Naciones Unidas A/HRC/29/32

Asamblea General

Distr. general
22 de mayo de 2015
Español
Original: inglés

Consejo de Derechos Humanos
29º período de sesiones
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, David Kaye*

Resumen

En el presente informe, preparado de conformidad con la resolución 25/2 del Consejo de Derechos Humanos, el Relator Especial aborda la utilización del cifrado y el anonimato en las comunicaciones digitales. Sobre la base de investigaciones relativas a las normas y la jurisprudencia internacionales y nacionales, y las aportaciones de los Estados y la sociedad civil, en este informe se llega a la conclusión de que el cifrado y el anonimato permiten a los individuos ejercer sus derechos a la libertad de opinión y de expresión en la era digital y, por lo tanto, merecen una protección sólida.

* Documento presentado con retraso.

Índice

I. Introducción

1. Las tecnologías digitales contemporáneas brindan a los gobiernos, empresas, delincuentes y bromistas una capacidad sin precedentes de atentar contra los derechos a la libertad de opinión y de expresión. La censura de la actividad en línea, la vigilancia y la reunión de datos masivas y específicas, los ataques digitales contra la sociedad civil y la represión resultado de la expresión en línea obligan a personas de todo el mundo a protegerse para no ser molestadas a causa de sus opiniones y poder buscar, recibir y difundir informaciones e ideas de toda índole. Muchos tratan de proteger su seguridad a través del cifrado, a saber, la codificación de datos para que solo los destinatarios deseados puedan acceder a ellos, que puede aplicarse a los datos en tránsito (correos electrónicos, mensajes, telefonía por Internet) y en reposo (discos duros, servicios en la nube). Otros buscan protección adicional en el anonimato, y utilizan tecnologías sofisticadas para ocultar su identidad y su huella digital. El cifrado y el anonimato, actualmente las principales vías de seguridad en línea, ofrecen a las personas un medio para proteger su privacidad, al permitirles buscar, leer, elaborar y compartir opiniones e información sin injerencia y al permitir a periodistas, organizaciones de la sociedad civil, miembros de grupos étnicos o religiosos, personas perseguidas debido a su orientación sexual o su identidad de género, activistas, eruditos, artistas y otros ejercer los derechos a la libertad de opinión y de expresión.

2. Aun así, al igual que el teléfono puede utilizarse tanto como para denunciar un delito a la policía como para conspirar para cometerlo, Internet también puede utilizarse de manera indebida para atentar contra los derechos de los demás, la seguridad nacional o el orden público. Con frecuencia, las fuerzas del orden y los servicios de inteligencia afirman que las comunicaciones anónimas o cifradas dificultan la investigación de los delitos financieros, los delitos relacionados con las drogas ilícitas, la utilización de niños en la pornografía y el terrorismo. Se han expresado preocupaciones legítimas por el hecho de que los acosadores y los delincuentes utilizan las nuevas tecnologías para atizar el acoso. Algunos Estados limitan o prohíben el cifrado y el anonimato por estos y otros motivos, y otros proponen o aplican medios para que las fuerzas del orden eludan estas medidas de protección y accedan a las comunicaciones personales.

3. A la luz de estos desafíos, en el presente informe se examinan dos preguntas relacionadas. Por un lado, ¿los derechos a la vida privada y a la libertad de opinión y de expresión amparan la comunicación segura en línea, concretamente a través del cifrado o el anonimato? Por otro lado, si la respuesta fuera afirmativa, ¿hasta qué medida pueden los gobiernos, de conformidad con el derecho de los derechos humanos, imponer restricciones al cifrado y el anonimato? En el presente informe se trata de responder a estas preguntas, examinar ejemplos de la práctica de los Estados y proponer recomendaciones. No se pretende abordar todas las cuestiones técnicas o jurídicas planteadas por las tecnologías digitales, aunque sí se señalan las más importantes para informes futuros.

4. Durante la preparación del informe, el Relator Especial distribuyó un cuestionario a los Estados en que solicitaba información pertinente sobre las leyes, normas, políticas y prácticas nacionales. Hasta el 1 de abril de 2015, 16 Estados habían respondido a esta solicitud[1]. El Relator Especial también publicó una convocatoria de presentación de aportaciones de las partes interesadas no gubernamentales, y organizó una reunión de expertos en Ginebra en marzo de 2015. Las respuestas de los gobiernos y las más de 30 aportaciones presentadas por

[1] Se recibieron respuestas de: Alemania, Austria, Bulgaria, Cuba, Eslovaquia, Estados Unidos de América, Grecia, Guatemala, Irlanda, Kazajstán, Líbano, Noruega, Qatar, República de Moldova, Suecia y Turquía.

organizaciones de la sociedad civil y particulares, que se pueden consultar en el sitio web del titular del mandato, contribuyeron de manera significativa a la preparación del informe.

5. En el sitio web del titular del mandato también se puede consultar un examen completo de las actividades del Relator Especial desde el inicio de su mandato en agosto de 2014. Con este informe, el primero del actual titular del mandato, se busca promover la labor sobre los obstáculos a la libertad de expresión en la era digital.

II. Comunicación segura y privada en la era digital

A. Cifrado y anonimato contemporáneos

6. Los enfoques modernos de la comunicación privada y segura se basan en ideas que han acompañado a la humanidad por milenios. El surgimiento del almacenamiento de datos electrónicos, Internet y la reunión y retención masivas de datos reveló que se necesitarían medios sofisticados para proteger los datos de particulares, empresas y gobiernos. Cuando el correo electrónico, la mensajería instantánea, los protocolos de transmisión de voz por Internet, las videoconferencias y los medios sociales pasaron de ser servicios destinados a un segmento reducido a modos de comunicación predominantes y fáciles de vigilar, los usuarios comenzaron a necesitar seguridad en línea para poder buscar, recibir y difundir informaciones sin riesgo de repercusiones, divulgación, vigilancia u otros usos indebidos de sus opiniones o expresión.

7. El cifrado, un proceso matemático de "convertir mensajes, información o datos en algo ilegible, excepto para el destinatario deseado"[2], protege la confidencialidad y la integridad del contenido contra el acceso o la manipulación de terceros. El cifrado fuerte, que antes era exclusivo de los militares y los servicios de inteligencia, ahora está al alcance del público, a menudo de manera gratuita, para proteger los correos electrónicos, las comunicaciones telefónicas, las imágenes, los discos duros y los navegadores. Con el "cifrado de clave pública", la forma dominante de seguridad de extremo a extremo para los datos en tránsito, el remitente utiliza la clave pública del destinatario para cifrar el mensaje y sus adjuntos, y el destinatario utiliza su propia clave privada para descifrarlo. El cifrado también se puede utilizar para crear firmas digitales con el fin de garantizar que un documento y su expedidor son auténticos, para autentificar y verificar la identidad de un servidor y para proteger la integridad de las comunicaciones entre clientes contra la falsificación o la manipulación del tráfico por terceros (ataques de intermediario). Dado que el cifrado de los datos en tránsito no protege contra los ataques a los datos no cifrados cuando permanecen en reposo en cualquiera de los puntos extremos (ni protege la seguridad de la clave privada), también se pueden cifrar los datos en reposo almacenados en computadoras portátiles, discos duros, servidores, tabletas, teléfonos móviles y otros dispositivos. Asimismo, puede que las prácticas en línea estén comenzando a diferir de los sistemas aquí descritos y estén pasando a la tecnología de "confidencialidad directa" u "off-the-record", en que se conservan las claves de forma efímera, en especial para usos como la mensajería instantánea.

8. Algunos actores piden que se debiliten o se mengüen los estándares de cifrado para que solo los gobiernos puedan acceder a las comunicaciones cifradas. Sin embargo, el cifrado debilitado no puede proteger los datos contra quienes tienen la capacidad de encontrar y aprovechar los puntos débiles, ya sean actores estatales o no estatales, con fines legítimos o ilegítimos. Casi todos los tecnólogos piensan que no existe un acceso especial que pueda estar únicamente al alcance de las autoridades

[2] Véase SANS Institute, "History of encryption" (2001).

estatales, ni siquiera aquellas que, en principio, buscan el interés público. En el entorno tecnológico contemporáneo, el cifrado debilitado intencionalmente, incluso con fines que tal vez sean legítimos, vulnera la seguridad en línea de todos.

9. En particular, el cifrado protege el contenido de las comunicaciones, pero no factores de identidad como la dirección IP, conocidos como metadatos. Mediante su análisis se puede reunir información significativa sobre la identidad de un usuario si este no emplea herramientas de anonimato. El anonimato consiste en impedir la identificación. Atendiendo un deseo humano común de proteger su identidad ante el público, el anonimato puede liberar al usuario para que explore y divulgue ideas y opiniones más de lo que lo haría si utilizara su identidad real. Los usuarios de Internet pueden adoptar seudónimos (o, por ejemplo, falsas cuentas de correo electrónico o de medios sociales) para esconder su identidad, su imagen, su voz y su ubicación, entre otros datos, pero la privacidad lograda mediante esos seudónimos es superficial y puede ser vulnerada fácilmente por los gobiernos u otras personas con los conocimientos técnicos necesarios. Si no se combinan las herramientas de cifrado y anonimato, la huella digital que dejan los usuarios puede revelar fácilmente su identidad. Los usuarios que buscan pleno anonimato o encubrimiento de su identidad (por ejemplo, escondiendo su dirección IP original) frente a la intromisión del Estado o de delincuentes pueden utilizar herramientas como las redes privadas virtuales (VPN), los servicios de proxy, las redes y programas de anonimato, y las redes entre pares[3]. Una herramienta de anonimato conocida, la red Tor, cuenta con más de 6.000 servidores descentralizados en todo el mundo que reciben y transmiten datos varias veces para ocultar la información de identidad sobre los puntos extremos, creando así un anonimato sólido para sus usuarios.

10. Una característica fundamental de la era digital es que la tecnología evoluciona sin cesar para satisfacer las exigencias del usuario. Si bien en el presente informe se mencionan las tecnologías contemporáneas que facilitan el cifrado y el anonimato, los análisis y conclusiones que en él figuran por lo general son válidos para los conceptos en que se apoyan las tecnologías actuales y deberían seguir siendo válidos cuando las nuevas tecnologías remplacen a las antiguas.

B. Usos de las tecnologías

11. Internet es muy valioso para la libertad de opinión y de expresión, porque amplía la voz y multiplica la información al alcance de todo el que pueda acceder a la red. En muy poco tiempo se ha convertido en el principal foro mundial público. Por este motivo, un Internet abierto y seguro debería figurar entre los principales requisitos para el disfrute de la libertad de expresión en la actualidad. No obstante, constantemente amenazado, es un espacio —similar al mundo real— en que la actividad delictiva, la represión individual y la reunión masiva de datos también existen. Por consiguiente, es importante que los usuarios hallen medios para protegerse en línea, que los gobiernos ofrezcan dicha seguridad en la ley y en las políticas y que los actores empresariales diseñen, elaboren y comercialicen productos y servicios seguros por defecto. Ninguno de estos imperativos es nuevo. A principios de la era digital, los gobiernos reconocieron la importancia del cifrado para la seguridad de la economía mundial, al usar o estimular su uso para proteger los números de identificación emitidos por las autoridades, las tarjetas de crédito y la

[3] Los servicios de proxy envían datos a través de un intermediario, o "servidor proxy", que envía información en nombre del usuario, y encubre de manera eficaz la dirección IP del usuario con su propia dirección ante el destinatario final. Las redes entre pares hacen particiones de datos y los almacenan en servidores interconectados y seguidamente cifran esos datos almacenados para que ningún servidor centralizado pueda identificar la información. Véase, por ejemplo, Freenet.

información bancaria, los documentos confidenciales de las empresas y las investigaciones sobre los propios delitos en línea[4].

12. El cifrado y el anonimato, separados o en su conjunto, crean una zona de privacidad para proteger opiniones y creencias. Por ejemplo, permiten las comunicaciones privadas y pueden encubrir una opinión frente al escrutinio externo, algo particularmente importante en los entornos políticos, sociales, religiosos o jurídicos hostiles. Cuando los Estados imponen censuras ilegales a través del filtrado y otras tecnologías, el uso del cifrado y el anonimato puede permitir a los ciudadanos superar los obstáculos y acceder a informaciones e ideas sin la intromisión de las autoridades. Los periodistas, investigadores, abogados y miembros de la sociedad civil pueden utilizar el cifrado y el anonimato para protegerse a sí mismos (y a sus fuentes, clientes y asociados) de la vigilancia y el acoso. La capacidad de buscar en la red, elaborar ideas y comunicarse de manera segura es tal vez, para muchos, la única manera de explorar aspectos básicos de su identidad como el género, la religión, la etnia, el origen nacional o la sexualidad. Los artistas pueden servirse del cifrado y el anonimato para salvaguardar y proteger su derecho a la expresión, en especial en las situaciones en que, además de que el Estado crea restricciones, la sociedad tampoco tolera las opiniones o formas de expresión poco convencionales.

13. El lado "oscuro" del cifrado y el anonimato emana del hecho de que las infracciones del mundo real también tienen lugar en el mundo virtual. Los agentes del orden y de lucha contra el terrorismo expresan su preocupación por el hecho de que terroristas y delincuentes comunes utilicen el cifrado y el anonimato para esconder sus actividades, dificultando así a los gobiernos la prevención y la realización de investigaciones del terrorismo, el tráfico ilícito de drogas, el crimen organizado y la utilización de niños en la pornografía, entre otros objetivos públicos. Los autores de actos de acoso y ciberacoso pueden utilizar el anonimato para esconderse cobardemente con fines de discriminación, en especial hacia miembros de grupos vulnerables. Sin embargo, al mismo tiempo las fuerzas del orden utilizan con frecuencia las mismas herramientas para garantizar su propia seguridad operacional en las operaciones encubiertas, mientras que los miembros de los grupos vulnerables pueden utilizar esas herramientas para proteger su vida privada frente al acoso. Además, los gobiernos tienen a su disposición un amplio conjunto de herramientas alternativas, como las escuchas telefónicas, la geolocalización y el seguimiento, el manejo de datos, la vigilancia tradicional y muchos otros medios, que refuerzan la labor contemporánea de aplicación de la ley y de lucha contra el terrorismo[5].

III. Cifrado, anonimato y derechos a la libertad de opinión y de expresión y a la vida privada

14. El marco jurídico de derechos humanos relativo al cifrado y el anonimato exige, en primer lugar, que se evalúe el alcance de los derechos correspondientes y su aplicación al cifrado y el anonimato; y, en segundo lugar, que se estime si pueden imponerse legalmente restricciones, y de ser así hasta qué punto, al uso de las tecnologías que promueven y protegen los derechos a la vida privada y a la libertad de opinión y de expresión.

[4] Véase OCDE, *Guidelines for Cryptography Policy* (1997).

[5] Véase Center for Democracy and Technology, "'Going Dark' versus a 'Golden Age for Surveillance'" (2011).

15. Los derechos a la vida privada[6] y la libertad de opinión y de expresión[7] han sido codificados en instrumentos universales y regionales de derechos humanos, interpretados por los órganos de tratados y tribunales regionales, y evaluados por los procedimientos especiales del Consejo de Derechos Humanos y durante el examen periódico universal. Las normas universales relativas a la vida privada, la opinión y la expresión se encuentran en el Pacto Internacional de Derechos Civiles y Políticos, en que 168 Estados son parte. Incluso para los otros Estados que no están vinculados por este instrumento, el Pacto presenta como mínimo un nivel que debe alcanzarse y a menudo refleja una norma del derecho consuetudinario; los países que han firmado pero no han ratificado el Pacto deben respetar su objeto y fin en virtud del artículo 18 de la Convención de Viena sobre el Derecho de los Tratados. Los sistemas jurídicos nacionales también protegen la vida privada, la opinión y la expresión, en ocasiones mediante el derecho constitucional o básico o con interpretaciones de este. Varios proyectos mundiales de la sociedad civil también han ofrecido muestras convincentes de la ley que debe aplicarse en el contexto de la era digital, como los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones y los Principios Mundiales sobre la Seguridad Nacional y el Derecho a la Información. Si bien las normas específicas pueden variar de un derecho a otro, o de un instrumento a otro, un rasgo común en el derecho es que, debido a que los derechos a la vida privada y a la libertad de expresión son tan fundamentales para la dignidad humana y la gobernanza democrática, las restricciones deben delimitarse de cerca, establecerse en la ley y aplicarse estrictamente y solo en circunstancias excepcionales. En la era digital, proteger esos derechos exige una vigilancia excepcional.

A. La vida privada como puerta a la libertad de opinión y de expresión

16. El cifrado y el anonimato brindan a los individuos y a los grupos una zona de vida privada en línea para sostener opiniones y ejercer la libertad de expresión sin injerencia o ataques arbitrarios o ilegales. El anterior titular del mandato señaló que los derechos a "la intimidad y la libertad de expresión se relacionan entre sí" y concluyó que el cifrado y el anonimato estaban amparados debido a la importancia que pueden tener para garantizar esos derechos (A/HRC/23/40 y Corr.1). Como reflejo del artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos ampara específicamente al individuo contra las "injerencias arbitrarias o ilegales en su vida privada, su familia, su domicilio o su correspondencia" y contra los "ataques ilegales a su honra y reputación", y dispone que "toda persona tiene derecho a la protección de la ley contra esas injerencias o esos ataques". La Asamblea General, el Alto Comisionado de las Naciones Unidas para los Derechos Humanos y los titulares de mandatos de los procedimientos especiales han reconocido que la vida privada es una puerta al disfrute de otros derechos, en especial la libertad de opinión y de expresión (véanse la

[6] El artículo 12 de la Declaración Universal de Derechos Humanos, el artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, el artículo 16 de la Convención sobre los Derechos del Niño, el artículo 22 de la Convención sobre los Derechos de las Personas con Discapacidad, el artículo 14 de la Convención Internacional sobre la Protección de los Derechos de Todos los Trabajadores Migratorios y de sus Familiares, el artículo 8 del Convenio Europeo de Derechos Humanos y el artículo 11 de la Convención Americana sobre Derechos Humanos protegen el derecho a la vida privada.

[7] El artículo 19 de la Declaración Universal y el Pacto Internacional de Derechos Civiles y Políticos, el artículo 9 de la Carta Africana de Derechos Humanos y de los Pueblos, el artículo 13 de la Convención Americana sobre Derechos Humanos y el artículo 10 del Convenio Europeo de Derechos Humanos protegen la libertad de expresión.

resolución 68/167 de la Asamblea General, el documento A/HRC/13/37 y la resolución 20/8 del Consejo de Derechos Humanos).

17. El cifrado y el anonimato son especialmente útiles al elaborar y compartir opiniones, acciones que a menudo tienen lugar en la correspondencia en línea, como los correos electrónicos, los mensajes de texto y otras interacciones en línea. El cifrado ofrece seguridad para que los individuos puedan "verificar que sus comunicaciones sean recibidas únicamente por los destinatarios a las que están dirigidas, sin injerencias ni modificaciones, y que todas las comunicaciones que reciban estén también libres de injerencias" (véase A/HRC/23/40 y Corr.1, párr. 23). Dado el potencial del análisis de los metadatos para explicitar "el comportamiento, las relaciones sociales, las preferencias privadas y la identidad de una persona" (véase A/HRC/27/37, párr. 19), el anonimato puede ser muy importante para proteger la correspondencia. Además de la correspondencia, los mecanismos internacionales y regionales han interpretado que la vida privada también abarca muchas otras circunstancias[8].

18. Las personas y la sociedad civil pueden ser objeto de injerencias y ataques de actores estatales y no estatales, contra los cuales el cifrado y el anonimato pueden proporcionar protección. En virtud del artículo 17, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos, los Estados tienen la obligación de proteger la vida privada contra las injerencias o ataques ilegales o arbitrarios. Con arreglo a dicha obligación efectiva, los Estados deben garantizar la existencia de leyes nacionales que prohíban las injerencias o ataques ilegales o arbitrarios contra la vida privada, sean cometidos por actores gubernamentales o no gubernamentales. Dicha protección debe incluir el derecho a recurso por una violación[9]. Para que el derecho a recurso sea significativo, se debe avisar a los usuarios de toda vulnerabilidad de su vida privada, por ejemplo el cifrado debilitado o la divulgación obligatoria de sus datos.

B. Derecho a no ser molestado a causa de sus opiniones

19. El artículo primero de la Declaración Universal de Derechos Humanos reconoce que todas las personas están "dotadas de razón y conciencia", un principio que se explicó en detalle en el derecho de los derechos humanos para incluir, entre otras cosas, la protección de la opinión, la expresión, las creencias y el pensamiento. El artículo 19, párrafo 1, del Pacto Internacional de Derechos Civiles y Políticos, que también retoma la Declaración Universal, dispone que "nadie podrá ser molestado a causa de sus opiniones". La opinión y la expresión están estrechamente relacionadas, y las restricciones al derecho a recibir informaciones e ideas pueden afectar la capacidad de sostener una opinión, y la injerencia en las opiniones necesariamente limita la expresión de estas. Sin embargo, el derecho de los derechos humanos ha establecido una distinción conceptual entre las dos. Durante las negociaciones sobre la redacción del Pacto, "la libertad de forjarse una opinión y elaborarla por medio del razonamiento se consideró absoluta y, a diferencia de la libertad de expresión, no susceptible de ser limitada por ley u otro poder"[10]. La capacidad de sostener una opinión libremente fue

[8] Observación general Nº 16 (1988) del Comité de Derechos Humanos, sobre el derecho al respecto de la vida privada, la familia, el domicilio o la correspondencia, y la protección de la honra y la reputación. Véanse también las fichas temáticas del Tribunal Europeo de Derechos Humanos sobre la protección de los datos (www.echr.coe.int/Documents/FS_Data_ENG.pdf) y el derecho a proteger su imagen (www.echr.coe.int/Documents/FS_Own_image_ENG.pdf).

[9] Véanse la observación general Nº 16 del Comité de Derechos Humanos y su observación general Nº 31, sobre la índole de la obligación jurídica general impuesta a los Estados partes en el Pacto; y el documento CCPR/C/106/D/1803/2008.

[10] Manfred Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993), pág. 441.

vista como un elemento fundamental de la dignidad humana y de la autogobernanza democrática, una garantía tan importante que el Pacto no permitiría injerencia, limitación o restricción alguna. Por consiguiente, las limitaciones permisibles del artículo 19, párrafo 3, se aplican expresamente solo al derecho a la libertad de expresión en el artículo 19, párrafo 2. La injerencia en el derecho a no ser molestado a causa de sus opiniones es, en cambio, una violación en sí misma del artículo 19, párrafo 1.

20. Los comentaristas y los tribunales han prestado mucha menos atención al derecho a no ser molestado a causa de sus opiniones que a la expresión. No obstante, se le debe prestar mayor atención porque los mecanismos de opinión han evolucionado en la era digital y expuesto a las personas a vulnerabilidades significativas. Con frecuencia, las personas conservan sus opiniones en formato digital, al almacenar sus opiniones y su historial de búsqueda y de navegación, por ejemplo, en discos duros, en la nube y en archivos de correo electrónico que las autoridades privadas y públicas con frecuencia retienen por períodos largos o incluso indefinidos. Asimismo, las organizaciones de la sociedad civil preparan y almacenan en formato digital memorandos, ponencias y publicaciones que entrañan forjarse y mantener opiniones. En otras palabras, mantener una opinión en la era digital no es un concepto abstracto que se limita a lo que pueda estar en nuestra mente. Con todo, hoy las opiniones en el espacio digital son objeto de ataques. En el mundo real, la injerencia en el derecho a no ser molestado a causa de sus opiniones puede suponer acoso físico, detención o medidas más leves para castigar a las personas a causa de su opinión (véase CCPR/C/78/D/878/1999, anexo, párrs. 2.5, 7.2 y 7.3). La injerencia también puede incluir medidas como la vigilancia específica, ataques distribuidos de denegación del servicio e intimidación, penalización y acoso en el mundo virtual o real. Con la injerencia digital específica se acosa a particulares y a organizaciones de la sociedad civil a causa de sus opiniones en múltiples formatos. El cifrado y el anonimato permiten a los usuarios impedir o mitigar este tipo de acoso.

21. El derecho a no ser molestado a causa de sus opiniones también abarca el derecho a forjarse opiniones. Los sistemas de vigilancia, tanto específicos como masivos, pueden vulnerar el derecho de las personas a forjarse opiniones, porque el temor a que su actividad en línea, como las búsquedas y las páginas visitadas, se divulgue sin su consentimiento probablemente puede disuadirlas de acceder a información, en especial si la vigilancia produce resultados represivos. Por todas estas razones, las restricciones relativas al cifrado y el anonimato deben evaluarse para determinar si constituyen una injerencia que no es permisible en el derecho a no ser molestado a causa de sus opiniones.

C. Derecho a la libertad de expresión

22. El derecho a la libertad de expresión previsto en el artículo 19, párrafo 2, del Pacto Internacional de Derechos Civiles y Políticos extiende la garantía de la Declaración Universal, que ya es amplia, al amparar la “libertad de buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras, ya sea oralmente, por escrito o en forma impresa o artística, o por cualquier otro procedimiento de su elección”. Un conjunto significativo de jurisprudencia, informes de los procedimientos especiales y resoluciones del sistema de las Naciones Unidas y de los sistemas regionales de derechos humanos destacan que la libertad de expresión “es esencial para el disfrute de otros derechos humanos y libertades y constituye un pilar fundamental para la construcción de una sociedad democrática y el fortalecimiento de la democracia” (resolución 25/2 del Consejo de Derechos Humanos). El Consejo de Derechos Humanos, la Asamblea General y los Estados a título individual a menudo afirman que las personas gozan de los mismos derechos en

el mundo virtual que en el mundo real[11]. En el presente informe no se repetirán todos los elementos de ese consenso. En el contexto del cifrado y el anonimato, tres aspectos del texto merecen especial atención (véanse los párrs. 23 a 26 *infra*).

23. **Libertad de buscar, recibir y difundir informaciones e ideas:** en entornos de censura imperante, las personas pueden verse obligadas a servirse del cifrado y el anonimato para eludir restricciones y ejercer el derecho a buscar, recibir y difundir informaciones. Algunos Estados han restringido el acceso con diversas herramientas. Por ejemplo, la censura estatal a veces plantea obstáculos insuperables al derecho de acceso a la información. Algunos Estados imponen restricciones basadas en el contenido, a menudo discriminatorias, o penalizan la expresión en línea, intimidan a la oposición y disidencia política y aplican leyes de difamación y lesa majestad para acallar a los periodistas, defensores y activistas. Una conexión VPN, o el uso de Tor o de un servidor proxy, combinado con el cifrado, es tal vez la única manera en que el individuo puede acceder a información o compartirla en esos entornos.

24. Cabe poner de relieve que el derecho de los derechos humanos también ampara el derecho a buscar, recibir y difundir informaciones e ideas científicas. La Declaración Universal y el Pacto Internacional de Derechos Económicos, Sociales y Culturales amparan los derechos a la educación y "a participar en el progreso científico y en los beneficios que de él resulten". Las tecnologías de cifrado y anonimato permiten a las personas beneficiarse de dicha información en situaciones en que, sin ellas, se les impediría hacerlo, y son por sí mismas ejemplos de progreso científico. Su uso faculta a las personas para acceder a los beneficios del progreso científico, acceso que podría estar limitado por el Gobierno. La Relatora Especial sobre los derechos culturales señala que "los derechos a la ciencia y a la cultura deben entenderse como inclusivos del derecho a tener acceso a las tecnologías de la información y las comunicaciones y a otras tecnologías y a usarlas en formas autodeterminadas y empoderantes" (véase A/HRC/20/26, párr. 19).

25. **Sin consideración de fronteras:** los principales instrumentos que garantizan la libertad de expresión reconocen explícitamente el alcance transfronterizo del derecho. Las personas gozan del derecho a recibir y transmitir información e ideas de toda índole más allá de sus fronteras[12]. Sin embargo, algunos Estados filtran o bloquean los datos basándose en palabras clave, y deniegan el acceso utilizando tecnologías relacionadas con el acceso al texto. El cifrado permite al usuario evitar dicha filtración, para que la información fluya a través de las fronteras. Además, las personas no controlan, y por lo general desconocen, la manera en que sus comunicaciones cruzan las fronteras. El cifrado y el anonimato pueden proteger la información de todos los individuos cuando transita por servidores situados en terceros países que filtran el contenido.

26. **Por cualquier procedimiento:** los artículos 19 de la Declaración Universal y el Pacto Internacional de Derechos Civiles y Políticos se redactaron con un espíritu previsor para dar cabida a futuros adelantos tecnológicos (A/HRC/17/27). Los Estados partes en el Pacto eligieron adoptar la expresión general "por cualquier otro procedimiento" en lugar de una enumeración de los medios existentes en ese momento. En parte por esta razón, los mecanismos internacionales han reconocido reiteradamente que las protecciones de la libertad de expresión también se aplican a

[11] Véanse, por ejemplo, la resolución 68/167 de la Asamblea General, la resolución 26/13 del Consejo de Derechos Humanos y la recomendación CM/Rec (2014) 6 del Comité de Ministros del Consejo de Europa a los Estados miembros sobre una guía de derechos humanos para los usuarios de Internet.

[12] El Tribunal Europeo de Derechos Humanos ha reconocido este punto. Véase *Ahmet Yildirim v. Turkey* (2012); *Cox v. Turkey* (2010); *Case of Groppera Radio AG and Others v. Switzerland* (1990).

las actividades en Internet. Los tribunales regionales también han reconocido que las protecciones se aplican en línea[13]. El Tribunal Europeo de Derechos Humanos, en relación con la protección correspondiente de la expresión otorgada por el Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales, ha señalado que las formas y medios con los que se transmite y recibe información están protegidos en sí mismos, porque cualquier restricción impuesta a los medios afecta necesariamente el derecho a recibir y difundir información[14]. En este sentido, las tecnologías de cifrado y anonimato son medios concretos mediante los cuales las personas ejercen su libertad de expresión.

D. Importancia de las empresas

27. Las empresas de diversos sectores pueden promover u obstaculizar la vida privada, la opinión y la expresión, también en relación con el cifrado y el anonimato. Gran parte de la comunicación en línea (o prácticamente toda en algunos los países) se realiza en redes que pertenecen a empresas privadas y son administradas por ellas, y otras empresas poseen y administran sitios web con contenido esencialmente generado por los usuarios. Otras son actores activos de los mercados de la vigilancia y de los programas espías, y proporcionan *hardware* y *software* a los gobiernos para debilitar la seguridad de los usuarios en línea. Otras desarrollan o prestan servicios para el almacenamiento seguro y privado en línea. Las entidades de telecomunicación, los proveedores de acceso a Internet, los buscadores, los servicios en la nube y muchos otros actores empresariales, con frecuencia descritos como intermediarios, promueven, regulan o debilitan la vida privada y la expresión en línea. Los intermediarios pueden almacenar cuantiosos volúmenes de datos de los usuarios, a los que los gobiernos a veces piden acceso. El cifrado y el anonimato pueden ser promovidos o debilitados por cada uno de estos actores empresariales.

28. Un estudio completo del papel que desempeñan las empresas en la protección de la seguridad de sus usuarios en la red no entra dentro del ámbito del presente informe, que se centra en las obligaciones de los Estados. Sin embargo, sigue siendo importante recalcar que "la responsabilidad de respetar los derechos humanos se aplica a todas las operaciones de la empresa en todo el mundo, independientemente de la ubicación de sus usuarios, y existe independientemente de si el Estado cumple con sus obligaciones de derechos humanos" (véase A/HRC/27/37, párr. 43). Como mínimo, las empresas deberían aplicar los principios establecidos en los Principios Rectores sobre las Empresas y los Derechos Humanos, los Principios de Libertad de Expresión y Privacidad de la Global Network Initiative, la Guía del Sector de Tecnologías de la Información y la Comunicación de la Comisión Europea para Implementar los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos, y los Principios Rectores del Diálogo de la Industria de las Telecomunicaciones, que alientan a las empresas a que se adhieran a la protección de los derechos humanos, obren con la diligencia debida para garantizar el efecto positivo de su labor en los derechos humanos y remedien los efectos negativos de su labor en los derechos humanos. En el futuro, el Relator Especial se centrará en el papel que

[13] Comisión Europea de Derechos Humanos, *Neij and Sunde Kolmisoppi v. Sweden* (2013); Tribunal Europeo de Derechos Humanos, *Perrin v. United Kingdom* (2005); Corte Africana de Derechos Humanos y de los Pueblos, *Zimbabwe Lawyers for Human Rights and Institute for Human Rights and Development (on behalf of Meldrum) v. Zimbabwe* (2009); *Caso Herrera Ulloa vs. Costa Rica*, *Herrera Ulloa vs. Costa Rica*, Excepciones Preliminares, Fondo, Reparaciones y Costas, Serie C Nº 107, IHRL 1490 (IACHR 2004).

[14] Véase *Autronic AG v. Switzerland* (1990); *De Haes and Gijsels v. Belgium* (1997), párr. 48; *News Verlags GmbH and Co.KG v. Austria* (2000).

deberían desempeñar las empresas en la preservación de la seguridad individual para ejercer la libertad de opinión y de expresión.

IV. Evaluación de las restricciones al cifrado y el anonimato

A. Marco legal

29. Las limitaciones permisibles al derecho a la vida privada deberían considerarse de forma estricta, en particular en una era en la que la vigilancia en línea está generalizada —ya sea pasiva o activa, general o específica—, independientemente de si las normas aplicables son "arbitrarias o ilegales" en virtud del artículo 17 del Pacto Internacional de Derechos Civiles y Políticos, "arbitrarias" con arreglo al artículo 12 de la Declaración Universal de Derechos Humanos, "arbitrarias o abusivas" de conformidad con el artículo 11 de la Convención Americana sobre Derechos Humanos, o de que "constituya una medida que, en una sociedad democrática, sea necesaria" en virtud del artículo 8 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales (véase A/HRC/13/37, párrs. 14 a 19). Las injerencias en la vida privada que limiten el ejercicio de la libertad de opinión y de expresión, como las que se describen en el presente informe, no deben en ningún caso interferir con el derecho a tener opiniones, y aquellas que limiten la libertad de expresión deben estar fijadas por la ley y ser necesarias y proporcionales para lograr uno de los objetivos que figuran en un grupo reducido de objetivos legítimos.

30. No se puede imponer restricción alguna al derecho de toda persona a no ser molestada a causa de sus opiniones; las restricciones en virtud del artículo 19, párrafo 3, del Pacto únicamente se aplican al derecho a la libertad de expresión enunciado en el artículo 19, párrafo 2. Cuando en ciertos entornos la opinión de una persona, expresada en un medio digital, da lugar a vigilancia o acoso, el cifrado y el anonimato pueden proporcionar la privacidad necesaria. Las restricciones a dichas herramientas de seguridad pueden interferir en la capacidad de las personas a mantener opiniones.

31. Las restricciones al cifrado y el anonimato, como elementos facilitadores del derecho a la libertad de expresión, deben cumplir tres requisitos bien conocidos: cualquier limitación a la libertad de expresión debe estar fijada por la ley; únicamente puede imponerse por razones legítimas (descritas en el artículo 19, párrafo 3, del Pacto); y debe ajustarse a estrictos criterios de necesidad y proporcionalidad.

32. En primer lugar, para que una restricción al cifrado o el anonimato esté "fijada por la ley", debe ser precisa, pública y transparente, y evitar acordar a las autoridades estatales una discrecionalidad sin trabas para aplicar la limitación (véase Comité de Derechos Humanos, observación general Nº 34 (2011)). Las propuestas de imponer restricciones al cifrado o el anonimato deberían estar sujetas a las observaciones de la opinión pública y únicamente deberían adoptarse, de hacerlo, de conformidad con el proceso legislativo ordinario. También deberían aplicarse estrictas salvaguardias judiciales y procesales para garantizar el derecho a un proceso con las debidas garantías a toda persona cuyo uso del cifrado o el anonimato sea objeto de restricción. En particular, una corte, un tribunal u otro órgano jurisdiccional independiente debe supervisar la aplicación de la restricción[15].

[15] Véanse el Pacto Internacional de Derechos Civiles y Políticos, artículo 2, párrafo 3 b); CCPR/C/79/Add.110, párr. 22; y los Principios de Johannesburgo sobre Seguridad Nacional, Libertad de Expresión y Acceso a la Información.

33. En segundo lugar, las limitaciones solo pueden justificarse para proteger intereses específicos: los derechos o la reputación de los demás; la seguridad nacional; el orden público; la salud o la moral públicas. Incluso cuando un Estado prohíba por ley la "apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia", de conformidad con el artículo 20 del Pacto, toda restricción a la libertad de expresión debe ajustarse a lo dispuesto en el artículo 19, párrafo 3 (A/67/357). No pueden invocarse otros motivos para justificar restricciones a la libertad de expresión. Además, como a menudo se citan objetivos legítimos como pretexto para fines ilícitos, las propias restricciones deben aplicarse de forma restrictiva[16].

34. En tercer lugar, el Estado debe mostrar que toda restricción al cifrado o el anonimato es "necesaria" para alcanzar el objetivo legítimo[17]. El Tribunal Europeo de Derechos Humanos ha concluido debidamente que el término "necesarias" que figura en el artículo 10 del Convenio Europeo para la Protección de los Derechos Humanos y de las Libertades Fundamentales significa que la restricción debe ser algo más que "útil", "razonable" o "deseable"[18]. Una vez que se haya logrado el objetivo legítimo, se debe dejar de aplicar la restricción. Habida cuenta de los derechos fundamentales en cuestión, las limitaciones deberían estar sujetas a una autoridad judicial independiente e imparcial, en particular para preservar el derecho de las personas a las debidas garantías procesales.

35. El criterio de necesidad también implica una evaluación de la proporcionalidad de las medidas que limitan el uso de la seguridad en línea y el acceso a esta[19]. Una evaluación de la proporcionalidad debe asegurar que la restricción sea "el instrumento menos perturbador de los que permitan conseguir el resultado deseado"[20]. La limitación debe tener por finalidad un objetivo específico y no interferir de forma indebida en otros derechos de las personas a las que se aplica la limitación, y la injerencia en los derechos de terceras personas debe limitarse y justificarse a la luz del interés específico que se desea lograr mediante dicha injerencia. La restricción también debe "guardar proporción con el interés que debe protegerse"[21]. Un alto riesgo de perjuicio a un interés crítico y legítimo del Estado puede justificar injerencias limitadas en la libertad de expresión. Por el contrario, cuando una restricción tiene un amplio impacto en personas que no presentan amenaza alguna para un interés legítimo del gobierno, la carga que pesa sobre el Estado para justificar la restricción será muy alta[22]. Además, un análisis de la proporcionalidad debe tener en cuenta que es muy probable que las injerencias en el cifrado y el anonimato sean utilizadas por las mismas redes criminales y terroristas a las que dichas limitaciones pretenden disuadir. En cualquier caso, es esencial que los Estados "justifiquen con claridad y pruebas" cualquier injerencia para permitir un debate público transparente sobre las restricciones que implican y posiblemente menoscaban la libertad de expresión (véase A/69/397, párr. 12).

---

16 Véase Comité de Derechos Humanos, observación general Nº 34 sobre la libertad de opinión y de expresión, párr. 30, y observación general Nº 31.

17 Véase Comité de Derechos Humanos, observación general Nº 34, párr. 2, y comunicación Nº 2156/2012, dictamen aprobado el 10 de octubre de 2014.

18 Véase *Case of The Sunday Times v. United Kingdom*, fallo de 26 de abril de 1979, párr. 59.

19 Véase Corte Africana de Derechos Humanos y de los Pueblos, *Lohe Issa Konate v. Burkina Faso*, demanda Nº 004/2013, párrs. 148 y 149 (2014); Tribunal Europeo de Derechos Humanos, *Case of The Sunday Times*, párr. 62.

20 Véase Comité de Derechos Humanos, observación general Nº 27 (1999) sobre la libertad de circulación, párr. 14.

21 Véase *ibid*., párr. 14.

22 Véase Comisión Interamericana de Derechos Humanos, OEA/Serv.L/V/II.149, párr. 134.

B. Práctica estatal: ejemplos y preocupaciones

36. Las tendencias relativas a la seguridad y la privacidad en línea son motivo de gran preocupación. Los Estados a menudo no proporcionan una justificación pública que avale las restricciones. Las comunicaciones cifradas y anónimas pueden frustrar a los agentes del orden y los funcionarios encargados de la lucha contra el terrorismo, y dificultan la vigilancia, pero las autoridades estatales por lo general no han dado ejemplos de situaciones —ni siquiera en términos generales, debido a la posible necesidad de confidencialidad— en las que una restricción haya sido necesaria para lograr un objetivo legítimo. Los Estados restan importancia al valor de las herramientas tradicionales no digitales en las actividades encaminadas a hacer cumplir la ley y luchar contra el terrorismo, incluida la cooperación transnacional[23]. En consecuencia, los ciudadanos no cuentan con la oportunidad de considerar si las restricciones a su seguridad en línea se justificarían por los beneficios reales en los ámbitos de la seguridad nacional y la prevención de los delitos. Las actividades destinadas a restringir el cifrado y el anonimato también tienden a ser reacciones rápidas al terrorismo, aunque los autores de estos delitos no hayan utilizado aparentemente el cifrado ni el anonimato para planear o llevar a cabo un atentado. Además, incluso cuando quepa afirmar que la restricción tiene por objeto lograr un interés legítimo, muchas leyes y políticas no cumplen habitualmente los criterios de necesidad y proporcionalidad y tienen efectos amplios y nocivos sobre la capacidad de todas las personas de ejercer libremente su derecho a la intimidad y a libertad de opinión y expresión.

37. También cabe señalar que las propias Naciones Unidas no han proporcionado herramientas de comunicación seguras a su personal ni a las personas que visitan los sitios web de las Naciones Unidas, lo que dificulta que las personas objeto de amenazas puedan ponerse en contacto por vía electrónica de manera segura con los mecanismos de derechos humanos de las Naciones Unidas[24].

1. Cifrado

38. Algunos gobiernos tratan de proteger o promover el cifrado para velar por la privacidad de las comunicaciones. Por ejemplo[25], el Marco Civil de Internet del Brasil, adoptado en 2014, garantiza la inviolabilidad y la confidencialidad de las comunicaciones electrónicas de los usuarios, y únicamente contempla excepciones en casos en los que se haya dictado una orden judicial. La Ley de Comercio Electrónico y la Ley de Telecomunicaciones de Austria no restringen el cifrado, y el Gobierno ha llevado a cabo campañas de sensibilización para educar al público acerca de la seguridad digital. La legislación y los reglamentos de Grecia promueven el uso eficaz tanto de las herramientas de cifrado como de anonimato. Alemania, Irlanda y Noruega permiten y promocionan el uso de tecnologías de cifrado y se oponen a cualquier intento de debilitar los protocolos de cifrado. De forma análoga, la legislación de Suecia y Eslovaquia no restringen el uso del cifrado en línea. Los Estados Unidos de América alientan el uso del cifrado, y el Congreso de los Estados Unidos estudiará con mayor detenimiento el proyecto de ley relativo a la seguridad de datos, que prohibiría al Gobierno obligar a las empresas a que rebajen la seguridad de sus productos o introduzcan puertas traseras en sus sistemas. Varios gobiernos, como los del Canadá,

[23] Pero véase Centre for International Governance Innovation y Chatham House, *Toward a Social Compact for Digital Privacy and Security: Statement by the Global Commission on Internet Governance* (2015).

[24] Por ejemplo, el personal de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (ACNUDH) en Ginebra no tiene acceso a sistemas de cifrado de correos electrónicos de extremo a extremo, y el sitio web del ACNUDH no está cifrado.

[25] Muchos ejemplos de este párrafo se han extraído de comunicaciones de los gobiernos pertinentes.

los Estados Unidos de América, los Países Bajos, el Reino Unido de Gran Bretaña e Irlanda del Norte y Suecia, financian actividades encaminadas a compartir conocimientos o impartir información acerca del uso de las tecnologías de cifrado y anonimato a fin de ayudar a los usuarios a eludir la censura y proteger su seguridad en línea. Además, los reglamentos de exportación deberían facilitar la transferencia de las tecnologías de cifrado en la medida de lo posible. Aunque el presente informe no proporciona una evaluación global en materia legal de todos los enfoques nacionales relativos al cifrado, estos elementos mencionados —no restricción o protección integral, el requisito de que se haya dictado una orden judicial para una limitación específica, y la educación pública— requieren de una aplicación más amplia como medio para proteger y promover los derechos de libertad de opinión y de expresión.

39. No obstante, la reglamentación sobre cifrado con frecuencia no se ajusta a las normas relativas a la libertad de expresión respecto de dos elementos fundamentales. En primer lugar, por regla general no se ha mostrado que las restricciones fueran necesarias para lograr un interés legítimo particular. Esto sucede especialmente debido a la profundidad y amplitud de otras herramientas, como los servicios de inteligencia y los métodos policiales tradicionales y la cooperación transnacional, que probablemente ya facilitan información sustancial para lograr objetivos específicos en materia de cumplimiento de la ley o para otros fines legítimos. En segundo lugar, tienen un efecto desproporcionado sobre la libertad de opinión y de expresión de que disfrutan las personas objeto de la restricción o el público en general.

Prohibición del cifrado para el uso particular

40. La prohibición total del uso de tecnologías de cifrado a título particular restringe de manera desproporcionada la libertad de expresión, porque priva a todos los usuarios de la red en una jurisdicción determinada del derecho a establecer un espacio privado para opinar y expresarse, sin que exista ninguna alegación particular de que el uso del cifrado tenga fines ilícitos.

41. La regulación estatal del cifrado puede equivaler a una prohibición, como las normas que: a) exigen licencias para usar tecnologías de cifrado; b) establecen estándares técnicos deficientes de cifrado; y c) controlan la importación y exportación de las herramientas de cifrado. Al limitar las herramientas de cifrado a los criterios establecidos por el gobierno y controlar la importación o exportación de las tecnologías de cifrado, los Estados se aseguran de que los programas de cifrado continúen adoleciendo de los puntos débiles que permiten a los gobiernos acceder al contenido de las comunicaciones. Por ejemplo, aunque la legislación puede estar en evolución, la India ha dispuesto que los proveedores de servicios no pueden hacer uso del "cifrado masivo" en sus redes; la legislación también ha restringido el uso del cifrado para particulares a una clave de 40 bits —que se puede descifrar fácilmente—, a menos que se haya obtenido una autorización previa, y dispone que cualquiera que utilice un cifrado más seguro debe proporcionar al Gobierno una copia de sus claves de cifrado[26]. La información recibida indica que es probable que los productos de cifrado en China deban ajustarse a los algoritmos de cifrado aprobados por el Gobierno y que no han sido sometidos a una revisión por pares para evaluar su seguridad[27]. La Autoridad de Telecomunicaciones del Pakistán exige una autorización previa para utilizar VPN y herramientas de cifrado[28]. Cuba requiere que las personas

[26] Gobierno de la India, Ministerio de Comunicaciones y Tecnologías de la Información, "Licence Agreement for Provision of Internet Services" (2007). Disponible en http://dot.gov.in/sites/default/files/internet-licence-dated%2016-10-2007_0.pdf. Véase en particular la sección 2.2, apartado vii).

[27] Véase, por ejemplo, la Ley de Lucha contra el Terrorismo, art. 15 (borrador inicial de 8 de noviembre de 2014). Disponible en http://chinalawtranslate.com/en/ctldraft/.

[28] Véase www.ispak.pk/Downloads/PTA_VPN_Policy.pdf.

que hagan uso del cifrado obtengan una autorización reglamentaria[29]. En Etiopía, el Gobierno está facultado para establecer estándares técnicos para el cifrado y recientemente promulgó un reglamento que penaliza la manufactura, el ensamblaje o la importación de cualquier equipo de telecomunicaciones sin obtener un permiso[30]. Dichas reglamentaciones interfieren de forma inadmisible en el uso particular del cifrado en las comunicaciones.

Debilitamiento intencionado del cifrado

42. Algunos Estados han aplicado o han propuesto aplicar el denominado "acceso de puerta trasera" en los productos disponibles en el mercado, obligando a los desarrolladores a instalar puntos débiles que permitan a las autoridades gubernamentales acceder a las comunicaciones cifradas. Algunos gobiernos han desarrollado o adquirido herramientas que permiten dicho acceso con fines de vigilancia interna[31]. Autoridades del Reino Unido y los Estados Unidos parecen abogar por que se exija un acceso de puerta trasera[32]. Los Estados que respaldan dichas medidas a menudo argumentan que es necesario un marco legal que regule el acceso de puerta trasera para interceptar el contenido de las comunicaciones cifradas. Sin embargo, los gobiernos que proponen el acceso de puerta trasera no han demostrado que el uso del cifrado por delincuentes o terroristas constituya una barrera insuperable para los objetivos relacionados con el cumplimiento de la ley. Además, en base a la tecnología existente, las deficiencias intencionadas menoscaban de forma invariable la seguridad para todos los usuarios de la red, ya que una puerta trasera, aunque haya sido concebida únicamente para permitir el acceso al gobierno, puede ser utilizada por otras entidades no autorizadas, incluidos otros actores estatales o no estatales. Dado su efecto generalizado e indiscriminado, el acceso de puerta trasera afectaría, de forma desproporcionada, a todos los usuarios de la red.

43. El debate acerca de esta cuestión pone de relieve un punto crítico: exigir que el cifrado cuente con un acceso de puerta trasera, incluso si responde a fines legítimos, amenaza la privacidad necesaria para el ejercicio sin trabas del derecho a la libertad de expresión. El acceso de puerta trasera tiene limitaciones prácticas; la explotación de los puntos débiles intencionados podría hacer que el contenido cifrado fuera susceptible a un ataque, incluso si únicamente se tiene la intención de permitir el acceso al gobierno o al control judicial. No cabe duda de que los gobiernos se enfrentan a un dilema cuando su obligación de proteger la libertad de expresión entra en conflicto con su obligación de prevenir las violaciones del derecho a la vida o a la integridad física, que se ven amenazados por el terrorismo y otras conductas delictivas. No obstante, los Estados disponen de otros recursos para solicitar la divulgación de información cifrada, como, por ejemplo, mediante órdenes judiciales. En dichas situaciones, los Estados deben demostrar que las limitaciones generales a la seguridad proporcionada por el cifrado serían necesarias y proporcionales. Los Estados deben mostrar, de forma pública y transparente, que no hay disponibles otros medios menos intrusivos, o bien que estos no han logrado los objetivos deseados, y que solamente medidas intrusivas amplias, como puertas traseras, podrían lograr el objetivo legítimo. Con todo, las medidas que imponen restricciones de aplicación

[29] Comunicación de Cuba.

[30] Véase la Ley Nº 761/2012 de Etiopía sobre los delitos de fraude en las telecomunicaciones, arts. 3 a 10.

[31] Véase Morgan Maquis-Boire y otros, *For Your Eyes Only* (2013, Citizen Lab).

[32] Véase el discurso pronunciado por el Primer Ministro David Cameron el 12 de enero de 2015 en la conferencia de promesas del Partido Conservador para las elecciones generales de 2015 y el discurso pronunciado por James Comey, Director del Buró Federal de Investigaciones, el 16 de octubre de 2014, titulado "Going dark: are technology, privacy and public safety on a collision course?", en la Brookings Institution, Washington D.C.

general a un gran número de personas, sin efectuar una evaluación caso por caso, con toda probabilidad no cumplirían el criterio de proporcionalidad.

Depósitos de claves

44. Un sistema de depósito de claves permite el acceso individualizado al cifrado, pero requiere que los usuarios almacenen sus claves privadas con el gobierno o "un tercero de confianza". Los depósitos de claves, sin embargo, tienen vulnerabilidades considerables. Por ejemplo, el sistema de depósito de claves depende de la integridad de la persona, departamento o sistema encargado de salvaguardar las claves privadas, y la propia base de datos con las claves podría ser vulnerable a un ataque, lo que socavaría la seguridad y privacidad de las comunicaciones de cualquier usuario. Los sistemas de depósitos de claves, rechazados (junto con el acceso de puerta trasera) tras un extenso debate en los Estados Unidos durante las denominadas "criptoguerras" del decenio de 1990, están vigentes en la actualidad en varios países y se ha propuesto su implantación en otros. En 2011, Turquía aprobó reglamentos que exigían a los proveedores de servicios de cifrado que proporcionaran copias de las claves de cifrado a los reguladores gubernamentales antes de ofrecer sus herramientas de cifrado a los usuarios[33]. Las vulnerabilidades inherentes a los depósitos de claves los convierten en una grave amenaza a la seguridad para ejercer la libertad de expresión.

Divulgación obligatoria de claves en contraposición al descifrado específico por orden judicial

45. En una situación en la que los argumentos de las fuerzas del orden o seguridad nacional pueden justificar que se solicite el acceso a las comunicaciones, las autoridades pueden considerar dos opciones: ordenar el descifrado de comunicaciones específicas o, debido a la falta de confianza de que la parte en cuestión cumpla con una orden de descifrado, la divulgación de la clave necesaria para el descifrado. Las órdenes para efectuar descifrados específicos pueden parecer más limitadas y menos probables de plantear cuestiones de proporcionalidad en comparación con la divulgación de claves, ya que se centran en comunicaciones específicas en lugar de un conjunto completo de comunicaciones de una persona cifradas por una clave en particular. La divulgación de claves, en cambio, podría exponer datos privados que sobrepasan lo estrictamente necesario por las exigencias de una situación[34]. Además, la divulgación de claves o las órdenes para efectuar descifrados con frecuencia obligan a las empresas a cooperar con los gobiernos, lo que genera notables desafíos en relación con los usuarios particulares de la red. La divulgación de claves existe por ley en una serie de países europeos[35]. En ambos casos, sin embargo, dichas órdenes deberían dictarse sobre la base de una ley a la que el público tenga acceso, con un ámbito de aplicación claramente delimitado y que se centre en personas concretas, implementada en virtud de una autoridad judicial imparcial e independiente, en particular para preservar el derecho de las personas a las debidas garantías procesales, y únicamente deberían adoptarse cuando sea necesario y no haya disponibles otros medios de investigación menos intrusivos. Dichas medidas solo pueden justificarse si tienen por objeto uno o varios usuarios específicos, con sujeción a supervisión judicial.

[33] Ley Nº 5651 relativa a la regulación de la difusión en Internet y la lucha contra los delitos cometidos a través de la difusión en Internet.

[34] El Coordinador de la Lucha contra el Terrorismo de la Comisión Europea ha instado a que se considere la posibilidad de implantar la divulgación obligatoria de claves. Véase Consejo de la Unión Europea, Secretaría General, documento de sesión D1035/15 (2015).

[35] Véase, por ejemplo, Reino Unido, Ley de Regulación de las Atribuciones de Investigación (divulgación obligatoria de claves); Francia, Ley Nº 2001-1062 (divulgación de claves de cifrado mediante autorización judicial); España, Ley General de Telecomunicaciones, Ley Nº 25/2007 (divulgación de claves).

Presunciones legales

46. Algunos Estados pueden considerar el mero uso de tecnologías de cifrado como una conducta ilícita. Por ejemplo, los cargos presentados contra los blogueros del blog Zone 9, en Etiopía, incluían insinuaciones de que la mera formación en materia de seguridad de las comunicaciones evidenciaba una conducta delictiva[36]. Dichas presunciones no se ajustan a los criterios de restricciones permisibles. De forma análoga, los Estados menoscaban los derechos a la vida privada y a la libertad de expresión cuando penalizan a aquellos que producen y distribuyen herramientas para facilitar a los activistas el acceso a la red.

2. Anonimato

47. Se ha reconocido el importante papel que desempeña el anonimato para salvaguardar y promover la privacidad, la libertad de expresión, la rendición de cuentas política, y la participación y el debate públicos[37]. La Declaración Universal de Derechos Humanos y el Pacto Internacional de Derechos Civiles y Políticos no abordan el anonimato. Durante la negociación del Pacto, se propuso incluir en el artículo 19, párrafo 1, la frase "el anonimato no está permitido". Sin embargo, la propuesta se rechazó, "entre otros motivos, porque el anonimato puede ser necesario en ocasiones para proteger al autor" y "una cláusula de ese tipo podría impedir el uso de seudónimos"[38]. La Relatora Especial sobre la libertad de expresión de la Comisión Interamericana de Derechos Humanos concluyó que "tanto el derecho a la libertad de pensamiento y expresión como el derecho a la vida privada protegen al discurso anónimo frente a las restricciones estatales"[39]. Varios Estados cuentan con una larga tradición de preservación del anonimato en sus culturas políticas, pero muy pocos brindan una protección general en la ley para la expresión anónima. Algunos Estados ejercen una presión significativa contra el anonimato, tanto en el mundo virtual como en el real. Con todo, como el anonimato facilita la opinión y expresión de manera significativa en la red, los Estados deberían protegerlo y no restringir por norma general las tecnologías que lo procuran. Los poderes judiciales de varios Estados han protegido el anonimato, al menos en un número limitado de casos. Por ejemplo, el Tribunal Supremo del Canadá recientemente declaró nula la obtención de datos sobre la identidad de usuarios anónimos de la red sin una orden judicial[40]. El Tribunal Constitucional de la República de Corea derogó leyes contra el anonimato al considerarlas inconstitucionales[41]. La Corte Suprema de los Estados Unidos ha protegido sistemáticamente el derecho de expresión anónima[42]. El Tribunal Europeo de Derechos Humanos ha reconocido que el anonimato es importante para la libertad de expresión, pero contempla limitaciones en los casos en que sea necesario para lograr objetivos legítimos.

48. Muchos Estados reconocen la legalidad de mantener el anonimato de las fuentes de los periodistas. La Suprema Corte de Justicia de México y el Código de Procedimientos Penales para el Estado de México reconocen el derecho de los

---

[36] Véase http://trialtrackerblog.org/2014/07/19/contextual-translation-of-the-charges-of-the-zone9-bloggers/.

[37] Véase, por ejemplo, Comisión Interamericana de Derechos Humanos, OEA/Serv.L/V/II.149, párr. 134; Estados Unidos, *McIntyre* v. *Ohio Elections Commission* (1995); Lord Neuberger, discurso en la Conferencia 5RB sobre Internet, titulado "What's a name? Privacy and Anonymous Speech on the Internet" (2014).

[38] Marc J. Bossuyt, *Guide to the "Travaux Préparatoires" of the International Covenant on Civil and Political Rights* (1987), págs. 379 y 380.

[39] Véase Organización de los Estados Americanos, comunicado de prensa Nº 17/15.

[40] *R.* v. *Spencer* (2014).

[41] Decisión 2010 Hun-Ma 47, 252 (consolidada) anunciada el 28 de agosto de 2012.

[42] *McIntyre* v. *Ohio Elections Commission* (1995), págs. 342 y 343.

periodistas a mantener el anonimato de sus fuentes; sin embargo, los periodistas son objeto de graves presiones[43]. Las Constituciones de la Argentina, el Brasil, el Ecuador y el Paraguay protegen expresamente a las fuentes; Chile, El Salvador, Panamá, el Perú, la República Bolivariana de Venezuela y el Uruguay protegen a las fuentes en la ley[44]. La Constitución de Mozambique protege a las fuentes, mientras que Angola afirma hacerlo por ley[45]. Australia, el Canadá, el Japón y Nueva Zelandia han establecido pruebas de sopesamiento para casos específicos a fin de analizar la protección de la fuente, aunque la presión que sufren los periodistas pueden socavar dicha protección con el paso del tiempo[46]. Los Estados a menudo vulneran el anonimato de las fuentes en la práctica, incluso cuando este está contemplado en la ley.

Prohibición del anonimato

49. La prohibición del anonimato en la red interfiere en el derecho a la libertad de expresión. No obstante, muchos Estados lo prohíben independientemente de cualquier interés gubernamental específico. La Constitución del Brasil (art. 5) prohíbe el discurso anónimo. La Constitución de la República Bolivariana de Venezuela (art. 57) prohíbe de forma similar el anonimato. En 2013, Viet Nam prohibió la utilización de seudónimos y, en consecuencia, las personas con un blog personal se vieron obligadas a publicar su nombre real y dirección[47]. En 2012, la República Islámica del Irán exigió la inscripción en un registro de todas las direcciones IP en funcionamiento en el país y que los usuarios de los cibercafés se registraran utilizando su nombre real antes de utilizar una computadora[48]. La legislación del Ecuador requiere que las personas que realizan comentarios en las páginas web y los propietarios de teléfonos celulares se registren utilizando su nombre real[49].

50. Algunos Estados han aprobado leyes que imponen la obligación de registrarse con el nombre real para poder realizar actividades en línea, una forma de prohibición del anonimato. En la Federación de Rusia, los blogueros que cuenten con más de 3.000 lectores diarios deben inscribirse en el registro de la entidad reguladora de los medios de comunicación e identificarse de forma pública, y, al parecer, los usuarios de los cibercafés deben identificarse para conectarse a las redes públicas inalámbricas[50]. Según la información recibida, China anunció una normativa que exigiría a los

43 Véase el nuevo Código Federal de Procedimientos Penales, art. 244.

44 Véanse Argentina, Constitución, art. 43; Brasil, Constitución, título II, cap. I, art. 5, XIV; Ecuador, Constitución, art. 20; Paraguay, Constitución, art. 29, apartado 1). Véanse también Chile, Ley Nº 19.733; El Salvador, Código Procesal Penal; Panamá, Ley Nº 67, art. 21; Perú, Código de Procedimientos Penales; Uruguay, Ley Nº 16099; República Bolivariana de Venezuela, Ley de Ejercicio del Periodismo, art. 8, *Gaceta Oficial* Nº 4819.

45 Véase Mozambique, Constitución, art. 48, apartado. 3; Angola, Ley Nº 7/06 de Prensa, art. 20, apartado 1.

46 Australia, Ley de 2007 por la que se modifica la Ley de Pruebas (privilegios de los periodistas); Canadá, Court of Queen's Bench de Alberta, *Wasylyshen* v. *Canadian Broadcasting Corporation* (2005); Japón, Caso Nº 2006 (Kyo) 19; Nueva Zelandia, Ley de Pruebas, art. 68 (2006).

47 Human Rights Watch, "Vietnam: new decree punishes press", 23 de febrero de 2011; Freedom House, "Vietnam: freedom of the press", 2012; Article 19 "Comment on Decree No. 02 of 2011 on Administrative Responsibility for Press and Publication Activities of the Prime Minister of the Socialist Republic of Vietnam" (junio de 2011).

48 República Islámica del Irán, proyecto de ley Nº 106, Autoridad Reguladora de las Comunicaciones.

49 Véase Ecuador, Ley Orgánica de Comunicación (2013).

50 El proyecto de ley Nº 428884-6, por el que se modifica la Ley de Información, Tecnologías de la Información y Protección de la Información y una serie de instrumentos legislativos de la Federación de Rusia acerca de la racionalización del intercambio de información con el uso de las redes de información y telecomunicaciones; Reuters, "Russia Demands Internet Users Show ID to Access Public Wifi", 8 de agosto de 2014.

usuarios de Internet registrarse con su nombre real para acceder a ciertos sitios web y evitaría difundir contenidos contrarios a los intereses nacionales[51]. Sudáfrica también exige que los usuarios de la red y teléfonos móviles se registren utilizando su nombre real[52].

51. Del mismo modo, los gobiernos a menudo requieren el registro de las tarjetas SIM; por ejemplo, casi 50 países de África se encuentran en proceso o ya requieren el registro de datos personales de identificación al activar una tarjeta SIM[53]. Colombia tiene desde 2011 una política de registro obligatorio de teléfonos celulares, y el Perú ha asociado todas las tarjetas SIM a un número de identificación nacional desde 2010[54]. Otros países están considerando la posibilidad de adoptar políticas de este tipo. Estas políticas menoscaban directamente el anonimato, en particular para aquellas personas que acceden a Internet únicamente a través de la tecnología móvil. El registro obligatorio de las tarjetas SIM puede proporcionar a los gobiernos la capacidad de vigilar a personas y periodistas más allá de cualquier interés gubernamental legítimo.

52. Los Estados también han tratado de combatir las herramientas de anonimato, como Tor, los servidores proxy y las VPN, denegando el acceso a estas herramientas. China ha bloqueado el acceso a Tor desde hace tiempo[55] y, según informaciones recibidas, funcionarios del Gobierno de Rusia ofrecieron más de 100.000 dólares de los Estados Unidos por las técnicas que permiten identificar a los usuarios anónimos de Tor[56]. Además, Etiopía[57], la República Islámica del Irán[58] y Kazajstán[59] han intentado, al parecer, bloquear el tráfico de Tor. Dado que dichas herramientas pueden ser los únicos mecanismos de que disponen los usuarios para ejercer su libertad de opinión y de expresión de forma segura, se debería proteger y promover el acceso a las mismas.

Restricciones durante períodos de agitación social

53. El discurso anónimo ha sido necesario para activistas y manifestantes, pero los Estados han tratado de prohibir o interceptar asiduamente las comunicaciones anónimas en épocas de protestas. Dichos intentos de interferir en la libertad de expresión tienen el objetivo ilegítimo de socavar el derecho a la manifestación pacífica, enunciado en la Declaración Universal y el Pacto Internacional de Derechos Civiles y Políticos.

[51] China Copyright and Media, “Internet User Account Name Management Regulations”, artículo 5 (2015).

[52] Sudáfrica, Regulación de la Interceptación de las Comunicaciones y Provisión de Información relacionada con la Comunicación, Ley Nº 70 de 2003; véase también la Ley de Transacciones y Comunicaciones Electrónicas, de 2002 (que requiere el registro con el nombre real a los proveedores de servicios).

[53] Kevin P. Donovan y Aaron K. Martin, “The Rise of African SIM Registration”, 3 de febrero de 2014.

[54] Véase Colombia, Decreto Nº 1630 de 2011; Perú 21, *Los celulares de prepago en la mira*, 27 de mayo de 2010.

[55] MIT Technology Review, *How China Blocks the Tor Anonymity Network*, 4 de abril de 2012.

[56] La oferta original está disponible en http://zakupki.gov.ru/epz/order/notice/zkk44/view/common-info.html?regNumber=0373100088714000008.

[57] Runa Sandvik, “Ethiopia Introduces Deep Packet Inspection”, The Tor Blog (31 de mayo de 2012); véase también Article 19, 12 de enero de 2015.

[58] “Phobos”, “Iran partially blocks encrypted network traffic”, The Tor Blog (10 de febrero de 2012).

[59] “Phobos”, “Kazakhstan upgrades censorship to deep packet inspection”, The Tor Blog (16 de febrero de 2012).

Responsabilidad de los intermediarios

54. Algunos tribunales estatales y regionales han avanzado hacia la imposición de responsabilidades a los proveedores de servicios de Internet y las plataformas de medios digitales para regular los comentarios de usuarios anónimos en la red. El Ecuador, por ejemplo, en su Ley Orgánica de Comunicación, requiere que los intermediarios generen mecanismos para grabar los datos personales, a fin de identificar a las personas que publican comentarios. En *Delfi v. Estonia* (demanda Nº 64569/09), el Tribunal Europeo de Derechos Humanos confirmó una ley de Estonia que impone responsabilidad a las plataformas digitales por los comentarios anónimos difamatorios que se publiquen en sus páginas. Probablemente, esta responsabilidad de los intermediarios resultará en políticas para el registro con nombres reales, lo que menoscaba el anonimato, o en la supresión total de publicaciones en los sitios web que no pueden permitirse implementar procedimientos de control, lo que perjudicaría a los medios independientes y más pequeños. Los Principios de Manila sobre la Responsabilidad de los Intermediarios, adoptados recientemente y enunciados por una coalición de organizaciones de la sociedad civil, brindan a los Estados y los mecanismos regionales e internacionales un conjunto coherente de directrices para proteger la libertad de expresión en la red.

Retención de datos

55. Las políticas amplias de retención obligatoria de datos limitan la capacidad de los usuarios para conservar el anonimato. La capacidad de un Estado para exigir a los proveedores de servicios de telecomunicaciones y de Internet que recopilen y almacenen información sobre las actividades en línea de todos los usuarios ha resultado de forma inevitable en que el Estado tenga la huella digital de todos los usuarios. La capacidad del Estado para recopilar y almacenar datos personales amplía su capacidad para llevar a cabo labores de vigilancia e incrementa la probabilidad de que se robe y difunda la información personal.

V. Conclusiones y recomendaciones

56. **El cifrado y el anonimato, y los conceptos de seguridad subyacentes, proporcionan la privacidad y seguridad necesarias para el ejercicio del derecho a la libertad de opinión y de expresión en la era digital. Dicha seguridad puede ser esencial para el ejercicio de otros derechos, incluidos los derechos económicos, el derecho a la vida privada, a un juicio con las debidas garantías, a la libertad de reunión y de asociación pacíficas, y el derecho a la vida y a la integridad física. Debido a su importancia para los derechos de libertad de opinión y de expresión, las restricciones al cifrado y el anonimato deben limitarse de forma estricta, de conformidad con los principios de legalidad, necesidad, proporcionalidad y legitimidad del objetivo. Por consiguiente, el Relator Especial formula las recomendaciones que figuran a continuación.**

A. Estados

57. **Los Estados deben revisar o establecer, según corresponda, las leyes y reglamentos nacionales que promuevan y protejan el derecho a la vida privada y a la libertad de opinión y de expresión. Respecto del cifrado y el anonimato, los Estados deben adoptar políticas de no restricción o protección integral, únicamente adoptar restricciones en función de cada caso y que cumplan los requisitos de legalidad, necesidad, proporcionalidad y legitimidad del objetivo,**

solicitar órdenes judiciales para toda limitación específica, y promover la seguridad y la privacidad en línea mediante la educación pública.

58. **Los debates sobre cifrado y anonimato se han centrado con demasiada frecuencia solamente en su posible uso con fines delictivos en épocas de terrorismo. Sin embargo, las situaciones de emergencia no eximen a los Estados de la obligación de velar por el respeto del derecho internacional de los derechos humanos. Las propuestas legislativas para la revisión o adopción de restricciones en materia de seguridad personal en línea deberían someterse a debate público y adoptarse mediante un procedimiento legislativo ordinario, público, informado y transparente. Los Estados deben promover la participación efectiva de un amplio espectro de actores y grupos minoritarios de la sociedad civil en dichos debates y procesos, y evitar adoptar legislación en la materia a través de procedimientos legislativos acelerados. El debate general debería destacar la protección que brindan el cifrado y el anonimato, especialmente a los grupos con mayor riesgo de sufrir una injerencia ilícita. Todo debate de ese tipo también debe tener en cuenta que las restricciones están sujetas a criterios estrictos: si interfieren con el derecho a la opinión, no se deben adoptar restricciones. Las restricciones a la privacidad que limitan la libertad de expresión —a los efectos del presente informe, las restricciones al cifrado y el anonimato— deben estar fijadas por la ley y ser necesarias y proporcionales para lograr uno de los objetivos que figuran en un grupo reducido de objetivos legítimos.**

59. **Los Estados deben promover sistemas de cifrado y anonimato fuertes. Las legislaciones nacionales deben reconocer que las personas son libres de proteger la privacidad de sus comunicaciones digitales mediante el uso de tecnologías y herramientas de cifrado que permitan mantener el anonimato en la red. La legislación y las reglamentaciones que protegen a los defensores de los derechos humanos y los periodistas también deben incluir disposiciones que permitan el acceso y respalden el uso de tecnologías para proteger sus comunicaciones.**

60. **Los Estados no deben restringir el cifrado y el anonimato, que facilitan y a menudo contribuyen al ejercicio del derecho a la libertad de opinión y de expresión. Las prohibiciones generalizadas no son necesarias ni proporcionales. Los Estados deben evitar todas las medidas que debiliten la seguridad de la que pueden disfrutar los usuarios de la red, como puertas traseras, estándares de cifrado deficientes y depósitos de llaves. Además, los Estados deben abstenerse de establecer la identificación de los usuarios como condición para acceder a las comunicaciones digitales y a los servicios en línea, y de obligar a los usuarios de teléfonos móviles que registren su tarjeta SIM. Los actores empresariales deberían asimismo considerar sus propias políticas que restringen el cifrado y el anonimato (entre otras cosas, mediante el uso de seudónimos). El descifrado por orden judicial, sujeto a la legislación nacional e internacional, solamente puede ser admisible cuando se base en leyes trasparentes a las que el público tenga acceso, y se aplique a las personas en función de cada caso (es decir, no a un grupo de personas) y esté sujeto a la orden de un juez y a la protección del derecho de las personas a las debidas garantías procesales.**

B. Organizaciones internacionales, sector privado y sociedad civil

61. **Los Estados, las organizaciones internacionales, las empresas y los grupos de la sociedad civil deben promover la seguridad en línea. Habida cuenta de la relevancia de las nuevas tecnologías de la comunicación en la promoción de los derechos humanos y el desarrollo, todas las personas interesadas deben promover sistemáticamente el acceso al cifrado y el anonimato sin discriminación. El**

Relator Especial hace un llamamiento urgente a las entidades del sistema de las Naciones Unidas, en particular aquellas que trabajan en el ámbito de los derechos humanos y la protección humanitaria, para que respalden el uso de herramientas para la seguridad de las comunicaciones a fin de velar por que las personas que interactúan con estas entidades lo hagan de forma segura. Las entidades de las Naciones Unidas deben revisar sus prácticas y herramientas de comunicación e invertir recursos en incrementar la seguridad y confidencialidad para las numerosas partes interesadas que interactúan con la Organización mediante comunicaciones digitales. Los mecanismos de protección de los derechos humanos deben prestar una atención particular cuando soliciten y gestionen la información recibida de la sociedad civil, los testigos y las víctimas de violaciones de los derechos humanos.

62. **Si bien el presente informe no extrae conclusiones sobre la responsabilidad empresarial relativa a la seguridad de las comunicaciones, no cabe duda de que, habida cuenta de las amenazas a la libertad de expresión en línea, los actores empresariales deben examinar la idoneidad de sus prácticas respecto de las normas de derechos humanos. Como mínimo, las empresas deben adherirse a principios como los establecidos en los Principios Rectores sobre las Empresas y los Derechos Humanos, los Principios de Libertad de Expresión y Privacidad de la Global Network Initiative, la Guía del Sector de Tecnologías de la Información y la Comunicación de la Comisión Europea para Implementar los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos, y los Principios Rectores del Diálogo de la Industria de las Telecomunicaciones. Las empresas, al igual que los Estados, deben abstenerse de bloquear o limitar la transmisión de comunicaciones cifradas y permitir la comunicación anónima. Debe prestarse atención a los esfuerzos para ampliar la disponibilidad de enlaces a los centros de datos, respaldar tecnologías seguras para los sitios web y desarrollar un sistema de cifrado predeterminado y generalizado de extremo a extremo. Los actores empresariales que proveen tecnología para socavar el cifrado y el anonimato deben ser especialmente transparentes en cuanto a sus productos y sus clientes.**

63. **Es preciso fomentar el uso de herramientas de cifrado y anonimato, así como una mayor cultura digital. El Relator Especial, reconociendo que el valor de las herramientas de cifrado y anonimato depende de su adopción generalizada, alienta a los Estados, las organizaciones de la sociedad civil y las empresas a que participen en una campaña para acercar el cifrado de forma deliberada o por defecto a los usuarios de todo el mundo y, cuando sea necesario, a que velen por que los usuarios en peligro dispongan de las herramientas para ejercer su derecho a la libertad de opinión y de expresión de forma segura.**