas o contribuir a su reparación por medios legítimos[66]. Para que un mecanismo extrajudicial sea eficaz, debe ser legítimo, accesible, predecible, equitativo, compatible con los derechos, transparente, fuente de aprendizaje continuo y, en el caso de los mecanismos de reclamación de nivel operacional, basarse en la participación y el diálogo[67].

52. En el Principio rector 19 se explican con detalle las medidas que deben adoptarse cuando una empresa no haya provocado o contribuido a provocar consecuencias negativas pero esas consecuencias estén directamente relacionadas con operaciones, productos o servicios prestados por sus relaciones comerciales. Entre ellas puede estar el ejercicio de la influencia que la empresa pueda tener sobre su socio o cliente para conseguir que ofrezca reparación[68].

53. Los Principios Rectores también ponen de relieve el papel que pueden desempeñar los mecanismos de reclamación de nivel operacional al abordar las reclamaciones de forma directa. Esos mecanismos pueden adoptar diversas formas en función del tipo de empresa afectada, las necesidades de las partes interesadas y el perfil de riesgo de la empresa en lo que respecta a los derechos humanos. Para determinar cómo pueden diseñarse y aplicarse en la práctica esos mecanismos en el sector de las TIC, es necesario seguir celebrando debates dentro del sector y en consulta con las partes interesadas.

54. En la práctica, hay importantes deficiencias y obstáculos para acceder a vías de recurso en casos de violaciones de la privacidad. El carácter y los efectos transnacionales de la vigilancia, la interceptación de las comunicaciones y las múltiples formas de tratamiento de datos personales, así como de sus consecuencias, plantea problemas jurídicos y prácticos (véase A/HRC/34/60, párr. 34). Además, la falta de conocimiento de las víctimas o la inexistencia de pruebas de la injerencia indebida constituyen obstáculos frecuentes para el acceso a las vías de recurso (véase A/HRC/27/37, párr. 40). Por ejemplo, las peticiones de los Estados para acceder a los datos que obran en poder de las empresas suelen ir acompañadas de "órdenes de reserva" en las que se prohíbe a estas últimas que informen a las personas interesadas. Además, los Estados no suelen informar a las personas afectadas por otras medidas de vigilancia, en particular en casos de vigilancia a gran escala. Si bien la notificación por adelantado o simultánea podría atentar contra la eficacia de las medidas de vigilancia legales, debe notificarse a las personas una vez que la vigilancia haya finalizado (véase A/HRC/23/40, párr. 82). Si eso no es posible, la ley debería al menos reconocer la legitimidad de las personas que, en teoría, puedan haberse visto afectadas por esas medidas (véase A/HRC/13/37, párr. 38). Asimismo, las empresas deberían informar a sus clientes cuando tomasen conocimiento de la existencia de filtraciones de datos personales que podrían haber afectado a sus derechos.

55. Las víctimas también encuentran obstáculos nuevos y cada vez más importantes en el contexto de la adopción algorítmica de decisiones, ya que las personas pueden no tener acceso a los datos de entrada ni derecho a impugnar las conclusiones del algoritmo o la forma en que las conclusiones se han utilizado para adoptar la decisión[69]. Los Estados y las empresas, en colaboración con otros interesados, deberían valorar posibles mecanismos para abordar esa cuestión, como la creación de órganos de auditoría especializados dotados de recursos suficientes.

[66] Principio rector 22.

[67] Principio rector 31.

[68] Principio rector 19 y su comentario. Véase también ACNUDH, "La responsabilidad de las empresas de respetar los derechos humanos: Guía para la interpretación", págs. 48 a 52.

[69] **¡Error! Referencia de hipervínculo no válida.**Véase la comunicación de la Universidad de Essex "Human Rights, Big Data and Technology Project", párr. 33.

56. La naturaleza de los daños causados por las vulneraciones de la privacidad es fuente de nuevos desafíos. Las consecuencias de ese tipo de abusos son difíciles de reparar y pueden tener efectos persistentes y otras consecuencias para los derechos humanos. La facilidad para conservar, intercambiar, reutilizar y fusionar datos y perfiles influye en la perdurabilidad de los datos digitales, lo que significa que las personas pueden enfrentarse a riesgos nuevos o persistentes para sus derechos en el futuro[70].

57. Las vulneraciones de la privacidad afectan significativamente a la vida de las personas, incluso cuando no hay consecuencias cuantificables económicas o de otra índole; la naturaleza de la vulneración no debería impedir que las víctimas obtuvieran reparación. Una posibilidad sería otorgar a las organizaciones de protección de los consumidores facultades para exigir reparación en nombre de las víctimas de abusos de la privacidad por parte de las empresas.

VII. Conclusiones y recomendaciones

58. **El marco internacional de derechos humanos ofrece una base sólida para formular respuestas a los múltiples desafíos que se plantean en la era digital. Existe la necesidad urgente de que los Estados cumplan plenamente sus obligaciones de respetar el derecho a la privacidad, así como su deber de proteger ese derecho, en particular en relación con los abusos cometidos por las empresas. Para lograr ese objetivo, los Estados deben establecer un marco jurídico y normativo apropiado, en particular leyes y reglamentos adecuados sobre protección de la privacidad que incorporen los principios de legalidad, proporcionalidad y necesidad, y establezcan salvaguardias y mecanismos de supervisión y reparación.**

59. **Existen muchas cuestiones que no han podido abordarse en el presente informe y que requieren un estudio más profundo, en particular la relación entre el derecho a la privacidad y otros derechos humanos, incluidos los derechos económicos, sociales y culturales; las consecuencias desproporcionadas o discriminatorias de las invasiones de la privacidad para las personas o grupos en situación de riesgo; los efectos de los macrodatos y el aprendizaje automático, en particular cuando se aplican a fines predictivos y preventivos, sobre el goce del derecho a la privacidad y otros derechos humanos; y la regulación de los mercados de tecnología de vigilancia.**

60. **Otra esfera a la que debería prestarse mayor atención es la naturaleza y la forma que deben adoptar los mecanismos de reparación para responder de manera eficaz a las situaciones en las que se ha vulnerado el derecho a la privacidad. Como primer paso, deberían identificarse de manera sistemática los tipos de medidas correctivas que resultarían apropiadas para las diferentes situaciones. Esto podría servir para la elaboración de nuevas orientaciones. Al realizar ese análisis, debería prestarse la debida atención a las orientaciones y recomendaciones formuladas en el marco del proyecto sobre rendición de cuentas y reparación de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH). En un plano más general, deberían hacerse esfuerzos para desarrollar instrumentos de orientación sectoriales sobre la responsabilidad de las empresas de respetar el derecho a la privacidad.**

61. **El Alto Comisionado recomienda a los Estados que:**

a) Reconozcan todas las consecuencias de las nuevas tecnologías, en particular las tecnologías basadas en datos, para el derecho a la privacidad, pero también para los demás derechos humanos;

b) Adopten una legislación sólida, rigurosa y exhaustiva sobre privacidad, en particular sobre protección de datos, que se ajuste al derecho internacional de los derechos humanos en lo que respecta a las salvaguardias, la supervisión y la reparación para proteger de manera efectiva el derecho a la intimidad;

[70] *Ibid*., párr. 7.

c) Velen por que los sistemas que emplean un gran volumen de datos, incluidos los que implican la recopilación y conservación de datos biométricos, solo se utilicen cuando los Estados puedan demostrar que son necesarios y proporcionales para lograr un fin legítimo;

d) Establezcan autoridades independientes con facultades para supervisar las prácticas del Estado y el sector privado en lo que respecta a la privacidad de los datos, investigar los abusos, recibir las denuncias presentadas por particulares y organizaciones e imponer multas y otras penas efectivas al tratamiento ilegal de datos personales por órganos privados y públicos;

e) Garanticen, a través de legislación apropiada y de otros medios, que toda injerencia en el derecho a la privacidad, en particular a través de la vigilancia de las comunicaciones y el intercambio de inteligencia, sea compatible con el derecho internacional de los derechos humanos, incluidos los principios de legalidad, fin legítimo, necesidad y proporcionalidad, independientemente de la nacionalidad o la ubicación de las personas afectadas, y aclaren que la autorización de medidas de vigilancia requiere que exista una sospecha razonable de que una persona concreta ha cometido o está cometiendo un delito penal o participa en actos que constituyen una amenaza específica para la seguridad nacional;

f) Refuercen los mecanismos destinados a autorizar y supervisar de manera independiente la vigilancia estatal y velen por que esos mecanismos sean competentes y cuenten con los recursos necesarios para hacer cumplir la legalidad, la necesidad y la proporcionalidad de las medidas de vigilancia;

g) Revisen las leyes para garantizar que no impongan requisitos de conservación general e indiscriminada de datos a las empresas de telecomunicaciones y de otros sectores;

h) Adopten medidas para aumentar la transparencia y la rendición de cuentas en la adquisición de tecnologías de vigilancia por los Estados;

i) Cumplan plenamente su obligación de prestar protección frente a las vulneraciones del derecho a la vida privada por las empresas en todos los sectores pertinentes, incluido el sector de las TIC, mediante la adopción de medidas apropiadas para prevenir, investigar, castigar y reparar esos abusos a través de políticas adecuadas, actividades de reglamentación y sometimiento a la justicia;

j) Velen por que todas las víctimas de violaciones y vulneraciones del derecho a la privacidad tengan acceso a recursos eficaces, incluso en los casos transfronterizos.

62. **El Alto Comisionado recomienda a las empresas que:**

a) Hagan todos los esfuerzos necesarios para cumplir con su responsabilidad de respetar el derecho a la privacidad y los demás derechos humanos. Como mínimo, las empresas deben hacer plenamente efectivos los Principios Rectores sobre las Empresas y los Derechos Humanos, lo que implica la aplicación efectiva de la diligencia debida en materia de derechos humanos en todas sus operaciones y en relación con todos los derechos humanos, incluido el derecho a la privacidad, y la adopción de medidas adecuadas para prevenir, mitigar y hacer frente a los efectos reales y potenciales de sus actividades;

b) Traten de asegurar un alto nivel de seguridad y confidencialidad en las comunicaciones que transmitan y en los datos personales que recopilen, almacenen o traten de otro modo. Realicen evaluaciones sobre el mejor modo de diseñar y actualizar la seguridad de los productos y servicios de forma continua;

c) Cumplan los principios de privacidad fundamentales mencionados en los párrafos 29 a 31 del presente informe y garanticen la mayor transparencia posible en las políticas y prácticas internas que afecten al derecho a la privacidad de sus usuarios y clientes;

d) Den reparación o contribuyan a dar reparación mediante procedimientos legítimos cuando hayan provocado o contribuido a provocar consecuencias negativas, entre otras cosas mediante mecanismos de reclamación eficaces a nivel operacional;

e) Contribuyan a la labor del proyecto sobre rendición de cuentas y reparación del ACNUDH destinado a elaborar directrices y recomendaciones para aumentar la eficacia de los mecanismos de reclamación no estatales en relación con las vulneraciones del derecho a la privacidad en el espacio digital.