Naciones Unidas A/HRC/35/22

Asamblea General

Distr. general
30 de marzo de 2017
Español
Original: inglés

Consejo de Derechos Humanos
35º período de sesiones
6 a 23 de junio de 2017
Tema 3 de la agenda
Promoción y protección de todos los derechos humanos, civiles, políticos, económicos, sociales y culturales, incluido el derecho al desarrollo

Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión

Nota de la Secretaría

La Secretaría tiene el honor de transmitir al Consejo de Derechos Humanos el informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye, elaborado de conformidad con la resolución 25/2 del Consejo. En sus dos informes anteriores al Consejo, el Relator Especial se centró en la libertad de opinión y de expresión en la era digital, detallando la manera en que las herramientas de cifrado y anonimato proporcionan la seguridad necesaria para el ejercicio de la libertad de expresión (A/HRC/29/32) y trazando las formas en que el sector de la tecnología de la información y las comunicaciones repercute en la libertad de expresión (A/HRC/32/38). El presente informe trata sobre las funciones que desempeñan los agentes privados que intervienen en la prestación de acceso a Internet y las telecomunicaciones. El informe examina las obligaciones de los Estados de proteger y promover la libertad de expresión en línea, evalúa el papel del sector del acceso digital y ofrece un conjunto de principios que podrían orientar las medidas que ha de adoptar el sector privado para proteger los derechos humanos.

GE.17-05047 (S) 070417 100417
1705047

Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión

Índice

I. Introducción

1. Los Estados recurren cada vez más al sector del acceso digital para controlar, limitar o vigilar la expresión en línea. Cuando las autoridades desean desconectar a los usuarios de sitios web, redes sociales o Internet, con frecuencia requieren la asistencia de los proveedores de servicios de Internet. Interfieren en los puntos de intercambio de Internet (IXPs) que facilitan el tráfico hacia un país o dentro de este. Acceden a las comunicaciones privadas y otros datos personales en poder de los proveedores de telecomunicaciones. En la actualidad, muchos de estos son de propiedad privada o son explotadas en forma privada. Bajo protesta, en silenciosa pasividad o con su colaboración voluntaria, a menudo los proveedores son esenciales para que el Estado pueda ejercer la censura y la vigilancia. Lo que los Gobiernos exigen a los agentes privados, y la forma en que estos responden, puede paralizar el intercambio de información; limitar la capacidad de los periodistas para investigar de forma segura; y disuadir de actuar a los denunciantes de irregularidades y los defensores de los derechos humanos. Los agentes privados también pueden restringir la libertad de expresión por iniciativa propia. Pueden asignar prioridad al contenido o las aplicaciones de Internet a cambio de pago u otros beneficios comerciales, modificando la forma en que los usuarios utilizan la información en línea. Las empresas que ofrecen servicios de filtrado pueden influir en el alcance del contenido accesible a sus abonados.

2. Los Estados y los agentes del sector privado repercuten en la libertad de expresión. Las obligaciones del Estado de proteger la libertad de expresión son claras, pero ¿qué deben hacer los agentes privados por sus usuarios? ¿Cómo deben respetar la libertad de expresión? ¿Qué medidas están adoptando para evaluar y abordar los riesgos que sus respuestas a las acciones y políticas de los Gobiernos podrían plantear a la libertad de expresión y a la privacidad? ¿Cuánta información deben compartir con sus clientes sobre las exigencias y solicitudes del Estado? Cuando los agentes privados están directamente involucrados o vinculados con abusos, ¿de qué recursos disponen las personas o el público en general cuyos intereses están en riesgo?

3. Los agentes privados que hacen posible el acceso digital sirven de mediadores y permiten el ejercicio de la libertad de expresión. Cabe recordar que los Estados son los principales impulsores de la censura y la vigilancia. Sin embargo, al igual que los Estados, que a menudo, aunque no siempre, recurren a los proveedores para adoptar medidas que hacen posible la censura, nosotros los usuarios, como beneficiarios de los notables avances de la era digital, merecemos comprender la forma en que estos agentes interactúan entre sí y en que estas interacciones y sus acciones independientes nos afectan, y qué responsabilidades tienen los proveedores de respetar los derechos fundamentales.

4. El presente informe es el resultado de más de un año de estudios y consultas que se inició en 2016 con la recopilación de datos del sector de la tecnología de la información y las comunicaciones (TIC) (véase A/HRC/32/38)[1]. En respuesta a una invitación a la presentación de información[2], el Relator Especial recibió 25 comunicaciones de Estados; 3 de empresas; 22 de la sociedad civil, académicos y otros; y 1 comunicación confidencial. Además, el Relator Especial convocó una sesión de intercambio de ideas organizada por ARTICLE 19 en Londres en julio de 2016, una reunión de expertos en el Human Rights Institute de la Universidad de Connecticut (Estados Unidos de América) en octubre de 2016, una consulta regional con el Relator Especial de la Comisión Interamericana de Derechos Humanos para la Libertad de Expresión, en Guadalajara (México) en diciembre de 2016, y una consulta regional en Beirut en febrero de 2017[3].

[1] Deseo dar las gracias a Amos Toh, asesor jurídico del mandato y becario de la Fundación Ford en la Facultad de Derecho de Irvine (Universidad de California) por su labor de investigación y análisis, así como la coordinación de la investigación sustancial y esencial llevada a cabo por estudiantes de la Facultad de Derecho de Irvine de la Universidad de California (taller de justicia internacional).

[2] Véase https://freedex.org/new-call-for-submissions-freedom-of-expression-and-the-telecommunications-and-internet-access-sector/.

[3] Las comunicaciones pueden consultarse en el sitio web del mandato. Puede encontrarse una sinopsis de las consultas celebradas y las aportaciones recibidas para la preparación del presente informe en un anexo complementario que también figura en el sitio web del mandato.

II. Obligación del Estado de proteger y promover la libertad de expresión en línea

5. El derecho internacional de los derechos humanos establece que todo individuo tiene derecho a la libertad de opinión y de expresión y de no ser molestado a causa de sus opiniones, el de investigar y recibir informaciones y opiniones, y el de difundirlas, sin limitación de fronteras, por cualquier medio de expresión (véanse la Declaración Universal de Derechos Humanos, artículo 19 y el Pacto Internacional de Derechos Civiles y Políticos, artículo 19). El Consejo de Derechos Humanos y la Asamblea General han reiterado que la libertad de expresión y otros derechos también deben aplicarse en línea (véanse las resoluciones del Consejo 26/13 y 32/13; la resolución 68/167 de la Asamblea General; y A/HRC/32/38). El Comité de Derechos Humanos, los anteriores titulares de mandatos y el Relator Especial han examinado las obligaciones de los Estados en virtud del artículo 19 del Pacto. En suma, los Estados no pueden obstaculizar ni limitar en modo alguno la capacidad de tener opiniones (véanse el artículo 19, párrafo 1, del Pacto; y A/HRC/29/32, párrafo 19). El artículo 19, párrafo 3, del Pacto establece que los Estados pueden limitar la libertad de expresión solo en los casos expresamente fijados por la ley y cuando sean necesarios para asegurar el respeto a los derechos o a la reputación de los demás o la protección de la seguridad nacional, el orden público o la salud o la moral públicas (véase Comité de Derechos Humanos, observación general núm. 34 (2011); A/71/373; y A/HRC/29/32).

6. Los Estados también tienen la obligación de adoptar medidas para proteger a las personas de injerencias indebidas en los derechos humanos cuando son cometidas por agentes privados (véase el artículo 2, párrafo 2, del Pacto; y Comité de Derechos Humanos, observación general núm. 31 (2004)). El derecho de los derechos humanos protege a las personas de las violaciones cometidas por el Estado, así como de los abusos cometidos por personas o entidades privadas (véase la observación general núm. 31, párrafo 8)[4]. Los Principios Rectores sobre las Empresas y los Derechos Humanos: Puesta en Práctica del Marco de las Naciones Unidas para "Proteger, Respetar y Remediar", aprobados por el Consejo de Derechos Humanos en 2011, explica que los Estados deben tomar medidas apropiadas para prevenir, investigar, castigar y reparar los abusos de agentes privados (véase A/HRC/17/31, anexo, principio 1). Esas medidas incluyen la adopción y aplicación de medidas legislativas, judiciales, administrativas, educativas y de otra índole adecuadas para cumplir sus obligaciones jurídicas que exigen o que propician el respeto de la libertad de expresión por las empresas y, cuando se producen abusos del sector privado, facilitan el acceso a un recurso efectivo (véanse la observación general núm. 31, párr. 7; y A/HRC/17/31, anexo, principios 3 y 25).

7. Las medidas gubernamentales que se describen a continuación a menudo vulneran las normas del derecho de los derechos humanos. Además, las injerencias gubernamentales en el sector del acceso digital se caracterizan por la falta de transparencia, que incluye leyes imprecisas que prevén la facultad discrecional excesiva de las autoridades, restricciones jurídicas a la divulgación de información a terceras partes relativas al acceso de los Gobiernos a datos de usuarios y órdenes de reserva concretas. La falta de transparencia socava el estado de derecho, así como la comprensión del público sobre este sector[5].

A. Interrupciones del servicio de Internet y las telecomunicaciones

8. Las interrupciones del servicio de Internet y las telecomunicaciones que entrañan medidas cuyo objetivo deliberado es impedir u obstaculizar el acceso o la divulgación de información en línea vulneran el derecho internacional de los derechos humanos (véase

[4] Véase también Comisión Africana de Derechos Humanos y de los Pueblos, observación general núm. 3 (2015) sobre el derecho a la vida, párr. 38; Corte Interamericana de Derechos Humanos, *caso Velásquez Rodríguez*, sentencia de 29 de julio de 1988, párr. 172; y Tribunal Europeo de Derechos Humanos, *Özel y otros c. Turquía*, sentencia de 17 de noviembre de 2015, párr. 170.

[5] Freedom Online Coalition, informe del Grupo de Trabajo 3 sobre Privacidad y Transparencia en Línea, noviembre de 2015.

A/HRC/32/13, párr. 10)[6]. Los Gobiernos suelen realizar u ordenar interrupciones del servicio, a menudo con la asistencia de agentes privados que operan redes o facilitan el tráfico en la red. Los ataques en gran escala contra la infraestructura de la red cometidos por particulares, como los ataques distribuidos de denegación del servicio, también pueden tener efectos de interrupción del servicio. Si bien con frecuencia las interrupciones guardan relación con el corte total del servicio en la red, también pueden ocurrir cuando el acceso a comunicaciones móviles, sitios web o redes sociales y aplicaciones para mensajes está bloqueado, ralentizado o "efectivamente inutilizable"[7]. Las interrupciones del servicio pueden afectar a ciudades o regiones dentro de un país, a todo un país o incluso a múltiples países y pueden durar desde algunas horas hasta meses.

9. Las interrupciones del servicio ordenadas de manera encubierta o sin una base jurídica clara vulneran el requisito establecido en el artículo 19, párrafo 3, del Pacto de que las restricciones deben estar "fijadas por la ley". En el Chad, el hecho de que las autoridades no proporcionaran una explicación pública significativa por una serie de interrupciones del acceso a Internet y las redes sociales entre febrero y octubre de 2016 llevó a suponer que habían sido ilegales[8]. En el Gabón, presuntamente se registraron cortes totales del acceso a la red todas las noches durante casi dos semanas durante el período electoral de 2016, en contravención de las garantías del Gobierno de que no se interrumpirían esos servicios[9].

10. Las interrupciones del servicio ordenadas de conformidad con leyes y reglamentos imprecisos tampoco cumplen con el requisito de legalidad. En Tayikistán, la Ley sobre el Estado de Emergencia modificada permite al Gobierno bloquear los servicios móviles y el acceso a Internet sin necesidad de contar con una decisión judicial cuando se haya declarado el estado de emergencia[10]. La Ley no define cuándo y con qué fines se puede declarar el estado de emergencia. Esa ambigüedad permite a las autoridades una discrecionalidad absoluta para disponer interrupciones del servicio. En algunos países, las autoridades se basan en leyes obsoletas para justificar interrupciones[11]. Las leyes y los reglamentos aprobados y aplicados en secreto también infringen el requisito de legalidad. En los Estados Unidos, el Centro Nacional de Coordinación para las Telecomunicaciones ha adaptado considerablemente, para su divulgación pública, el procedimiento operativo estándar 303, un reglamento ejecutivo que establece "procedimientos detallados" sobre la "interrupción de servicios celulares"[12]. Si bien estos procedimientos no se han invocado públicamente, la posibilidad de que las autoridades eludan la fiscalización jurídica y la rendición pública de cuentas vulnera el artículo 19 del Pacto.

11. Las restricciones a la libertad de expresión solo podrán imponerse para lograr los objetivos especificados en el artículo 19, párrafo 3, del Pacto y no se pueden hacer valer como justificación para silenciar a los defensores de la democracia (véanse Comité de Derechos Humanos, observación general núm. 34, párr. 23; y A/71/373, párr. 26). Sin embargo, con frecuencia los Gobiernos disponen interrupciones del servicio durante manifestaciones, elecciones y otros acontecimientos de interés público extraordinario, con escasa o ninguna explicación[13]. En Bahrein, las interrupciones del acceso móvil y a Internet en Duraz presuntamente coincidieron con sentadas frente a la casa de un destacado líder

[6] Access Now registró 15 interrupciones del servicio en 2015 y 56 en 2016. La primera interrupción del servicio registrada presuntamente ocurrió en Nepal en febrero de 2005.

[7] Comunicación de Access Now, parte I, pág. 1.

[8] Comunicación de Internet Sans Frontières, pág. 2, Chad, marzo de 2016.

[9] *Ibid.*, Gabón, enero de 2016.

[10] Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH), Observaciones preliminares del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Sr. David Kaye, al final de su visita a Tayikistán, comunicado de prensa (9 de marzo de 2015).

[11] India, Código de Procedimiento Penal , art. 144; también Apar Gupta y Raman Jit Singh Chima, "The cost of internet shutdowns", *The Indian Express* (26 de octubre de 2016).

[12] Estados Unidos, procedimiento operativo estándar 303 del Centro Nacional de Coordinación para las Telecomunicaciones.

[13] Comunicación de Access Now, parte I, págs. 5 a 7.

religioso cuya ciudadanía el Gobierno había revocado[14]. Aparentemente se negó a los usuarios de Internet en la República Bolivariana de Venezuela el acceso a Internet durante las protestas generalizadas contra el Gobierno realizadas en 2014[15]. Se han registrado interrupciones del acceso a la red antes, durante y después de elecciones o protestas en el Camerún[16], Gambia[17], la India[18], Myanmar[19], la República Islámica del Irán[20], Uganda[21] y Montenegro[22].

12. No explicar ni reconocer las interrupciones del servicio crea la percepción de que tienen por objeto impedir la transmisión de información, críticas o disenso. Los informes de represión y actos de violencia tolerados por el Estado tras interrupciones del acceso a la red han dado lugar a acusaciones en el sentido de que algunos Estados aprovechan la oscuridad para cometer y encubrir abusos. En el Sudán, por ejemplo, el acceso a Internet se suspendió durante varias horas durante la brutal represión de manifestantes que protestaban contra el aumento de los precios del combustible en septiembre de 2013[23].

13. Los observadores también han señalado la creciente utilización de interrupciones del acceso a Internet para impedir que los alumnos se copien en exámenes nacionales. Tal vez Uzbekistán haya sido el primer país en invocar esta justificación durante los exámenes de ingreso a la universidad en 2014[24]. En 2016 las autoridades presuntamente ordenaron interrupciones del servicio de Internet durante exámenes en la India, Argelia, Etiopía y el Iraq[25].

14. Las interrupciones del acceso a la red invariablemente vulneran la norma de necesidad. Esta exige demostrar que las interrupciones lograrían su objetivo declarado, que en realidad suelen socavar. Algunos Gobiernos sostienen que es importante prohibir la difusión de noticias sobre ataques terroristas, aunque se trate de informes precisos, a fin de prevenir el pánico y actos de imitadores[26]. Sin embargo, se ha llegado a la conclusión de que mantener la conectividad a la red puede mitigar las preocupaciones sobre la seguridad pública y ayudar a restablecer el orden público. Durante los disturbios que tuvieron lugar en Londres en 2011, por ejemplo, las autoridades utilizaron las redes sociales para identificar a los autores, difundir información precisa y llevar a cabo operaciones de limpieza. En Cachemira, la policía ha destacado el papel positivo de los teléfonos móviles para localizar a personas atrapadas durante ataques terroristas[27].

15. La duración y el alcance geográfico pueden variar, pero las interrupciones del servicio son por lo general desproporcionadas. Los usuarios afectados pierden el acceso a los servicios de emergencia y a información sobre la salud, la banca móvil y el comercio

[14] Centro para los Derechos Humanos de Bahrein, *Digital Rights Derailed in Bahrain* (2016), págs. 13 y 14.

[15] Danny O'Brien, "Venezuela's Internet crackdown escalates into regional blackout", Fundación de la Frontera Electrónica (20 de febrero de 2014).

[16] ACNUDH, "UN expert urges Cameroon to restore Internet services cut off in rights violation", comunicado de prensa (10 de febrero de 2017).

[17] Deji Olukotun, "Gambia shuts down Internet on eve of elections", Access Now (30 de noviembre de 2016).

[18] Software Freedom Law Center, "Internet shutdowns in India, 2013-2016".

[19] Freedom House, "Freedom on the Net: Myanmar" (2011).

[20] Center for Democracy and Technology, "Iran's Internet throttling: unacceptable now, unacceptable then" (3 de julio de 2013).

[21] ARTICLE 19, "Uganda: Blanket ban on social media on election day is disproportionate", comunicado de prensa (18 de febrero de 2016).

[22] Global Voices, "WhatsApp and Viber blocked on election day in Montenegro" (17 de octubre de 2016).

[23] Human Rights Watch, "Sudan: Dozens killed during protests" (27 de septiembre de 2013).

[24] Comunicación de Access Now, parte I; también Freedom House, "Freedom on the Net: Uzbekistan" (2016).

[25] Comunicación de Access Now, parte I.

[26] Véase, por ejemplo, ACNUDH, "Preliminary conclusions and observations by the UN Special Rapporteur on the right to freedom of opinion and expression to his visit to Turkey, 14-18 November 2016", comunicado de prensa (18 de noviembre de 2016).

[27] Institute for Human Rights and Business (IHRB), "Security v. Access: The impact of mobile network shutdowns", estudio de caso: Telenor Pakistan (septiembre de 2015), págs. 31 y 32.

electrónico, el transporte, las clases en las escuelas, la fiscalización de la votación y las elecciones, la información publicada sobre los principales acontecimientos y crisis, y las investigaciones sobre derechos humanos[28]. Habida cuenta del número de actividades y servicios esenciales que afectan, las interrupciones del servicio restringen la libertad de expresión y constituyen una injerencia en otros derechos fundamentales.

16. Las interrupciones del servicio también afectan a esferas distintas de las que revisten interés específico[29]. En el período previo al desfile conmemorativo del día nacional del Pakistán de 2015, las redes de comunicación móviles presuntamente se cortaron en el lugar del desfile así como en las zonas circundantes que no presentaban riesgos para la seguridad[30]. Durante la visita del Papa a Filipinas en 2015, la interrupción del servicio de las redes móviles, por motivos de seguridad, afectó a zonas muy alejadas del itinerario[31]. Por lo general, los Gobiernos suelen interrumpir los servicios o plataformas más eficientes, seguros o utilizados más ampliamente[32].

B. Acceso gubernamental a datos de los usuarios

17. La vigilancia gubernamental actual se basa en el acceso a las comunicaciones y los datos conexos pertenecientes a usuarios de redes de propiedad privada. Si bien con frecuencia este acceso requiere la asistencia de agentes privados, también puede obtenerse sin su conocimiento o participación. Al igual que otras formas de vigilancia, el acceso a datos de los usuarios puede constituir una injerencia indebida en la privacidad de las personas y limitar en forma tanto directa como indirecta el libre intercambio y evolución de ideas (véase A/HRC/23/40, párr. 24). El acceso indebido a los datos personales implícitamente advierte a los usuarios que deben actuar con cautela y en lo posible evitar la expresión de opiniones polémicas, el intercambio de información confidencial y otras formas de libertad de expresión que pueden ser objeto de la fiscalización del Gobierno (véase A/HRC/27/37, párr. 20).

Solicitudes de datos de usuarios

18. Las leyes y reglamentos imprecisos violan el requisito de legalidad (véase A/HRC/23/40, párr. 50). La Ley de Comunicación y Multimedia de Malasia, por ejemplo, permite a las autoridades disponer la divulgación de "cualquier comunicación o clase de comunicaciones" sobre "cualquier emergencia pública o en aras de la seguridad pública". La Ley no define las condiciones que provocan una situación de emergencia pública y la certificación del Rey se considera "prueba concluyente sobre la cuestión"[33]. En Qatar los organismos encargados de la aplicación de la ley gozan de amplio derecho a solicitar acceso a los clientes de proveedores de comunicaciones en casos de seguridad o emergencia nacional[34]. Estas disposiciones facultan a las autoridades a solicitar datos de los usuarios simplemente invocando la seguridad nacional. Por consiguiente, los usuarios no pueden predecir con certeza razonable las circunstancias en que sus comunicaciones y datos conexos pueden divulgarse a las autoridades.

19. Los proveedores solo deben verse obligados a divulgar datos de los usuarios cuando se lo ordenan las autoridades judiciales certificando la necesidad y proporcionalidad para alcanzar un objetivo legítimo. El Código Penal del Canadá exige que las autoridades de aplicación de la ley presenten a un juez las solicitudes de divulgación de los registros telefónicos en investigaciones penales, para su aprobación[35]. En Portugal, las autoridades

[28] Comunicación de Access Now, parte I, págs. 11 a 14; también comunicación de Global Network Initiative.

[29] IHRB, "Security v. Access: The impact of mobile network shutdowns", estudio de caso: Telenor Pakistan (septiembre de 2015), pág. 20.

[30] *Ibid.*, págs. 27 y 28.

[31] Deniz Duru Aydin, "Five excuses governments (ab)use to justify Internet shutdowns", Access Now (6 de octubre de 2016).

[32] Comunicación de ARTICLE 19, pág. 2.

[33] Malasia, Ley de Comunicación y Multimedia (1998), art. 266.

[34] Qatar, Decreto-Ley núm. 34 de 2006.

[35] Véase la comunicación del Canadá, pág. 6.

deben obtener una orden judicial para exigir la divulgación de datos sobre comunicaciones[36]. Sin embargo, la legislación nacional a menudo no requiere que las solicitudes de datos tengan autorización judicial. En Bangladesh, las autoridades solo exigen la aprobación del poder ejecutivo para acceder a los datos de comunicaciones pertenecientes a abonados de telecomunicaciones por motivos de seguridad nacional y defensa del orden público[37].

20. Las leyes que exigen a los agentes privados crear grandes bases de datos accesibles a los Gobiernos plantean preocupaciones de necesidad y proporcionalidad. En Kazajstán el proveedor debe conservar durante dos años los números de teléfono, los correos electrónicos y las direcciones del protocolo Internet (IP), así como información sobre facturación[38]. La Federación de Rusia exige que los agentes privados guarden el contenido de las llamadas y los mensajes de texto de todos sus clientes por un período de seis meses, y los metadatos de las comunicaciones conexas durante tres años[39]. Ambos países también exigen que estos datos se almacenen localmente[40]. En los países en que los teléfonos móviles son un medio de comunicación generalizado, las leyes de registro obligatorio de tarjeta SIM efectivamente exigen que la mayor parte de la población divulgue datos personales de identificación (véase A/HRC/29/32, párr. 51). La retención obligatoria de una gran cantidad de datos de usuarios es contraria a las garantías procesales establecidas, que requieren, por ejemplo, la sospecha individual de que se cometió una infracción.

Menoscabo del cifrado

21. Desde el informe del Relator Especial sobre el cifrado y el anonimato (A/HRC/29/32), han aumentado en todo el mundo las medidas innecesarias y desproporcionadas para menoscabar el cifrado, lo que amenaza con socavar tanto la libertad de expresión como la seguridad digital de los usuarios. En el Reino Unido de Gran Bretaña e Irlanda del Norte, por ejemplo, la Ley de Regulación de Facultades de Investigación de 2016 permite al Secretario de Estado emitir "notificaciones de capacidad técnica" que exigen a los proveedores eliminar la "protección electrónica" de las comunicaciones, una medida que podría obligar a ingresar al sistema por una "puerta trasera" o limitar o debilitar el cifrado[41]. Los Estados no han proporcionado pruebas suficientes de que estos factores de vulnerabilidad sean el medio menos invasivo de proteger la seguridad nacional y el orden público, en particular en vista de la profundidad y amplitud de otras herramientas de investigación a su disposición (*ibid*., párr. 39).

Acceso directo

22. El acceso directo a Internet y a las redes de telecomunicaciones permite a las autoridades interceptar y vigilar las comunicaciones con escasa fiscalización jurídica o rendición de cuentas. Los adelantos tecnológicos han aumentado la capacidad de los organismos de inteligencia y encargados de hacer cumplir la ley para obtener una conexión directa a redes sin la participación o el conocimiento del operador de la red[42]. En las elecciones generales de 2014 en la ex República Yugoslava de Macedonia, las autoridades de inteligencia presuntamente obtuvieron acceso directo a las principales redes de telecomunicaciones del país para interceptar las comunicaciones de más de 20.000 personas, incluidos políticos, activistas, funcionarios públicos y periodistas. En muchos casos se envió también una transcripción de las llamadas telefónicas a las personas

[36] Portugal, Código de Procedimiento Penal, arts. 187 a 190.

[37] Bangladesh, Ley de Reglamentación de las Telecomunicaciones (2001), art. 97 (Ka).

[38] Kazajstán, Resolución del Gobierno núm. 1593 (23 de diciembre de 2011).

[39] ACNUDH, carta dirigida al Gobierno de la Federación de Rusia, 28 de julio de 2016 (OL RUS, julio de 2016).

[40] Comunicación de ARTICLE 19, pág. 5.

[41] Reino Unido de Gran Bretaña e Irlanda del Norte, Ley de Regulación de Facultades de Investigación de 2016, art. 253; también ACNUDH, carta dirigida al Gobierno del Reino Unido, 22 de diciembre de 2015 (AL GBR, abril de 2015).

[42] Comunicación de Privacy International; y comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, pág. 3.

cuyas llamadas se interceptaron[43]. En la India, al parecer las autoridades están desarrollando un programa para el Sistema Central de Vigilancia que permitiría "que un organismo gubernamental suministrara electrónicamente los números telefónicos seleccionados sin ninguna intervención manual de proveedores de servicios de telecomunicaciones en una red segura"[44]. Estas actividades no parecen estar previstas por la ley, pues carecen tanto de autorización judicial como de supervisión externa. Además, los riesgos que plantean para la seguridad y la integridad de la infraestructura de la red suscitan preocupaciones de proporcionalidad.

C. Neutralidad de la red

23. La neutralidad de la red —el principio de que todos los datos de Internet deben ser tratados en pie de igualdad, sin injerencia indebida— promueve el acceso más amplio posible a la información[45]. En la era digital, la libertad de elegir entre distintas fuentes de información solo tiene sentido cuando el contenido de Internet y las aplicaciones de todo tipo son transmitidos sin discriminación o injerencia indebida por agentes no estatales, incluidos los proveedores. La obligación positiva del Estado de promover la libertad de expresión sostiene firmemente la neutralidad de la red, a fin de promover el mayor acceso no discriminatorio posible a la información.

Priorización paga

24. Con arreglo a planes de priorización paga, los proveedores dan un trato preferencial a determinados tipos de tráfico de Internet sobre otros a cambio de un pago o de otros beneficios comerciales. Estos planes efectivamente establecen vías rápidas en Internet para proveedores de contenidos que pueden permitirse pagar más y vías lentas para todos los demás[46]. Esta jerarquía de datos socava las opciones de los usuarios. Los usuarios deben pagar costos más elevados o reciben un servicio de menor calidad cuando intentan acceder al contenido de Internet y sus aplicaciones en las vías lentas. Al mismo tiempo, podrían encontrarse ante contenidos a los que se ha dado prioridad sin su conocimiento ni aprobación.

25. Varios Estados prohíben la priorización paga. Por ejemplo, los Países Bajos, uno de los primeros países que adoptó la neutralidad de la red, prohíbe a los proveedores hacer "depender el precio de las tarifas de acceso a Internet de los servicios y aplicaciones que se ofrecen o utilizan por medio de estos"[47]. La Ordenanza de Internet Abierta de 2015 de la Comisión Federal de Comunicaciones de los Estados Unidos prohíbe que los "administradores de una red de proveedores de banda ancha favorezcan directa o indirectamente un tipo de tráfico determinado respecto de otro... a cambio de una contrapartida (monetaria o de otra índole) de un tercero, o en beneficio de una entidad afiliada"[48].

Tarifa cero

26. La tarifa cero es la práctica de no cobrar por la utilización de datos de Internet relacionados con una aplicación o un servicio determinados; mientras que otros servicios o aplicaciones están sujetos a costos medidos. Los arreglos de tarifa cero varían desde planes

[43] Privacy International, "Macedonia: Society On Tap" (23 de marzo de 2016).

[44] Comunicación de Access Now, parte II, pág. 4.

[45] Comunicación de Luca Belli; y comunicación de ARTICLE 19, págs. 7 y 8.

[46] Dawn C. Nunziato y Arturo J. Carrillo, "The price of paid prioritization: The international and domestic consequences of the failure to protect Net neutrality in the United States", *Georgetown Journal of International Affairs*: International Engagement on Cyber V: Securing Critical Infrastructure (2 de octubre de 2015), pág. 103.

[47] Países Bajos, Ley de Telecomunicaciones, art. 7.4a, párr. 3. Telecommunications Act. ders on ber Vlo, ernet Intermediaries, or Assessing Benefits and Harms e 19. lecom service providers on.

[48] Estados Unidos, Comisión Federal de Comunicaciones, Protecting and Promoting the Open Internet, FCC 15-24 (12 de marzo de 2015), párr. 18. Esta Ordenanza, posiblemente cuestionada en el momento en que se redactó el presente informe, sigue siendo un modelo útil para la regulación de la neutralidad de la red.

de datos que eximen a un abonado del régimen de costos medidos por algunos servicios de Internet, hasta la provisión de acceso ilimitado a determinados servicios sin suscribirse a un plan[49]. Independientemente de las variaciones, los arreglos de tarifa cero priorizan el acceso al contenido y pueden aumentar el costo de los datos medidos. Los usuarios que tienen dificultades para pagar datos medidos podrían terminar por recurrir exclusivamente a servicios con tarifa cero, lo que daría lugar a un acceso limitado a la información a comunidades que ya podrían estar marginadas en su acceso a la información y la participación pública.

27. Los arreglos de tarifa cero pueden proporcionar a los usuarios acceso limitado a Internet en zonas que, de otro modo, carecerían totalmente de acceso[50]. Sin embargo, los usuarios podrían seguir careciendo de acceso más amplio a Internet y quedar atrapados en entornos cerrados en línea[51]. La suposición de que un acceso limitado, a la larga, se convertirá en uno de plena conectividad requiere mayor estudio. Podría depender de factores como el comportamiento de los usuarios, las condiciones del mercado, la situación de los derechos humanos y el entorno reglamentario[52].

28. Estas consideraciones contrapuestas han dado lugar a variaciones en los métodos de reglamentación. En la India, la preocupación pública por las funciones básicas gratuitas de Facebook culminó con una prohibición de todo arreglo cuyo efecto sea "ofrecer o cobrar tarifas discriminatorias al consumidor por servicios de datos sobre la base del contenido"[53]. En Chile, Noruega, los Países Bajos, Finlandia, Islandia, Estonia, Letonia, Lituania, Malta y el Japón rigen restricciones a la tarifa cero[54]. En cambio, los Estados Unidos, y posteriormente el Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), aprobaron directrices basadas en un enfoque caso por caso[55]. Los Estados que adopten un enfoque caso por caso deben examinar cuidadosamente y, de ser necesario, rechazar los arreglos que, entre otras cosas, aplican la tarifa cero al contenido conexo, condicionan la tarifa cero al pago o favorecen el acceso a ciertas aplicaciones dentro de una clase de aplicaciones similares (por ejemplo, tarifa cero a determinados servicios de transmisión de música y no a todas las transmisiones de música). Además, los Estados deben exigir la divulgación de información empresarial significativa sobre las prácticas de gestión del tráfico en la red. Por ejemplo, Chile exige a los proveedores de servicios de Internet que divulguen información sobre la velocidad de acceso a Internet, diferenciando entre el precio y la velocidad de las conexiones nacionales e internacionales, así como la naturaleza y garantías del servicio[56].

III. Proveedores de acceso digital y libertad de expresión

29. Si bien la obligación de los Estados de respetar y proteger la libertad de expresión está consolidada, los agentes privados que establecen, gestionan y mantienen el acceso digital también desempeñan un papel fundamental.

[49] Erik Stallman y R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms", Center for Democracy and Technology (enero de 2016).

[50] *Ibid*., págs. 4 y 11.

[51] Barbara van Schewick, "Network neutrality and zero-rating", comunicación presentada a la Comisión Federal de Comunicaciones de los Estados Unidos (19 de febrero de 2014), pág. 7.

[52] Erik Stallman y R. Stanley Adams, IV, "Zero Rating: A framework for assessing benefits and harms", Center for Democracy and Technology (enero de 2016), pág. 15.

[53] India, Autoridad de Regulación de las Telecomunicaciones, "TRAI releases the Prohibition of Discriminatory Tariffs for Data Services Regulations, 2016", comunicado de prensa (8 de febrero de 2016).

[54] Emily Hong, "A zero sum game? What you should know about zero-rating", *New America Weekly*, número 109 (4 de febrero de 2016).

[55] Estados Unidos, Comisión Federal de Comunicaciones, Protecting and Promoting the Open Internet, FCC 15-24 (12 de marzo de 2015), párr. 21; y Organismo de Reguladores Europeos de las Comunicaciones Electrónicas (ORECE), Guidelines on the Implementation by National Regulators of European Net Neutrality Rules (agosto de 2016) (BoR (16) 127).

[56] Chile, Ley núm. 20453, art. 24 H (D).

A. Proveedores de servicios de telecomunicaciones e Internet

30. Los proveedores de servicios de telecomunicaciones y los proveedores de servicios de Internet (denominados colectivamente en el presente informe "proveedores") ofrecen una amplia gama de servicios. Aunque principalmente conectan a sus abonados a las redes que conforman Internet, también permiten a los usuarios comunicarse y compartir información a través de servicios móviles y fijos (véase A/HRC/32/38, párr. 16). Si bien en muchas regiones los proveedores siguen siendo estatales, hay cada vez más proveedores establecidos y administrados en forma privada. El sector también tiene carácter cada vez más multinacional: algunos de los mayores proveedores operan redes en distintos países y regiones, a menudo mediante asociaciones con empresas nacionales o sus propias filiales.

31. Como guardianes de vastas redes de información, los proveedores hacen frente a considerables presiones de parte de los Gobiernos para realizar actividades de censura y vigilancia. Para operar una red en un país, deben hacer importantes inversiones en infraestructura física y empresarial, incluidos equipo de red y personal. Están normalmente sujetos a la legislación local y otros requisitos de concesión de licencias establecidos en acuerdos con el Estado. Además de la presión jurídica, los proveedores se han enfrentado con otro tipo de intimidación no jurídica, como amenazas a la seguridad de sus empleados e infraestructura en caso de incumplimiento[57].

32. Si bien algunos proveedores intentan oponerse a la censura y la vigilancia, muchos contribuyen con los Gobiernos sin oponer mayor resistencia. En los Estados Unidos, uno de los mayores proveedores presuntamente ha creado un "superbuscador" que facilita el acceso de las autoridades a llamadas telefónicas de clientes, aunque no están jurídicamente obligados a hacerlo[58]. En el Reino Unido, una denuncia presentada ante la Organización de Cooperación y Desarrollo Económicos alegó que los principales proveedores concedían al organismo de inteligencia del país acceso a sus redes y a los datos de los clientes mucho más allá de lo que exigía la ley en ese momento[59].

33. Cada vez más proveedores están concertando acuerdos con los medios de comunicación y otras empresas productoras de contenidos que amenazan la neutralidad de la red y están ejerciendo intensa presión para obtener concesiones a las normas de neutralidad de la red. Por ejemplo, mientras que reguladores europeos estaban elaborando directrices de neutralidad de la red, 17 de los principales proveedores de la región presentaron el "Manifiesto sobre el 5G" y advirtieron que directrices "excesivamente prescriptivas" retrasarían su inversión en 5G, la generación siguiente de conexión móvil a Internet[60].

B. Puntos de intercambio de Internet

34. Los IXPs permiten el intercambio de tráfico de Internet entre redes administradas por diferentes proveedores dentro de un país o una región determinados[61]. Esta forma de interconexión impide que el tráfico de Internet local o regional tome rutas internacionales largas y tortuosas, mejorando así la velocidad y eficiencia de la conectividad a Internet. Los IXPs pueden ser establecidos por empresas de infraestructura de Internet como parte de un amplio conjunto de servicios que se venden a los proveedores, o funcionar como organizaciones sin fines de lucro o voluntarias[62].

[57] Comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, pág. 10.

[58] Dave Maass y Aaron Mackey, "Law enforcement's secret 'super search engine' amasses trillions of phone records for decades", Fundación de la Frontera Electrónica (29 de noviembre de 2016).

[59] Privacy International, "OECD complaint against BT, Verizon Enterprise, Vodafone Cable, Viatel, Level 3, and Interoute".

[60] Comunicación de ARTICLE 19, pág. 9.

[61] Véase www.bgp4.as/internet-exchanges/.

[62] Jason Gerson y Patrick Ryan, "A primer on Internet exchange points for policymakers and non-engineers", *Social Science Research Network* (12 de agosto de 2012), pág. 10.

35. Los IXPs manejan un enorme volumen de tráfico de Internet que puede filtrarse o interceptarse a petición de los Gobiernos. El número cada vez mayor de incidentes de censura y vigilancia en los que intervienen IXPs indica que son los principales puntos de embotellamiento para el acceso a Internet, aunque su función precisa no está clara. Por ejemplo, en 2013 la forma en que fue bloqueado el acceso a YouTube en el Pakistán indicó que la plataforma fue filtrada por puntos de intercambio de Internet, y no por proveedores de servicios de Internet, mediante un procedimiento conocido como "inyección de paquetes"[63]. Según un memorando interno filtrado de un proveedor multinacional de servicios de Internet que opera en el Ecuador, los usuarios no pudieron acceder a Google y YouTube en marzo de 2014 porque la Asociación de Proveedores de Internet, una entidad privada del Ecuador que administra dos de los principales IXPs del país, "bloqueó el acceso a ciertas páginas de Internet por solicitud del Gobierno nacional"[64]. Las revelaciones de vigilancia masiva llevadas a cabo por el Organismo Nacional de Seguridad de los Estados Unidos han suscitado la preocupación de los especialistas en tecnología en el sentido de que el Organismo esté interceptando una proporción importante de tráfico de Internet nacional y extranjero centrándose en los IXPs de los Estados Unidos[65]. En septiembre de 2016, el punto de intercambio de Internet más grande del mundo, que se encuentra en Alemania, impugnó ordenamientos jurídicos emitidos por el organismo de inteligencia del país de vigilar las comunicaciones internacionales en tránsito a través de su concentrador[66].

C. Redes de distribución de contenido

36. Una red de distribución de contenido es una red de servidores estratégicamente ubicados en todo el mundo que tiene por objeto permitir la distribución eficiente de páginas web y otros contenidos de Internet. Los grandes productores de contenido dependen de redes de distribución de contenido para llegar al mayor número de usuarios lo más rápidamente posible[67]. Una red de distribución de contenido almacena copias del contenido de las plataformas y encauza la solicitud de contenido de los servidores de la plataforma a los servidores de su red más próximos a los usuarios[68]. Este proceso aumenta la velocidad de entrega de contenido, en particular a los usuarios situados lejos de los servidores de la plataforma. Las redes de distribución de contenido se consideran una salvaguardia efectiva contra el bloqueo de un sitio web; las medidas de censura contra servidores que acogen un sitio web o plataforma en particular no afectan a la red de distribución de contenido ni a la entrega de copias del mismo contenido a los usuarios[69]. Las redes de distribución de contenido también se han convertido en un baluarte fundamental contra las perturbaciones en la red. Las solicitudes de acceso rápido han incentivado a las redes de distribución de contenido a invertir importantes recursos en infraestructura y servicios que puedan soportar ataques distribuidos de denegación del servicio y otros ataques malintencionados[70].

37. La resiliencia a la censura de las redes de distribución de contenido las ha hecho objeto de restricciones desproporcionadas a la libertad de expresión. En Egipto, el bloqueo del sitio web de *The New Arab* en agosto de 2016 también perturbó el acceso al contenido

[63] Zubair Nabi, "The anatomy of web censorship in Pakistan" (2013), pág. 4.

[64] Katitza Rodríguez, "Documentos filtrados revelan la maquinaria de censura en el Ecuador", Fundación de la Frontera Electrónica (14 de abril de 2016).

[65] Andrew Clement y Jonathan Obar, "Canadian Internet 'boomerang' traffic and mass NSA surveillance: Responding to privacy and network sovereignty challenges", en *Law, Privacy and Surveillance in Canada in the Post-Snowden Era,* Michael Geist, ed. (University of Ottawa Press, 2015).

[66] De Cix, "Information on the lawsuit against the Federal Republic of Germany" (16 de septiembre de 2016).

[67] Geoff Huston, "The death of transit?", Asia Pacific Network Information Centre (27 de octubre de 2016).

[68] Vangie Beal, "CDN – Content Delivery Network", Webopedia.

[69] John Holowczak y Amir Houmansadr, "CacheBrowser: bypassing Chinese censorship without proxies using cached content" (2015).

[70] Geoff Huston, "The death of transit?", Asia Pacific Network Information Centre (27 de octubre de 2016).

en otros sitios que, aunque no estaban afiliados, compartían la misma red de distribución de contenido, lo que llevó a los investigadores a creer que las autoridades habían atacado esa red en particular[71]. En China, aparentemente un filtro nacional ha bloqueado la red de distribución de contenido de EdgeCast, que procesa el contenido de un gran número de sitios web del país[72].

38. Como las redes de distribución de contenido procesan un gran volumen de solicitudes de usuarios de contenido de Internet de múltiples sitios web y plataformas, también son vulnerables a la vigilancia de los Gobiernos. En 2016, por ejemplo, Amazon Web Services, que acoge a una de las mayores redes de distribución de contenido del mundo[73], informó de que las solicitudes de los Gobiernos de acceso a los datos se duplicaron con creces respecto del año anterior[74]. Los investigadores también consideran que las actividades de vigilancia masiva se centran estratégicamente en las redes de distribución de contenido para maximizar la recopilación de información, aunque la forma concreta en que esto se lleva a cabo y el alcance de la participación de la red de distribución de contenido, en su caso, no están claros[75].

D. Proveedores de equipo de red

39. Los proveedores suministran el equipo y los programas informáticos que forman la base de Internet y las redes de telecomunicaciones. El equipo de red normalmente incluye *routers*, conmutadores y puntos de acceso que facilitan la interconexión de múltiples dispositivos y redes (véase A/HRC/32/38, párr. 18). Los proveedores también han diversificado sus actividades para suministrar equipo de protocolo de transmisión de voz por Internet (VoIP), que facilita llamadas inalámbricas, y tecnología de la Internet de las cosas (IoT), que permite la creación de redes entre dispositivos inteligentes[76]. Los proveedores rara vez tratan directamente con los consumidores: sus principales clientes son los operadores de redes, como los Gobiernos, los proveedores de servicios de Internet y las redes de distribución de contenido. Como resultado de ello, están obligados a configurar las redes basándose en las especificaciones técnicas solicitadas por esos operadores, incluidas aquellas dictadas por la legislación local (como los requisitos de aplicación de la ley y de seguridad nacional). Sin embargo, los proveedores también pueden diseñar o modificar el equipo y la tecnología a fin de asegurar la coherencia con las especificaciones privadas o gubernamentales.

40. En vista de su modelo comercial, los proveedores deben responder a los retos en materia de derechos humanos que enfrentan o crean sus clientes. En la esfera de la vigilancia, los proveedores muchas veces se ven obligados por las medidas de "interceptación legal", que requieren la configuración de redes para que los Gobiernos tengan acceso a los datos de los usuarios[77]. Además, los proveedores pueden ser contratados para establecer "sistemas de administración y mediación" que facilitan el intercambio de los datos interceptados entre el operador de la red y la autoridad gubernamental, así como los sistemas gubernamentales que procesan los datos

[71] Leonid Evdokimov y Vasilis Ververis, "Egypt: Media censorship, Tor interference, HTTPS throttling and ads injections?", Open Observatory of Network Interference (27 de octubre de 2016).

[72] Joss Wright, "A quick investigation of EdgeCast CDN blocking in China", blog, Oxford Internet Institute (18 de noviembre de 2014).

[73] En el momento de redactarse el presente informe, Amazonas Cloudfront acogía el mayor número de dominios de sitios web del mundo.

[74] Amazon Information Request Report (junio de 2016).

[75] Véase, por ejemplo, Harrison Weber, "How the NSA & FBI made Facebook the perfect mass surveillance tool", *Venture Beat* (15 de mayo de 2014).

[76] Michael E. Raynor y Phil Wilson, "Beyond the dumb pipe: The IoT and the new role for network service providers", Deloitte University Press (2 de septiembre de 2015).

[77] Véase, por ejemplo, resolución del Consejo de la Unión Europea de 17 de enero de 1995 sobre la interceptación legal de las telecomunicaciones, *Diario Oficial* núm. C 329; y comunicación de Privacy International, págs. 2 y 3.

interceptados[78]. En los casos en que los proveedores también administran las redes que han construido, también pueden ser responsables de tramitar las solicitudes gubernamentales de datos de los usuarios en nombre del operador[79].

41. El diseño del equipo y la tecnología de red con múltiples usos plantea preocupaciones relativas a la libertad de expresión y la privacidad. Por ejemplo, los dispositivos de inspección profunda de paquetes se utilizan para fines técnicos inocuos, como la administración de la congestión de la red, y también se han empleado para filtrar contenidos de Internet, interceptar comunicaciones y ralentizar las corrientes de datos. Las redes de telefonía móvil están configuradas para detectar en tiempo real la ubicación de teléfonos móviles a fin de garantizar el acceso a servicios de telefonía móvil desde cualquier lugar, pero esa detección puede utilizarse también para apuntar a los usuarios[80].

42. Algunos datos indican que los proveedores pueden proporcionar apoyo a la censura y la vigilancia por los Gobiernos. En un caso pendiente ante los tribunales de los Estados Unidos, se ha acusado a Cisco de ayudar a diseñar, aplicar y mantener una red de vigilancia y seguridad interna china conocida como Escudo de Oro[81]. (Cisco niega esas afirmaciones[82].) En Etiopía, los grupos de derechos humanos determinaron que ZTE Corporation había diseñado e instalado una base de datos de gestión de clientes para Ethio Telecom que permitía la vigilancia invasiva[83].

E. Otros agentes privados

43. Las conclusiones y recomendaciones que figuran en el presente informe se aplican a toda entidad que se ocupa del suministro de acceso digital, como se ha descrito más arriba. Un número cada vez mayor de empresas de Internet está incorporando servicios e infraestructura de acceso digital a su cartera de servicios. Por ejemplo, Alibaba y Tencent, dos de las mayores empresas chinas de Internet, ahora también ofrecen servicios de distribución de contenido en sus redes[84]. Google ha venido experimentando con métodos para proporcionar acceso inalámbrico que dejan de lado a los proveedores tradicionales; en 2010, puso en marcha un servicio de conexión a Internet de alta velocidad para hogares y empresas de ciudades seleccionadas de los Estados Unidos[85]. También está trabajando con Facebook y Microsoft para construir redes de cables submarinos que les permitan conectar a los usuarios sin depender de equipos o sistemas de terceros[86].

44. Las organizaciones de elaboración de normas, aunque no sean estrictamente "agentes del sector", establecen los protocolos y las normas técnicos que permiten la interoperabilidad en la infraestructura de telecomunicaciones e Internet. La elaboración de normas que no tiene en cuenta los aspectos de derechos humanos puede afectar negativamente a la libertad de expresión. Por ejemplo, el hecho de que la incorporación de la seguridad de capa de transporte (TLS) como característica del protocolo de transferencia de hipertexto (HTTP) no sea obligatoria dejó al tráfico en la web vulnerable a la censura y la vigilancia. Por consiguiente, los esfuerzos de la comunidad técnica para incorporar la

[78] IHRB, "Human rights challenges of telecommunications vendors: addressing the possible misuse of telecommunications systems: case study: Ericsson" (noviembre de 2014), pág. 16.

[79] *Ibid.*, pág. 17.

[80] *Ibid*., pág. 13.

[81] Tribunal de Distrito de los Estados Unidos, Distrito Norte de California, División San José, *Doe y otros c. Cisco Systems, Inc. y otros*, causa núm. 5:11-cv-02449-EJD-PSGx (18 de septiembre de 2013).

[82] John Earnhardt, "Cisco Q&A on China and censorship", blogs de Cisco (2 de marzo de 2006).

[83] Human Rights Watch, "They know everything we do: telecom and Internet surveillance in Ethiopia" (25 de marzo de 2014).

[84] Tencent Cloud CDN y Alibaba Cloud CDN.

[85] Klint Finley, "Google eyes blazing-fast wireless as a way into your home", *Wired* (12 de agosto de 2016).

[86] Joon Ian Wong, "Google and Facebook are doubling down on Internet infrastructure with a new Pacific cable", *Quartz* (17 de octubre de 2016).

diligencia debida en materia de derechos humanos en la elaboración de normas es un paso en la dirección correcta[87].

IV. Responsabilidades en materia de derechos humanos de los proveedores de acceso digital

45. Los Principios Rectores sobre las Empresas y los Derechos Humanos reconocen la responsabilidad de las empresas de respetar los derechos humanos, independientemente de las obligaciones de los Estados o de la puesta en práctica de esas obligaciones (véase A/HRC/17/31, anexo; y A/HRC/32/38, párrs. 9 y 10). Ofrecen una línea de base mínima para la rendición de cuentas corporativa en materia de derechos humanos que insta a las empresas a adoptar declaraciones públicas de su compromiso de respetar los derechos humanos, refrendadas por funcionarios o ejecutivos directivos superiores; realizar los procesos de diligencia debida que "determinen, prevengan, mitiguen y expliquen" de forma sustantiva las repercusiones reales y potenciales sobre los derechos humanos de todas las operaciones de la empresa; y disponer la reparación de las consecuencias negativas sobre los derechos humanos o cooperar en esta (véase A/HRC/17/31, anexo, principios 16 a 24).

A. Aspectos relacionados con el contexto

46. Los Principios Rectores subrayan la necesidad de que las empresas tengan en cuenta las particularidades del contexto en que operan al ejecutar sus responsabilidades en materia de derechos humanos *(ibid.)*. En el sector del acceso digital, deben tenerse en cuenta varios contextos.

Los proveedores de acceso suministran un bien público

47. El sector del acceso digital es parte del negocio de la expresión digital; su viabilidad comercial depende de usuarios que buscan, reciben y facilitan información e ideas en las redes que construye y opera. Dado que las redes de propiedad privada son indispensables para el ejercicio de la libertad de expresión contemporánea, sus operadores también asumen funciones sociales y públicas esenciales. Las decisiones del sector, ya sea en respuesta a las demandas gubernamentales o sobre la base de intereses comerciales, pueden afectar directamente a la libertad de expresión y los derechos humanos conexos de formas beneficiosas y perjudiciales.

Las restricciones al acceso a Internet afectan a la libertad de expresión en todo el mundo

48. Las repercusiones del sector sobre los derechos humanos muchas veces son mundiales y afectan a los usuarios, incluso en mercados que trascienden los que atiende la empresa de que se trate. Por ejemplo, la vigilancia de un solo punto de intercambio de Internet en los Estados Unidos puede captar grandes corrientes de comunicaciones entre estadounidenses y extranjeros, e incluso algunas únicamente entre extranjeros. Del mismo modo, las vulnerabilidades de seguridad en el diseño de las redes afectan a todos los usuarios que dependen de la red comprometida para el acceso digital, incluidos los usuarios situados lejos de la red. Por consiguiente, las empresas deben identificar y abordar las repercusiones más amplias de sus actividades sobre la libertad de expresión en general, además de sus efectos en los clientes o titulares de derechos en los mercados en que operan. Sin duda, la manera en que explican sus efectos puede variar en función de su tamaño, los recursos, la propiedad, la estructura y el contexto operativo (*ibid.*, principio 14). Por ejemplo, todos los proveedores deben investigar las solicitudes de datos de los usuarios para determinar si cumplen un conjunto mínimo de formalidades, independientemente del

[87] Internet Research Task Force, "Research into human rights protocol considerations" (25 de febrero de 2017). Puede consultarse en https://datatracker.ietf.org/doc/draft-irtf-hrpc-research/?include_text=1. El anexo complementario analiza más detenidamente las funciones y responsabilidades de las organizaciones de elaboración de normas.

origen de la solicitud o el usuario afectado. Sin embargo, mientras que un proveedor multinacional puede contar con equipos especiales de investigación, un proveedor de tamaño pequeño o mediano puede encargar a sus equipos jurídicos o de políticas públicas que desempeñen esa función.

El sector es vulnerable a la presión del Estado contra la libertad de expresión...

49. Los Principios Rectores procuran subsanar las deficiencias que persisten en la rendición de cuentas de las empresas debido a la falta de legislación nacional o de su aplicación[88]. Sin embargo, la aplicación rigurosa del derecho interno también plantea problemas de derechos humanos en el sector del acceso digital. Por ejemplo, los Estados pueden responsabilizar a los proveedores por el contenido publicado por los usuarios en sus redes o presionarlos para que lo restrinjan, con arreglo a leyes tan variadas como las relativas a los delitos de incitación al odio, difamación, cibernéticos y lesa majestad. Sin embargo, esa responsabilidad intermediaria crea un fuerte incentivo para censurar: los proveedores podrían considerar más seguro no impugnar una reglamentación de ese tipo sino regular excesivamente el contenido de modo que también se restrinja la expresión legítima y lícita. La presión para prestar asistencia en la censura y la vigilancia estatales también se intensifica cuando las autoridades hostigan, amenazan o detienen a empleados o intentan manipular las redes o los equipos de la empresa[89].

... pero también se encuentra en una posición única para asegurar el respeto de los derechos de los usuarios

50. La doble función del sector como facilitador del acceso digital y punto natural para las restricciones impuestas por los Estados destaca su importancia como baluarte contra los excesos públicos y privados. Por ejemplo, los proveedores de servicios suelen estar en mejores condiciones de frenar una solicitud de interrupción del servicio o de datos de los usuarios. Las redes de distribución de contenido están en una situación estratégica dentro de la infraestructura de Internet para contrarrestar los ataques malintencionados que perturban el acceso. Los proveedores están especialmente cualificados para evaluar si sus productos se utilizan o se utilizarán para facilitar abusos de los derechos humanos, en particular cuando llevan a cabo la diligencia debida en los procesos de venta o prestan servicios permanentes.

B. Responsabilidad de respetar la libertad de expresión de los usuarios

51. Para poner en práctica sus compromisos en materia de derechos humanos, el sector del acceso digital debe asignar recursos suficientes por lo menos a las prácticas que se describen a continuación. Aunque estos principios se evalúan en el contexto del acceso digital, también son pertinentes para otros sectores de la economía digital, como las redes sociales, el comercio, la vigilancia y las búsquedas.

1. Diligencia debida

52. Los procesos de diligencia debida permiten que un proveedor de acceso digital determine, prevenga y mitigue las repercusiones sobre los derechos humanos de sus actividades (véase A/HRC/17/31, anexo, principio 19). Si bien un enfoque único de la diligencia debida no es posible ni aconsejable, las evaluaciones del impacto en los derechos

[88] Yael Ronen, "Big Brother's little helpers: the right to privacy and the responsibility of Internet service providers", *Utrecht Journal of International and European Law*, vol. 31, núm. 80 (febrero de 2015), pág. 76.

[89] En 2014, un pedido de interrupción del servicio que recibió el proveedor multinacional de telecomunicaciones Orange de las autoridades de la República Centroafricana supuestamente estuvo "acompañada de la amenaza de sanciones personales en caso de incumplimiento". Véase la comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, pág. 11.

humanos constituyen un medio de medir y abordar los riesgos a la libertad de expresión y la privacidad[90]. La diligencia debida supone por lo menos los siguientes elementos.

Políticas que rijan la realización de la diligencia debida

53. Las empresas deben establecer criterios claros y específicos para determinar las actividades que afectan a la libertad de expresión y poner en marcha los procesos de diligencia debida[91]. Los efectos pasados y presentes de una empresa en los derechos humanos, así como la práctica del sector, proporcionan indicadores útiles. En el sector del acceso digital, estas actividades podrían incluir fusiones y adquisiciones; la entrada o la salida del mercado; solicitudes gubernamentales o no gubernamentales de restricción al contenido o de datos de los usuarios; la formulación o modificación de las políticas de restricción al contenido y la privacidad; cambios de productos relativos a la moderación del contenido o comunicaciones cifradas; mecanismos que facilitan el acceso priorizado a contenido y aplicaciones en Internet; el diseño, la venta y la compra de equipo y tecnologías de interceptación y filtrado, así como los servicios de capacitación y consultoría conexos[92]. Esta lista, que dista mucho de ser exhaustiva, "exige una vigilancia y actualización constante", teniendo en cuenta las nuevas esferas de negocios, la evolución de la tecnología y otros cambios en el contexto operativo[93].

Cuestiones que han de examinarse

54. Los procesos de diligencia debida deben examinar de manera crítica al menos la legislación local y las leyes y normas internacionales aplicables, incluidos los posibles conflictos entre la legislación local y los derechos humanos; los riesgos a la libertad de expresión y la privacidad incorporados en los productos y servicios de la empresa; las estrategias para mitigar y prevenir esos riesgos; los límites sobre la eficacia de esas estrategias, habida cuenta del entorno jurídico, reglamentario u operativo en que funciona la empresa; y el potencial para promover los derechos humanos en todas las operaciones de la empresa[94].

Proceso interno y capacitación

55. Si bien los profesionales que se ocupan de las cuestiones de los derechos humanos en las operaciones de una empresa son importantes, no deben ser los únicos responsables de la diligencia debida, sino que otros grupos funcionales pertinentes de la empresa también deben intervenir. Ello exige el diálogo y la colaboración entre distintas unidades de la empresa (como las encargadas del derecho a la privacidad, la aplicación de la ley, las relaciones con el gobierno, el cumplimiento, la gestión de riesgos, el desarrollo de productos y las operaciones) y profesionales (como ingenieros, investigadores de las experiencias de los usuarios, equipos de ventas y ejecutivos de la empresa)[95]. En el contexto de la privacidad, los investigadores han llegado a la conclusión de que "atraer la participación de altos ejecutivos de unidades y asignarles responsabilidades" en la gestión de la privacidad y "dotar al personal de conocimientos especializados sobre la protección de la intimidad y la responsabilidad personal de la privacidad [...] en las unidades de la

[90] Entre los principales proveedores de telecomunicaciones que han realizado evaluaciones del impacto en los derechos humanos figuran Telia Company y Telefónica. *Ibid*., págs. 7 y 8.

[91] Nokia ha incorporado una función automatizada que marca las posibles ventas que plantean riesgos relativos a los derechos humanos en su herramienta de ventas. *Ibid*., pág. 7.

[92] Comisión Europea, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), págs. 32 a 36.

[93] Michael A. Samway, "Business, human rights and the Internet: a framework for implementation", en *Human Dignity and the Future of Global Institutions*, Mark P. Lagon y Anthony Clark Arend, eds. (Washington D.C., Georgetown University Press, 2014), pág. 308.

[94] *Ibid*., págs. 310 a 312, para un panorama más amplio de los temas pertinentes que deben abarcar los procesos de diligencia debida.

[95] Comisión Europea, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pág. 36.

empresa" crea un entorno propicio para la protección de la privacidad[96]. Otras prácticas de gestión similares podrían asegurar el respeto de la libertad de expresión por la empresa. En el caso de las pequeñas y medianas empresas, estas consideraciones podrían requerir que todo el personal participe en las actividades de diligencia debida[97].

Conocimientos especializados externos

56. Habida cuenta de la amplia base de conocimientos necesarios, los procesos de diligencia debida tienen que aprovechar los conocimientos especializados externos no gubernamentales, entre otros de la sociedad civil, las organizaciones internacionales de derechos humanos, los mecanismos de derechos humanos de organizaciones internacionales y regionales, las instituciones académicas y la comunidad técnica. Los foros de múltiples interesados también ofrecen oportunidades de aprendizaje compartido y rendición de cuentas mutua. Por ejemplo, los investigadores han llegado a la conclusión de que la participación en iniciativas sobre derechos humanos específicas del sector o la industria, como la Global Network Initiative y el Grupo de Diálogo de la Industria de las Telecomunicaciones, coincide con el cumplimiento de las empresas en cuanto a la protección de los derechos humanos[98].

Consultas con los usuarios y los titulares de derechos afectados

57. Todos los proveedores de acceso digital afectan a la libertad de expresión de los usuarios finales en una u otra forma. Por consiguiente, incluso las empresas que no tienen contacto directo con los consumidores deben consultar a los usuarios finales como parte de su proceso de evaluación de riesgos. Esas consultas se distinguen de los esfuerzos más amplios de participación de interesados múltiples descritos más arriba y contempla un "diálogo bidireccional" para "reunir opiniones concretas o asesoramiento de los interesados afectados (o sus representantes) que luego se tienen en cuenta en los procesos internos de adopción de decisiones e implementación de la empresa"[99]. Por ejemplo, podría consultarse a personas y grupos vulnerables o marginados mientras se realizan las negociaciones para la obtención de licencias en entornos operativos de alto riesgo o durante el diseño, las pruebas y la implantación de políticas de tarifa cero. Las consultas sustantivas deben incluir actividades de divulgación periódicas dirigidas a las organizaciones de la sociedad civil, que podrían constituir un indicador útil de las necesidades y los intereses de los usuarios finales en determinadas comunidades, y que a su vez podrían exponerse a un mayor riesgo de presión por sus actividades de promoción.

Evaluaciones de la dinámica existente

58. Las empresas deben adaptar rápidamente los procesos de diligencia debida a los cambios en las circunstancias o el contexto operacional. Por ejemplo, la evaluación de los riesgos debe continuar después de la fase de diseño y a intervalos regulares durante todo el ciclo de vida del producto o servicio, teniendo en cuenta factores como los cambios en la tecnología y la infraestructura y las vulnerabilidades conexas de la seguridad, las alteraciones del comportamiento de los consumidores, y las modificaciones de la situación jurídica, política y social en la que operan las empresas[100].

2. Incorporación de salvaguardias de los derechos humanos en la etapa de diseño

59. Tal como sucede con todo desarrollo de tecnología importante, las opciones de diseño e ingeniería reflejan consideraciones de políticas públicas y deben guiarse por el

[96] Kenneth A. Bamberger y Deirdre K. Mulligan, *Privacy on the Ground: Driving Corporate Behavior in the United States and Europe* (Cambridge, Massachusetts, MIT Press, 2015), pág. 177.

[97] Comisión Europea, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), pág. 37.

[98] Comunicación de Ranking Digital Rights, pág. 5.

[99] Comisión Europea, *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights* (2013), págs. 37 y 38.

[100] Business for Social Responsibility, Applying the Guiding Principles on Business and Human Rights to the ICT industry, Version 2.0: Ten lessons learned, documento de información (septiembre de 2012), pág. 9.

respeto de los derechos humanos. Por ejemplo, la "fragmentación de redes" *(network slicing)*, una tecnología clave para redes 5G, puede permitir a los proveedores de telefonía móvil gestionar el tráfico de manera más eficiente y atender a la creciente diversidad de necesidades de los consumidores en la era de la Internet de las cosas (IoT). Al mismo tiempo, las redes también pueden "fragmentarse" en vías rápidas y lentas que den prioridad al acceso a algunas aplicaciones de Internet sobre otras, lo que podría interferir con la neutralidad de la red. Por consiguiente, las empresas deben asegurarse de que las innovaciones en el equipo y la tecnología de red, en particular los que tienen usos múltiples, estén diseñadas y desplegadas para que sean compatibles con la libertad de expresión y las nomas de privacidad[101].

60. Las empresas deben asumir un papel activo y comprometido en la elaboración de medidas de mejora de la libertad de expresión y la privacidad. Por ejemplo, las medidas de seguridad digital que detectan y previenen ataques distribuidos de denegación del servicio y la piratería deben ponerse en práctica de manera que apunten al tráfico malintencionado sin comprometer la interacción legítima entre personas, organizaciones y comunidades. La configuración del equipo de red para reducir al mínimo la reunión de información innecesaria acerca de los usuarios, habida cuenta de los requisitos locales jurídicos y de direccionamiento, evita eficazmente las solicitudes de datos excesivamente amplias, ya que las empresas no pueden entregar información que no tienen[102]. Aunque la información sobre los usuarios se registre, la fijación de límites importantes acerca de si esta debe conservarse y durante cuánto tiempo, también limita el alcance de los datos personales y confidenciales disponibles para su acceso por terceros.

3. Participación de los interesados

61. El involucramiento de los Gobiernos, las empresas asociadas y otras partes interesadas en las cuestiones de derechos humanos puede impedir o mitigar las violaciones de los derechos humanos más adelante. Las empresas que tratan directamente con los Gobiernos deben impulsar las salvaguardias de los derechos humanos en las licencias de explotación y los contratos de venta, por ejemplo, garantizar que no pueda accederse al equipo de red ni que este pueda modificarse sin el conocimiento de la empresa (lo que podría hacerse a los efectos de facilitar los abusos de los derechos humanos). La intervención oportuna en litigios (como presentaciones de *amicus curiae* en causas incoadas por grupos de la sociedad civil o empresas del sector contra leyes de censura o vigilancia) y las medidas de presión relativas a los derechos humanos en los procesos legislativos y de formulación de políticas también pueden promover la protección jurídica de la libertad de expresión y la privacidad.

62. Los acuerdos con empresas asociadas deben permitir que todas las partes cumplan sus responsabilidades en materia de derechos humanos. En particular, estos acuerdos deben concebirse para asegurar que las filiales, los asociados de empresas conjuntas, los proveedores y los distribuidores cumplan las políticas relativas a la libertad de expresión y la privacidad que la empresa haya establecido. Por ejemplo, cuando las operaciones locales reciben solicitudes de censura o vigilancia no habituales, la política de la empresa debe velar por que estas se comuniquen a los directivos a nivel mundial para su examen[103]. También deben ponerse mecanismos de denuncia de irregularidades a disposición de los empleados y los contratistas. En la medida en que las empresas ya mantienen relaciones comerciales que plantean preocupaciones en materia de derechos humanos, deben tratar de fortalecer su influencia a lo largo del tiempo para prevenir o mitigar el daño que puedan ocasionar[104].

[101] ARTICLE 19, "Our 5G future: Light at the end of the tunnel or Internet fast-lane for the elite?" (15 de septiembre de 2016).

[102] Fundación de la Frontera Electrónica, "User privacy for ISPs and accidental ISPs".

[103] Comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, págs. 13 y 16.

[104] SHIFT, "Using leverage in business relationships to reduce human rights risks" (Nueva York, noviembre de 2013).

63. Las empresas también pueden mejorar el respeto de los derechos humanos por medio de la adopción de medidas de colaboración. Esa colaboración incluye actividades conjuntas de extensión y promoción con empresas del sector; la cooperación con órganos regionales o internacionales, incluidos los mecanismos de derechos humanos y las instituciones económicas; y la participación en asociaciones del sector e iniciativas de interesados múltiples[105]. Las consultas periódicas con los usuarios, la sociedad civil y los titulares de derechos afectados también pueden movilizar el apoyo público a los esfuerzos de la empresa para resistir las extralimitaciones de los Gobiernos. La colaboración intersectorial fortalece la solidez normativa de las mejores prácticas y normas en materia de derechos humanos acordadas, intensificando la presión sobre los Gobiernos y las empresas del sector para que las cumplan.

4. Estrategias de mitigación[106]

64. En la medida en que las empresas se ocupan de la reglamentación de los contenidos y las solicitudes de datos de los usuarios, pueden adoptarse políticas y prácticas específicas para mitigar los daños de las restricciones impuestas por los Gobiernos.

Velar por que las solicitudes de restricciones al contenido y de datos de los clientes cumplan estrictamente la ley

65. Las empresas deben velar por que todas las solicitudes de restricciones al contenido y de datos de los clientes cumplan no solo los requisitos de procedimiento y jurídicos especificados en la legislación local, sino también las normas relativas a las garantías procesales establecidas en el plano internacional[107]. Habida cuenta de su pertinencia para los derechos humanos, esas solicitudes deben ser autorizadas por tribunales u órganos jurisdiccionales independientes e imparciales. Además, las empresas deben exigir que las solicitudes se hagan por escrito e incluyan una explicación clara de la base jurídica y el nombre, cargo y firma del funcionario autorizante. Las empresas también deben tratar de verificar que el funcionario o entidad gubernamental pertinente esté autorizado a emitir esa solicitud[108]. Estas formalidades deben cumplirse aunque la legislación no las requiera. Además, las empresas deben mantener un registro escrito de todas las comunicaciones entre ellas y el solicitante relativas a cada una de las solicitudes y registros de acceso a los datos de los usuarios al ejecutar la solicitud, siempre que dicho registro no plantee riesgos indebidos de la privacidad[109].

Interpretación del alcance de las solicitudes gubernamentales y las leyes

66. Los marcos jurídicos y las solicitudes de los Gobiernos imprecisos y abiertos hacen difícil la labor de las empresas de determinar si cumplen la legislación local. Sin embargo, las empresas pueden mitigar esa incertidumbre mediante la adopción de políticas a nivel de toda la empresa que encomienden a todas las unidades de la empresa, incluidas las filiales locales, que resuelvan cualquier ambigüedad jurídica en favor del respeto de la libertad de expresión, la privacidad y otros derechos humanos. Estas políticas se basan no solo en las responsabilidades en materia de derechos humanos de los proveedores, sino también en la obligación de los Estados de cumplir las leyes aplicables en materia de derechos humanos y las disposiciones pertinentes de protección en el marco de la legislación local (como la Constitución y las leyes de procedimiento penal y de protección de datos).

[105] Comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, pág. 12; y comunicación de Global Network Initiative, pág. 7

[106] La orientación proporcionada en la presente sección se nutrió en gran medida de la comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones y de Global Network Initiative, “Implementation guidelines for the principles on freedom of expression and privacy”.

[107] Véanse, por ejemplo, los Principios de Manila sobre la Responsabilidad de los Intermediarios y los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, redactados en conjunto por varias organizaciones no gubernamentales.

[108] Global Network Initiative, “Implementation guidelines”, págs. 5 y 6; y comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, págs. 8 a 10.

[109] Comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, págs. 8 y 9.

67. En la práctica, las empresas deben, en la medida en que se pueda, interpretar las solicitudes de manera que se vele por la menor restricción posible al contenido y el acceso a los datos de los clientes. Por ejemplo, cuando las solicitudes parecen excesivamente amplias, Global Network Initiative recomienda a las empresas que pidan aclaraciones sobre su alcance y obtengan las modificaciones apropiadas[110].

Impugnación de las solicitudes y leyes subyacentes

68. Las empresas tienen interés en operar en un entorno jurídico que respete los derechos humanos, las normas de debido proceso y el estado de derecho. Las empresas deben estudiar todas las opciones jurídicas para impugnar las solicitudes que son excesivamente invasivas, como las solicitudes de interrupción del servicio o de plataformas enteras, la retirada de sitios web dirigida evidentemente a contenidos críticos o de disenso, o las solicitudes de datos de clientes que abarquen a un número amplio de usuarios no especificados[111].

69. Al igual que cualquier decisión de incoar un procedimiento judicial, las empresas pueden tener en cuenta una serie de consideraciones, como los "posibles efectos beneficiosos [en materia de derechos humanos], las probabilidades de éxito, la gravedad del caso, los costos, la representatividad del caso y si el caso es parte de una tendencia más amplia"[112]. Sin embargo, las empresas deben atribuir un peso considerable a los aspectos de derechos humanos en sus procesos de adopción de decisiones y evaluar cuidadosamente los posibles beneficios y riesgos para los derechos humanos. Por ejemplo, las empresas deben estar dispuestas a impugnar las solicitudes demasiado amplias cuando exista una probabilidad razonable de éxito, aun cuando esos desafíos podrían requerir una gran cantidad de recursos; por otra parte, las empresas pueden buscar otras opciones si hay probabilidades de que la impugnación cree un precedente o una reacción adversos y socave la libertad de expresión y la privacidad.

5. Transparencia

70. La transparencia es una característica fundamental que el sector del acceso digital tiene la responsabilidad de respetar. La información sobre las actividades gubernamentales que requieren asistencia o participación empresarial debe divulgarse en la mayor medida permitida por la ley. Las empresas deben ser conscientes de que la sociedad civil utiliza esa información principalmente para impugnar los abusos de los derechos humanos en los tribunales, denunciar agravios ante los mecanismos nacionales o internacionales en nombre de los usuarios o buscar otros medios de rendición de cuentas. En consecuencia, esa divulgación de información debe ser periódica y permanente, y tener un formato accesible que proporcione el contexto adecuado.

71. Aun si la legislación local limita la transparencia plena, las empresas deben divulgar toda la información publicable pertinente. Por ejemplo, si las empresas tienen prohibido revelar el origen o la base de una solicitud de interrupción del servicio, deben tratar de proporcionar información actualizada de manera periódica sobre los servicios afectados o restablecidos, las medidas que estén adoptando para abordar la cuestión y las explicaciones después del hecho. Algunas medidas de transparencia innovadoras, como la publicación de datos agregados y la retención selectiva de información[113], también mitigan los efectos de las órdenes de reserva y otras leyes de divulgación. Las empresas deben divulgar todas las leyes locales que respetan y, cuando sea posible, impugnar toda ley o reglamento que impida o dificulte que sean transparentes ante los usuarios y el público en general[114].

[110] *Ibid*.

[111] Yael Ronen, "Big Brother's little helpers" (febrero de 2015), pág. 81.

[112] Global Network Initiative, "Implementation guidelines".

[113] Por ejemplo, cuando se exigió a "Telia Company que suspendiera los servicios, la empresa no afirmó que se había debido a problemas técnicos", comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, pág. 14.

[114] Grupo de Diálogo de la Industria de las Telecomunicaciones, "Information on country legal frameworks pertaining to freedom of expression and privacy in telecommunications" (2016).

72. Las empresas deben divulgar sus políticas y medidas que afectan a la libertad de expresión. Estas incluyen las políticas de retención y uso de datos, las prácticas de gestión de redes y la venta y la compra de tecnologías de filtrado e interceptación[115]. Las empresas también deben divulgar información sobre la frecuencia, el alcance y el tema de los procesos de diligencia debida y un resumen de las conclusiones de alto nivel. En general, las empresas deben consultar los recursos, cada vez más numerosos, que analizan los valiosos indicadores de transparencia y otras buenas prácticas en materia de transparencia. También debe consultarse a los usuarios, la sociedad civil y las empresas del sector acerca del diseño y la aplicación de las medidas de transparencia.

6. Reparación efectiva

73. Si bien algunos aspectos de la responsabilidad de las empresas han avanzado en los últimos años, las medidas de reparación a menudo suelen estar ausentes de la agenda del sector privado. Sin embargo, la reparación es un pilar fundamental de la responsabilidad de las empresas y debe suministrarse siempre que una empresa haya "provocado o contribuido a provocar consecuencias negativas" (véase A/HRC/17/31, anexo, principio 22). Los Estados tienen la obligación primordial de reparar las violaciones de los derechos humanos relacionadas con empresas, en particular las que instigan, como la restricción excesiva al contenido, las solicitudes ilícitas de datos de los usuarios y la vigilancia desproporcionada. Sin embargo, las empresas que no aplican medidas adecuadas de diligencia debida y otras salvaguardias también pueden provocar esos abusos o contribuir a ellos. En esas situaciones, las empresas deben "reparar [las consecuencias negativas] o contribuir a su reparación por medios legítimos" *(ibid.)*.

74. La reparación puede ser tanto financiera como no financiera (*ibid*., principio 27). Cuando la libertad de expresión se ve menoscabada, los recursos adecuados pueden incluir el acceso a mecanismos de reclamación e información sobre la violación y garantías de no repetición[116]. Los usuarios cuyas cuentas hayan sido injustamente suspendidas podrían requerir la satisfacción de ser escuchados y recibir explicaciones y garantías de no repetición[117].

75. También pueden reformarse o fortalecerse las políticas y los mecanismos preexistentes para responder a las violaciones de la libertad de expresión. Por ejemplo, un proveedor podría introducir mejoras en su política de restricción de contenido y capacitar a sus equipos de moderación de contenido para reducir la probabilidad de una retirada injusta de sitios web o de restricciones excesivas al contenido, como el filtrado. Los mecanismos de denuncia de los clientes también podrían actualizarse para permitir a los usuarios detectar las prácticas de gestión del tráfico de redes, las clasificaciones de filtrado comercial y otras restricciones al contenido que consideren indebidamente restrictivas o injustas.

V. Conclusiones y recomendaciones

76. **Las personas dependen del acceso digital para ejercer derechos fundamentales, incluida la libertad de opinión y de expresión, el derecho a la vida y diversos derechos económicos, sociales y culturales. Además, periódicamente hacen frente a obstáculos al acceso, desde interrupciones del servicio hasta la vigilancia. El presente informe trata mayormente de los obstáculos que deniegan, disuaden o excluyen la libertad de expresión mediante una contundente dependencia de la censura digital. El informe no aborda otros obstáculos graves, como la falta de una infraestructura de conectividad adecuada, los elevados costos de acceso impuestos por los Gobiernos, la desigualdad de género y las barreras lingüísticas, que también pueden constituir formas de**

[115] Comunicación de Ranking Digital Rights.

[116] Comunicación del Grupo de Diálogo de la Industria de las Telecomunicaciones, pág. 17.

[117] Peter Micek y Jeff Landale, "Forgotten pillar: the Telco remedy plan", Access Now (mayo de 2013), pág. 6.

censura[118]. Por consiguiente, se centra en gran parte en las funciones y obligaciones de los Estados. Pero estos ejercen cada vez más la censura por conducto del sector privado. El informe ha tratado de abordar no solo las limitaciones a las acciones estatales en virtud del derecho de los derechos humanos sino también los principios que deben observar los agentes privados para respetar los derechos humanos. A continuación se exponen las principales recomendaciones, que ya se señalaron en el análisis anterior.

Estados y Consejo de Derechos Humanos

77. **El Consejo de Derechos Humanos, en su resolución 32/13, condenó inequívocamente las medidas cuyo objetivo deliberado era impedir u obstaculizar el acceso o la divulgación de información en línea, vulnerando el derecho internacional de los derechos humanos, y exhortó a todos los Estados a que se abstuvieran de adoptar estas medidas, o cesaran de aplicarlas. Esta condena, que es fundamental para la promoción por el Consejo de los derechos humanos en línea, se debe complementar y especificar. La prevención o perturbación deliberada del acceso incluye toda acción que interrumpa o torne ineficaz el acceso a las redes de telecomunicaciones, los servicios de telefonía móvil o las plataformas de las redes sociales. Es importante que el Consejo, en su labor futura, aclare las normas que se aplican al acceso digital, como se describe en el presente informe, para promover el derecho a la libertad de opinión y de expresión en Internet.**

78. **También es decisivo que el Consejo y los Estados establezcan las conexiones entre la injerencia en la privacidad y la libertad de expresión. Sin duda, la injerencia en la vida privada debe evaluarse por sus propios méritos en virtud del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos y otras normas del derecho de los derechos humanos. Pero determinadas injerencias, como las solicitudes excesivas de datos sobre los usuarios y la retención de esos datos por terceros, pueden tener efectos disuasorios de corto y largo plazo sobre la libertad de expresión, y deben evitarse, como cuestión de derecho y de política. Como mínimo, los Estados deben velar por que la vigilancia sea autorizada por una autoridad judicial independiente, imparcial y competente que certifique que la solicitud es necesaria y proporcional para proteger un objetivo legítimo.**

79. **El Relator Especial está especialmente preocupado por las denuncias de amenazas e intimidación a empresas, sus empleados y su equipo e infraestructura. Además, el énfasis del Consejo en el importante papel del sector privado, así como la necesidad de su protección, merece consideración. Los Estados deben examinar todas sus actividades para obtener acceso a la red a fin de garantizar que sean legítimas, necesarias y proporcionadas, prestando especial atención a que constituyan el medio menos invasivo de proteger un objetivo legítimo.**

80. **La función de protección que los Estados pueden ejercer sobre el sector privado debe tener límites. Estos no deben promover la ganancia económica de los agentes privados por sobre los derechos de los usuarios a la libertad de opinión y de expresión. Por consiguiente, los Estados deben prohibir los intentos de asignar prioridad a ciertos tipos de contenido o aplicaciones en Internet por un pago u otros beneficios comerciales.**

81. **La intersección entre la conducta de los Estados y las funciones empresariales en la era digital sigue siendo bastante nueva para muchos Estados. Un camino provechoso a seguir, tanto a nivel internacional como nacional, supondría la elaboración de planes de acción nacionales sobre empresas y derechos humanos a fin de establecer vías significativas para todas las categorías del sector del acceso digital a fin de determinar y abordar sus respectivas repercusiones sobre los derechos humanos.**

[118] Comunicación de la Global Commission on Internet Governance; Arco Iris Libre de Cuba, Centro de Información Hablemos Press, Centro de Información Legal CubaLex, Mesa de Diálogo de la Juventud Cubana Plataforma Femenina Nuevo País, “Situación del derecho a la libertad de opinión y de expresión en Cuba” (julio de 2016), pág. 20.

Agentes privados

82. **Durante años, las personas y las empresas del sector del acceso digital han comprendido que desempeñan un papel esencial en la gran expansión del acceso a la información y los servicios de comunicaciones. Participan en un negocio en que el modelo de éxito debe incluir la ampliación del acceso, la eficiencia, la diversidad y la transparencia. Deben adoptar los principios señalados en el presente informe como herramientas para fortalecer sus propias funciones en la promoción de los derechos de los usuarios a la libertad de expresión. En este espíritu, además de los compromisos de política de alto nivel con los derechos humanos, el sector debe asignar recursos suficientes para el cumplimiento de esos compromisos, incluidas la diligencia debida, las opciones de diseño e ingeniería orientadas a los derechos, la participación de los interesados, las estrategias para evitar o mitigar los riesgos en materia de derechos humanos, la transparencia y la reparación efectiva. Al hacerlo, el diseño y la aplicación de medidas de rendición de cuentas en materia de derechos humanos por las empresas deben nutrirse de los conocimientos especializados internos y externos, y garantizar una aportación cabal de los clientes y otros titulares de derechos afectados, la sociedad civil y la comunidad de derechos humanos.**

83. **Esto no quiere decir que las empresas privadas no hacen frente a presiones. Todo lo contrario. Sin embargo, cuando los Estados solicitan la participación de las empresas en la censura o la vigilancia, estas deben tratar de prevenir o mitigar las repercusiones negativas sobre los derechos humanos de su participación en la mayor medida permitida por la ley. En cualquier caso, las empresas deben adoptar todas las medidas legítimas necesarias para garantizar que no causen violaciones de los derechos humanos, contribuyan a estas ni sean cómplices en estas. Los acuerdos con empresas asociadas deben estructurarse de modo que todas las partes cumplan sus responsabilidades en materia de derechos humanos. Las empresas también deben fortalecer la influencia que tienen en sus relaciones comerciales preexistentes para prevenir o mitigar las repercusiones negativas sobre los derechos humanos.**