Naciones Unidas A/HRC/32/38

Asamblea General

Distr. general
11 de mayo de 2016
Español
Original: inglés

Consejo de Derechos Humanos
32º 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*

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. El informe marca el inicio de una serie de estudios sobre cuestiones relativas a la reglamentación estatal, el sector privado y la libertad de expresión en la era digital. En él, el Relator Especial examina el marco jurídico de la libertad de expresión y los principios aplicables en el sector privado, identifica a los principales participantes del sector de la tecnología de la información y las comunicaciones que repercuten sobre la libertad de expresión e introduce diversas cuestiones jurídicas y de políticas que estudiará durante su mandato.

* Este informe se presenta con retraso para poder incluir en él la información más reciente.

GE.16-07644 (S) 020616 030616
1607644

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

Índice

I. Introducción

1. La función que desempeña el sector privado en la era digital parece estar generalizada y ampliarse constantemente, de manera que ese sector se ha convertido en uno de los elementos impulsores de la mayor expansión del acceso a la información de la historia. Algunos de los grandes foros de expresión pública de las redes sociales son propiedad de empresas privadas. Las principales plataformas que agregan e indexan el conocimiento global y diseñan los algoritmos que determinan qué información se publica en Internet son fruto de la iniciativa privada. Además, tanto la inversión en la infraestructura para la tecnología móvil, con la que miles de millones de personas se comunican y acceden a Internet, como su mantenimiento y titularidad están en manos privadas. Las herramientas que emplean las fuerzas del orden y los organismos de inteligencia se crean, por lo general, a partir de productos de los sectores privados de la vigilancia y el procesamiento de datos. Son empresas privadas las que diseñan, fabrican y generalmente mantienen los dispositivos o servicios donde se almacenan los datos personales más importantes (desde información financiera y sanitaria hasta correos electrónicos, mensajes de texto, historiales de búsqueda, fotografías y vídeos).

2. La libertad de opinión y de expresión, tal como la ejercemos en la actualidad, debe buena parte de su pujanza al sector privado, que ostenta un enorme poder en el espacio digital, actuando como pasarela de la información y como intermediario de la expresión. En los entornos digitales, no pueden obviarse ciertas cuestiones importantes sobre el derecho aplicable y el alcance de la autoridad privada y de la regulación pública. ¿Deberían tener esos agentes privados las mismas responsabilidades que las autoridades públicas? ¿Deberían tales responsabilidades derivarse del derecho de los derechos humanos, de las condiciones de servicio, de los arreglos contractuales o de otras fuentes? ¿Cómo deberían estructurarse las relaciones entre las empresas y los Estados? Cuando se enfrentan con presiones para dirigir sus negocios de una manera que atente contra la libertad de expresión, ¿qué medidas deben adoptar los agentes privados? ¿Negarse a entrar en los mercados o salir de ellos? ¿Aconsejar a sus clientes sobre esas presiones? A medida que el mundo se adentra cada vez más en el espacio digital, con la "Internet de las cosas" en un horizonte próximo, es esencial ofrecer pautas sobre cómo garantizar la promoción, la protección y el disfrute de los derechos.

3. El presente informe tiene varios objetivos[1]. En primer lugar, en él se trata de determinar cuáles son las categorías de agentes privados que influyen más destacadamente en la libertad de expresión en la era digital. En segundo lugar, se ponen de relieve cuestiones relativas a la manera en que el sector privado protege la libertad de opinión y de expresión y a la responsabilidad de las autoridades públicas en lo que se refiere a garantizar la protección del espacio para la expresión. En tercer lugar, se identifican varias esferas en las que parece que es más necesario ofrecer pautas sobre cuestiones normativas. Esas esferas se abordarán y se consolidarán mediante la presentación de informes temáticos, informes de los países e informes de visitas a empresas, y mediante comunicaciones y consultas a los Gobiernos, al sector empresarial y a la sociedad civil. En resumen, el presente documento es el primero de una serie de informes que presentará el Relator Especial para proporcionar pautas sobre cómo deben los agentes privados proteger y promover la libertad de expresión en la era digital.

[1] El Relator Especial quisiera dar las gracias a su asesor jurídico, Amos Toh, y a sus alumnos de la Facultad de Derecho de Irvine (Universidad de California) por su ayuda en la preparación del informe.

4. El presente informe se elaboró a partir de un proceso público de aportaciones y consultas. El 3 de diciembre de 2015, el Relator Especial solicitó aportaciones para el informe. Desde la fecha en que hizo pública la solicitud, el Relator Especial recibió 15 comunicaciones de Estados[2] y otras 15 de organizaciones[3]; todas ellas se encuentran en el sitio web del Relator Especial[4]. El Relator Especial también se benefició enormemente de las consultas. Mantuvo una reunión los días 25 y 26 de enero de 2016 con 25 miembros de la sociedad civil en la Facultad de Derecho de Irvine (Universidad de California) y otra reunión con 20 personas del sector privado y de la sociedad civil el 29 de febrero de 2016 en la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos en Ginebra. Los resúmenes de las reuniones también se encuentran en el sitio web del Relator Especial.

II. La libertad de expresión, los Estados y el sector privado en la era digital

5. El presente informe de recopilación parte de una cuestión fundamental: ¿hasta qué punto debería considerarse que es responsabilidad del sector de la tecnología de la información y las comunicaciones promover y proteger la libertad de opinión y de expresión? Para responder a esta pregunta, es necesario empezar con un compendio de las disposiciones del derecho internacional de los derechos humanos que obligan a los Estados a promover y proteger la libertad de expresión y de los principios relativos a las responsabilidades del sector privado en materia de derechos humanos.

A. Marco jurídico internacional

6. El artículo 19 del Pacto Internacional de Derechos Civiles y Políticos y la Declaración Universal de Derechos Humanos protegen el derecho de toda persona a no ser molestada a causa de sus opiniones, a buscar, recibir y difundir informaciones e ideas de toda índole, sin consideración de fronteras y por cualquier procedimiento. Hoy es algo corriente afirmar que las personas tienen los mismos derechos en el contexto virtual y en el real. El anterior titular del mandato destacó el aumento en el número y las formas de restricción del derecho a la información en línea (véase A/HRC/17/27) y demostró la repercusión del aumento de la vigilancia digital en la libertad de expresión (véase A/HRC/23/40). En 2015, el Relator Especial hizo hincapié en la importancia del cifrado y el anonimato para proteger y promover la libertad de expresión (véase A/HRC/29/32). En declaraciones conjuntas, el Relator Especial y varias contrapartes regionales han puesto de relieve cuestiones relativas a la responsabilidad de los intermediarios, el acceso, las restricciones de contenido y otros temas clave que afectan a la libertad de expresión en línea.

7. En el artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos se permiten ciertas restricciones a la libertad de expresión (pero no a la libertad de opinión,

[2] Armenia, El Salvador, Eslovaquia, Estados Unidos de América, Estonia, Grecia, Jordania, Kuwait, Mauricio, México, Países Bajos, Perú, República de Moldova, Rumania y Turquía.

[3] Artículo 19; Asociación para el Progreso de las Comunicaciones; Center for Democracy and Technology; Centro de Tecnología y Sociedad; Centro para la Gobernanza de la Comunicación de la Universidad Nacional de Derecho de Nueva Delhi; Instituto de Derechos Humanos de Dinamarca; Derechos Digitales; European Digital Rights; Grupo de Trabajo sobre Privacidad y Transparencia en Línea de la Freedom Online Coalition; Global Network Initiative; Institute for Human Rights and Business; International Centre for Not-for-Profit Law; Internet Society; Red Progresista Coreana – Jinbonet; Privacy International; Ranking Digital Rights; y New America.

[4] Se pueden consultar en la dirección www.ohchr.org/EN/Issues/FreedomOpinion/Pages/Annual.aspx.

según lo dispuesto en el artículo 19, párrafo 1). En el artículo 19, párrafo 3, se establece que, para ser legítimas, tales restricciones deberán estar fijadas por la ley y ser necesarias para asegurar el respeto a los derechos o a la reputación de los demás o para la protección de la seguridad nacional, el orden público o la salud o la moral públicas. Las restricciones han de ser lo bastante precisas y accesibles para el público para limitar las facultades discrecionales de las autoridades y ofrecer a las personas orientaciones pertinentes (véase la observación general núm. 34 (2011) relativa al artículo 19: libertad de opinión y libertad de expresión). Para que sea necesaria, no basta con que una restricción sea útil, razonable o conveniente[5]. También está claramente establecido que la necesidad implica una evaluación de la proporcionalidad (véase A/HRC/29/32). La proporcionalidad exige demostrar que las medidas restrictivas son el instrumento menos perturbador de los que permitirían desempeñar su función protectora y que guardan proporción con el interés que debe protegerse (véase la observación general núm. 34). Cuando las restricciones no cumplen las condiciones establecidas en el artículo 19, párrafo 3, las personas tienen derecho a un recurso efectivo, según se establece en el artículo 2, párrafo 3, del Pacto.

8. En el mundo virtual, las personas disfrutan también de todos los demás derechos, como el derecho a la vida privada, a las creencias religiosas, el derecho de asociación y de reunión pacífica, el derecho a la educación, a la cultura y el derecho a no ser objeto de discriminación. Los Estados tienen tanto la obligación negativa de abstenerse de violar derechos como la positiva de garantizar su disfrute. Para cumplir esas obligaciones positivas, es probable que las autoridades públicas tengan que adoptar medidas para proteger a las personas de los actos de partes privadas[6].

B. Marco de responsabilidades del sector privado

9. El derecho de los derechos humanos no regula directamente con carácter general las actividades o responsabilidades de las empresas privadas. Existen múltiples iniciativas para orientar a las empresas en el respeto de los derechos fundamentales. El Consejo de Derechos Humanos apoyó los Principios Rectores sobre las Empresas y los Derechos Humanos: puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar" (véase A/HRC/17/4 y A/HRC/17/31). Basándose en las normas vigentes de derechos humanos, con los Principios Rectores se reafirma que los Estados deben cerciorarse de que no solo los órganos estatales, sino también las empresas bajo su jurisdicción, respetan los derechos humanos[7].

10. Los Principios Rectores constituyen un marco para examinar las responsabilidades de las empresas privadas en el sector de la tecnología de la información y las comunicaciones en todo el mundo, con independencia de las obligaciones del Estado o de la aplicación de estas últimas. En los Principios Rectores, por ejemplo, se afirma que las empresas tienen la responsabilidad global de evitar que sus propias actividades provoquen o contribuyan a provocar consecuencias negativas sobre los derechos humanos y hacer frente a esas consecuencias cuando se produzcan, y de tratar de prevenir o mitigar las consecuencias negativas sobre los derechos humanos directamente relacionadas con

[5] Tribunal Europeo de Derechos Humanos, demanda núm. 6538/74, *The Sunday Times v. The United Kingdom* (26 de abril de 1979), párr. 59.

[6] Véase la observación general núm. 31 (2004) sobre la índole de la obligación jurídica general impuesta a los Estados Partes en el Pacto Internacional de Derechos Civiles y Políticos. Es probable que haya otras normas del derecho internacional que se apliquen directamente a las actividades de los agentes privados, como la tipificación penal de los crímenes de lesa humanidad, los crímenes de guerra y los actos de genocidio, en virtud del derecho internacional humanitario.

[7] Principios Rectores sobre las Empresas y los Derechos Humanos, capítulo. I A) 1).

operaciones, productos o servicios prestados por sus relaciones comerciales, incluso cuando no hayan contribuido a generarlos (principio 13)[8].

11. Según los Principios Rectores, proceder con la diligencia debida permite a las empresas identificar, prevenir, mitigar y responder de las consecuencias negativas de sus actividades sobre los derechos humanos[9]. En el entorno digital, las decisiones internas sobre cómo atender las peticiones de los Gobiernos de restringir el contenido o el acceso de los clientes a la información, sobre la aprobación de las condiciones de servicio o las opciones de diseño e ingeniería que afectan a la seguridad y la privacidad, y las decisiones relativas a la prestación o rescisión de los servicios en un mercado determinado pueden tener consecuencias sobre los derechos humanos.

12. En aras de la transparencia, en los Principios Rectores se establece que las empresas deben estar preparadas para explicar las medidas que toman para hacer frente a las consecuencias de sus actividades sobre los derechos humanos, sobre todo cuando los afectados o sus representantes planteen sus inquietudes[10]. El Alto Comisionado de las Naciones Unidas para los Derechos Humanos también ha instado a las empresas del sector de la información y las comunicaciones a que revelen los riesgos y las exigencias de los Gobiernos de manera transparente (véase A/HRC/27/37). Las revelaciones significativas contribuyen a esclarecer, entre otras cosas, en qué medida y en qué contexto solicitan los Gobiernos la retirada de contenido y de datos de clientes, los procesos que se emplean para gestionar tales solicitudes y la interpretación de las leyes, políticas y normativas correspondientes. Las obligaciones en materia de transparencia empresarial pueden incluir también el deber de revelar los procesos e informes relativos a la aplicación de las condiciones de servicio y las solicitudes privadas de regulación de contenido y de datos de usuarios.

13. Por último, la responsabilidad de respetar implica asegurar la disponibilidad de recursos (desde reparaciones morales hasta indemnizaciones y garantías de no repetición) cuando las empresas privadas hayan provocado o contribuido a provocar consecuencias negativas[11].

14. Los Principios Rectores constituyen un punto de partida útil para señalar las responsabilidades privadas en materia de información y comunicaciones, aunque también hay otros proyectos que han formulado propuestas de principios para el sector. Los Principios de Libertad de Expresión y Privacidad de la Global Network Initiative parten de la experiencia y los conocimientos especializados de los inversores, la sociedad civil y la comunidad académica. La Comisión Europea publicó la *Guía del sector de tecnologías de la información y la comunicación para aplicar los Principios Rectores de las Naciones Unidas sobre las Empresas y los Derechos Humanos*. Existen varias iniciativas de la sociedad civil, como los Principios de Manila sobre la Responsabilidad de los Intermediarios, en que se establece la protección mínima de los intermediarios con arreglo a las normas sobre la libertad de expresión; la Declaración Africana sobre Derechos y Libertades en Internet, en la que se promueven los principios y normas de derechos humanos en cuanto a la apertura en la formulación y la aplicación de políticas de Internet en el continente africano; y el Índice de Rendición de Cuentas de las Empresas de Ranking Digital Rights, que sirve para evaluar a una serie de importantes empresas privadas del sector digital en función de su respeto a la libertad de expresión y las normas de privacidad. La sociedad civil también actúa para comprobar y equilibrar a otros agentes que intervienen en la gobernanza de Internet: por ejemplo, con el Código de Buenas Prácticas en

[8] *Ibid*. cap. II A) 11) a 13).
[9] *Ibid*. cap. II A) 17).
[10] *Ibid*. cap. II B) 21).
[11] *Ibid*. cap. II B) 22).

Información, Participación y Transparencia en la Gobernanza de Internet se trata de velar por que los procesos pertinentes se comuniquen eficazmente al público, deban rendir cuentas a todas las partes interesadas y hagan hincapié en la participación democrática.

III. Las funciones del sector privado y la regulación pública/privada

A. Influencia de las empresas privadas en la libertad de expresión

15. Las funciones que desempeñan las empresas privadas para organizar Internet, acceder a ella, alimentarla y regularla son muy variadas y a menudo las categorías se superponen[12].

1. Habilitar la conexión a Internet

16. Mientras que los proveedores de servicios de Internet conectan específicamente a sus abonados a la red, los proveedores de servicios de telecomunicaciones ofrecen una gama más amplia de servicios, como acceso a la radio, la televisión y las comunicaciones telefónicas fijas y móviles. Existen grandes empresas multinacionales que ofrecen los dos tipos de servicio, no solo en su Estado de origen, sino también a nivel global. Vodafone, por ejemplo, es un proveedor británico que posee y administra redes en 27 países y que cuenta con redes asociadas en otros más de 50. TeliaSonera, con sede en Finlandia y Suecia, presta servicio en mercados de toda Eurasia, y MTS Rusia opera en el territorio nacional y ofrece también servicios de telecomunicaciones en Armenia, Turkmenistán y Uzbekistán. Las empresas de ese tipo son a menudo propietarias de importantes elementos de la infraestructura técnica que sustenta Internet y el tráfico de telecomunicaciones (que incluye cables de red de fibra óptica, satélites o enlaces inalámbricos) y se encargan de su mantenimiento. Los proveedores de servicios de Internet de mercados locales y regionales pueden gestionar un número limitado de esas redes o alquilar capacidad de red a los grandes operadores para conectar a sus abonados a Internet. La propiedad estatal es bastante común entre los proveedores de servicios: Suiza, por ejemplo, posee el 51% de las acciones de Swisscom AG[13] y el Uruguay es propietario de Antel, un importante proveedor de servicios de telecomunicaciones en el país[14]. Si bien actualmente los proveedores de servicios de telecomunicaciones y de Internet son quienes suelen encargarse de dar acceso a Internet, cada vez hay más empresas híbridas que ofrecen acceso a Internet además de otros servicios conexos[15].

2. Diseñar y mantener equipos físicos y sistemas operativos que faciliten el procesamiento de la información y el acceso a Internet

17. Las empresas de *hardware* diseñan y fabrican equipos informáticos que conectan a las personas a Internet. Sin embargo, el abanico de dispositivos equipados con funciones de

[12] Véase, por ejemplo, "Strategy panel: ICANN's role in the Internet governance ecosystem" (23 de febrero de 2014); R. Mackinnon y otros, *Fostering Freedom Online: The Role of Internet Intermediaries* (París, UNESCO, 2014); y D. A. Hope, *Protecting Human Rights in the Digital Age* (febrero de 2011).

[13] Véase www.swisscom.ch/en/about/investors/shares/ownership-structure.html.

[14] Véase www.antel.com.uy/antel/; http://cs.stanford.edu/people/eroberts/cs181/projects/2006-07/latin-america/uruguayIntro.html.

[15] Google, por ejemplo, proporcionará acceso a servicios inalámbricos a través de su servicio Google Fiber, además de funciones de búsqueda, alojamiento de contenido y redes sociales, entre otras. Véase https://fiber.google.com/about/.

informática personal se amplía constantemente y es imposible de frenar, habida cuenta de la avalancha de conectividad a la que se hace referencia en términos generales como la "Internet de las cosas", un concepto que alude a la conexión digital de todos los aspectos de nuestra existencia contemporánea. Automóviles, neveras, televisores y relojes son solo algunos ejemplos de dispositivos "inteligentes" que en la actualidad incorporan funciones de navegación, mensajería y otras prestaciones asociadas a Internet.

18. Además, los proveedores de telecomunicaciones y de servicios de Internet compran los equipos y otros componentes que constituyen los elementos físicos troncales de sus redes a proveedores de infraestructuras y a fabricantes de equipos. Estos productos van desde simples *routers* y conmutadores hasta dispositivos de inspección profunda de paquetes, filtrado de redes y dispositivos de bloqueo de Internet, además de centros de supervisión de vigilancia de redes. Cada vez es más frecuente que esas empresas también ofrezcan servicios, consultoría, cursos de formación e incluso gestión.

3. Asignar dominios de Internet

19. De la asignación y venta de las direcciones electrónicas (es decir, los localizadores uniformes de recursos o URL) se ocupan los registros y registradores de nombres de dominio, bajo la supervisión de la Corporación para la Asignación de Nombres y Números en Internet (ICANN), una entidad sin ánimo de lucro. En la actualidad, el registrador más grande del mundo alberga más de 61 millones de nombres de dominio.

4. Información sobre alojamiento web

20. Los servicios de alojamiento web permiten a los usuarios cargar y enviar archivos y otros materiales a los navegadores de sus lectores o clientes. Esas empresas suelen ofrecer almacenamiento de datos, correo electrónico y otros servicios relacionados con los sitios web que sus clientes han adquirido.

5. Facilitar la agregación, el intercambio y la búsqueda de información

21. Los buscadores establecen la conexión esencial entre los usuarios que buscan información y quienes la crean, la agregan y la publican. De hecho, los algoritmos de los buscadores dictan qué ven los usuarios y en qué orden de prioridades, y pueden manipularse para limitar un determinado contenido o darle prioridad. No obstante, las búsquedas de información no se hacen únicamente en buscadores. Los agregadores de contenido, los servicios de investigación especializados, las plataformas de las redes sociales y las redes profesionales también permiten a los usuarios efectuar búsquedas.

6. Producir contenido propio y regular el acceso

22. Las empresas que crean o adquieren contenido producido en sus plataformas suelen tener los derechos de autor sobre ese contenido, lo que les permite monetizarlo y gestionar su acceso. Algunos de los titulares de derechos de autor más influyentes son empresas de medios y de entretenimiento, como medios de información, editoriales, sellos discográficos y estudios de cine y televisión.

7. Conectar a los usuarios y las comunidades

23. Las empresas también proporcionan múltiples servicios que conectan a los usuarios a través de varias plataformas, como el correo electrónico, chats, hilos de discusión, y redes de contactos sociales y profesionales. Los más destacados en esa esfera son los proveedores de correo electrónico, las redes sociales y otras plataformas de redes de contactos, además de los tablones de anuncios electrónicos. Además de esas plataformas, los sitios web de noticias, las plataformas de comercio electrónico y las tiendas de aplicaciones permiten

intercambiar información e ideas mediante reseñas, comentarios y debates. Los sistemas de pago por Internet también incorporan una funcionalidad de red de contactos sociales.

8. Vender bienes y servicios y facilitar las transacciones

24. El comercio electrónico facilita la venta de bienes y servicios y otras transacciones comerciales entre empresas y consumidores, entre unas empresas y otras, o entre consumidores. Las formas en que las empresas dan acceso a estas transacciones, las promueven o las organizan, además del modo en que protegen la gran cantidad de información personal que tales transacciones generan, puede afectar a la libertad de expresión y a la privacidad de sus clientes.

9. Reunir datos, adaptarlos a nuevos fines y venderlos

25. La gran mayoría de las empresas descritas anteriormente recaba información a partir de sus usuarios y acerca de ellos; una información que luego puede utilizarse para adaptar los mensajes publicitarios al perfil de los destinatarios, personalizar los servicios existentes, reducir los riesgos de seguridad o cerrar cuentas de usuarios abusivos. No obstante, también pueden hacer negocio con la recopilación y el análisis de información, ofreciendo servicios de diseño, personalización o venta de tecnologías de vigilancia y de análisis de información, o servicios de consultoría para facilitar operaciones de mantenimiento del orden, inteligencia, ciberseguridad y vigilancia.

B. La regulación en la era digital

26. El ecosistema regulatorio en Internet es amplio y variado, y en él intervienen agentes nacionales, regionales e internacionales, del sector público y del privado, así como del ámbito académico y de la sociedad civil. Algunos aspectos de la tecnología de la información y las comunicaciones, como la prestación de servicios de telecomunicaciones y de Internet, están regulados desde hace tiempo por normas estatales e internacionales y se someten, además, al escrutinio público. Otras esferas, como las búsquedas, las redes sociales y la venta de tecnologías de vigilancia, son también cada vez con mayor frecuencia sometidas al escrutinio público, a medida que aumentan sus repercusiones y su influencia en el ejercicio de la libertad de expresión en Internet.

1. Normas técnicas

27. Las normas y procesos técnicos garantizan que la infraestructura, las redes y las aplicaciones que integran las redes de Internet y de telecomunicaciones funcionen sin contratiempos. La infraestructura física sobre la que fluye el tráfico de Internet (como el cableado de red y los satélites) está configurada en función de varios requisitos técnicos que garantizan su correcto funcionamiento y opera con arreglo a ellos. Entre las organizaciones que elaboran esos requisitos, destacan la Unión Internacional de Telecomunicaciones, que establece normas para la interoperabilidad de las redes de telecomunicaciones; el Instituto de Ingenieros Electricistas y Electrónicos, una asociación profesional que elabora normas para la transmisión wifi; y la Groupe Speciale Mobile Association, una asociación internacional privada del sector de las comunicaciones móviles que elabora normas para redes de telefonía móvil.

28. Otro grupo de organizaciones se ocupa de crear y desarrollar normas técnicas sobre cómo comunicar, almacenar, organizar y presentar datos en Internet. La Internet Engineering Task Force desarrolla y mantiene el Protocolo de Control de Transmisión/Protocolo Internet, que determina cómo se conectan los dispositivos a Internet y cómo se transmiten datos entre ellos. El Consorcio World Wide Web crea normas sobre

cómo mostrar contenido web e interactuar con él que incluyen, entre otras cosas, cuestiones que tienen que ver con el contenido lingüístico y el acceso para las personas con discapacidad. La ICANN formula políticas para el registro de nombres de dominios de primer nivel, tanto genéricos (como .com, org, .edu), como con código de país (.cn, .tj, .sg) o específicos para una comunidad o sector (como .aero). La Autoridad de Números Asignados en Internet, su órgano subsidiario, se encarga de la distribución de las direcciones IP, que se asignan a cada dispositivo que se conecta a Internet y lo identifican con etiquetas numéricas únicas.

29. Si bien las normas técnicas tienen profundas consecuencias para la libertad de expresión, la Comisión de Ciencia y Tecnología para el Desarrollo de las Naciones Unidas ha observado que en muchas ocasiones no se tienen suficientemente en cuenta los problemas de derechos humanos en el marco de la formulación de políticas[16]. Desde luego, las partes interesadas y demás personas que lo deseen pueden participar activamente o como observadores en el trabajo de la mayoría de esos organismos. Sin embargo, puesto que para que la participación sea significativa es necesario tener un nivel generalmente alto de conocimientos técnicos, no siempre se incluyen en los debates las perspectivas de derechos humanos, aunque las opciones técnicas y de diseño pueden repercutir sustancialmente en la libertad de expresión[17].

2. La gobernanza de Internet y la formulación de políticas

30. Los instrumentos jurídicos internacionales no abordan explícitamente la manera en que los Estados y otros agentes deberían mantener una Internet libre y abierta, y regular esta cuestión por ley puede que no siempre sea el enfoque adecuado. De hecho, la gobernanza de Internet no es del ámbito exclusivo de los órganos especializados o los Gobiernos. Recientemente, la Cumbre Mundial sobre la Sociedad de la Información puso de relieve la importancia continua de abordar la cuestión de la gobernanza con un enfoque que integre a los Gobiernos, las empresas y la sociedad civil, además de a interesados y expertos del ámbito académico y técnico (véase la resolución 70/125 de la Asamblea General). En el contexto del comercio mundial, los principios de no discriminación establecidos en virtud de los acuerdos internacionales administrados por la Organización Mundial del Comercio pueden forzar a los Estados a limitar o regular de algún otro modo los servicios no neutrales. La Organización Mundial de la Propiedad Intelectual también se ha enfrentado a un creciente número de peticiones de asesoramiento por parte de los Estados miembros sobre marcos legislativos que les permitan aplicar las obligaciones de los tratados en entornos digitales. Varios órganos regionales, como la Unión Africana, la Comisión Europea y la Organización de los Estados Americanos, procuran garantizar que la

[16] Véase “The mapping of international Internet public policy issues” del Grupo de Expertos entre Períodos de Sesiones de la Comisión de Ciencia y Tecnología para el Desarrollo (noviembre de 2014).

[17] No cabe duda de que algunas organizaciones han dedicado recursos a la tarea de incorporar las perspectivas de derechos humanos en los debates técnicos. La ICANN, por ejemplo, ha creado un grupo de trabajo intercomunitario sobre su responsabilidad corporativa y social de respetar los derechos humanos; dicho grupo de trabajo tiene por objetivo situar y entender los problemas y las posibles soluciones asociados a la responsabilidad corporativa y social de la ICANN (https://community.icann.org/display/gnsononcomstake/CCWP+on+ICANN's+Corporate+and+Social+Responsibility+to+Respect+Human+Rights). Algunas organizaciones no gubernamentales también han hecho contribuciones a los debates técnicos centradas en los derechos humanos. Véase, por ejemplo, Neils ten Oever, “Research into human rights protocol considerations”, que se puede consultar en https://datatracker.ietf.org/doc/draft-tenoever-hrpc-research/.

política global de Internet esté formulada y se aplique teniendo en cuenta las leyes, las particularidades y los problemas de sus respectivas regiones[18].

31. Algunas organizaciones que redactan normas técnicas se encargan también de formular políticas. Por ejemplo, la Unión Internacional de Telecomunicaciones desarrolla y coordina las políticas de telecomunicaciones globales. La ICANN, en consulta con los Gobiernos, el sector privado, la sociedad civil y otras instancias pertinentes, emite opiniones sobre las políticas relativas a los tipos de nombres de dominios de primer nivel que pueden registrarse y sobre quiénes pueden reclamar su titularidad.

32. Las iniciativas lideradas por las empresas del sector también tienen por objeto afrontar los desafíos que plantea la gobernanza de Internet y que la normativa jurídica vigente no aborda adecuadamente. Por ejemplo, en el proyecto Copyright Alert System participan asociaciones comerciales del mundo del cine y de la industria discográfica y proveedores de servicios de Internet para desarrollar y aplicar un enfoque unificado contra la violación de los derechos de autor en Internet. El Grupo de Diálogo de la Industria de las Telecomunicaciones reúne a operadores de telecomunicaciones y proveedores para abordar problemas de libertad de expresión y del derecho a la privacidad en dicho sector.

33. Si bien muchas de esas iniciativas son de carácter privado, a veces cooperan con los Estados o cuentan con su respaldo. Por ejemplo, la Internet Watch Foundation del Reino Unido de Gran Bretaña e Irlanda del Norte, que ofrece a los proveedores de servicios de Internet y las plataformas de alojamiento web un servicio de "notificación y retirada" que los alerta en caso de que detecte contenido posiblemente delictivo en sus redes, también ofrece a las fuerzas del orden "datos exclusivos" para sus investigaciones sobre contenido de ese tipo.

IV. Cuestiones jurídicas y políticas

34. La multiplicidad de funciones que desempeña el sector de las tecnologías de la información y las comunicaciones pone de manifiesto cuestiones relacionadas con aspectos jurídicos y de políticas que han de ser estudiadas y desarrolladas por los mecanismos internacionales de derechos humanos.

A. Regulación del contenido

35. Muchas de las preguntas sobre el papel de las empresas privadas en la era digital se centran en la regulación del contenido. Por ejemplo, ¿de qué manera facilitan o solicitan los Estados la retirada o censura de contenido y las restricciones innecesarias o desproporcionadas del derecho a buscar, recibir y transmitir contenido en Internet a través de plataformas y redes privadas? ¿Cómo responden las empresas privadas a esas demandas y a otras presiones externas? Cuando el sector privado elabora y pone en práctica sus propias políticas y normas internas para proteger y promover los derechos en línea, ¿qué repercusiones tienen estas en la expresión individual y en el acceso a la información?

36. El contenido digital transmitido por redes privadas y alojado en plataformas privadas es cada vez con mayor frecuencia regulado tanto por el Estado como por las empresas. El universo de contenido generado por los usuarios está en constante expansión: los blogs, los mensajes de texto, los hilos de discusión, las fotografías, los vídeos y las publicaciones en las redes sociales son solo una muestra del tipo de contenido que los

[18] Véase, por ejemplo, Comisión Europea, *Guía del Sector de las TIC* (párr. 14 de este documento); y Comisión Interamericana de Derechos Humanos, Relatoría para la Libertad de Expresión, F*reedom of Expression and the Internet* (2013).

usuarios crean y comparten diariamente. Las empresas que gestionan redes y plataformas para ese contenido, conocidas como intermediarios, podrán "dar acceso, alojar, transmitir e indexar contenido, productos y servicios originados por terceros" aunque ellos no sean quienes creen o produzcan dicho contenido[19].

37. Por lo general, los Estados suelen solicitar que se retire contenido aduciendo motivos de difamación, blasfemia, normas electorales, acoso o discurso de odio, provocación, propiedad intelectual, obscenidad e indecencia, captación para actividades terroristas o enaltecimiento del terrorismo, protección de la seguridad nacional y la seguridad pública, protección de la infancia y prevención de agresiones sexistas. Los Estados también han regulado algunos problemas asociados a la libertad de expresión que existen desde hace mucho tiempo pero que se complican cada vez más en la era digital, como el "derecho al olvido" y la pluralidad y la diversidad (por ejemplo, la neutralidad de la red). Los intermediarios establecen y aplican unas condiciones de servicio diseñadas para abordar muchas de estas cuestiones por razones jurídicas, comerciales o de otra índole. Muchos de esos temas suscitan preguntas sobre cómo encontrar el equilibrio adecuado entre libertad de expresión y otros derechos humanos (como el derecho a la vida privada y a la no discriminación). Si bien las regulaciones de contenido suelen ser de carácter restrictivo, pueden también exigir la transmisión de mensajes ordenados o autorizados por el Gobierno[20], o prohibir la tarificación diferenciada para el contenido y los servicios de distribución de contenido[21].

1. Regulación estatal

38. Los Estados regulan el contenido digital con medios jurídicos, políticos y técnicos diversos. Entre las tendencias preocupantes, destacan las siguientes.

Vaguedad de las leyes

39. Las regulaciones de contenido suelen traducirse en leyes, órdenes judiciales o directivas u ordenanzas emitidas por organismos administrativos a los que se ha delegado la competencia de gestionar las cuestiones relativas a las telecomunicaciones y a Internet. Por ejemplo, China modificó recientemente su Ley de Ciberseguridad para prohibir que las personas y organizaciones hiciesen uso de Internet para "alterar el orden social" o "perjudicar el interés público"[22]. Del mismo modo, en un proyecto de ley que se está examinando en Nigeria se prohíbe publicar en "cualquier medio" declaraciones "con la intención dolosa de desacreditar o poner a la opinión pública en contra de" una persona, grupo o institución gubernamental[23]. Ese tipo de redacción permite que las autoridades ejerzan una amplia discrecionalidad para determinar qué tipos de expresiones digitales vulnerarían sus condiciones. En consecuencia, es probable que las personas y las empresas actúen con excesiva cautela para evitar sanciones onerosas, filtrando el contenido de condición jurídica incierta y adoptando otras modalidades de censura y autocensura.

[19] MacKinnon y otros, *Fostering Freedom Online*, pág. 19; K. Perset, *The Economic and Social Role of Internet Intermediaries* (OCDE, 2010).

[20] Véase Vodafone Group Plc, "Response on issues relating to mobile network operations in Egypt" (2011).

[21] La India, por ejemplo, prohíbe a los proveedores de servicios ofrecer o cobrar tarifas discriminatorias por servicios de datos en función del contenido (Reglamento de Prohibición de las Tarifas Discriminatorias por Servicios de Datos, 2016).

[22] China, Ley de Ciberseguridad (2015), art. 9.

[23] Parlamento de Nigeria, proyecto de ley para prohibir las peticiones frívolas y otros asuntos conexos, artículo 3, párrafo 3.

Responsabilidad excesiva de los intermediarios

40. Los Estados a menudo solicitan la cooperación de intermediarios para hacer cumplir las reglamentaciones sobre redes y plataformas privadas. Los proveedores de servicios de Internet y de telecomunicaciones, por ejemplo, están obligados a cumplir las leyes y reglamentos locales como condición para obtener sus licencias de explotación, un requisito legítimo que resulta problemático cuando las leyes locales o su aplicación contravienen el derecho de los derechos humanos. En cambio, las empresas menos limitadas por los requisitos para la concesión de licencias, como las plataformas de las redes sociales, los buscadores y los registradores de nombres de dominio, se enfrentan a la amenaza de que los Estados alteren la infraestructura local, amenacen la seguridad de los empleados locales, o bloqueen el acceso local a sus plataformas.

41. Las empresas privadas también pueden recurrir a intermediarios para que limiten o retiren contenido. Por ejemplo, suelen presentarse denuncias asociadas a la propiedad intelectual cuando una empresa alega que una persona ha compartido o utilizado contenido vulnerando sus derechos de autor o ha creado un nombre de dominio que infringe sus derechos de marca. Si bien se puede recurrir a la doctrina del uso leal o a otras medidas de defensa frente a esas denuncias, los marcos jurídicos sobre la propiedad intelectual pueden inhibir la expresión cultural y artística (véase A/HRC/28/57).

42. El Tribunal de Justicia de la Unión Europea, en el asunto *Google Spain c. Mario Costeja González*, obligó a Google, en virtud de la Directiva de la Unión Europea sobre protección de datos, a eliminar de la lista de resultados vínculos a páginas web que mencionaban el nombre de Mario Costeja González, a pesar de que la publicación original de dichas páginas no se retiró[24]. La decisión ha tenido una importante repercusión fuera del contexto europeo[25]. El alcance y la aplicación de esta decisión ponen de relieve cuestiones relativas a cómo alcanzar el equilibrio adecuado entre el derecho a la vida privada y la protección de datos personales, por un lado, y el derecho a buscar, recibir y difundir información que incorpore ese tipo de datos, por otro.

43. Cada vez se recurre con mayor frecuencia a intermediarios para evaluar la validez de las peticiones de los Estados y de las denuncias de las empresas privadas en función de criterios jurídicos generales y para que retiren contenido o eliminen vínculos con arreglo a dichas evaluaciones. Por ejemplo, en la Ley de Delitos Cibernéticos de 2015 de la República Unida de Tanzanía únicamente se exime de responsabilidad a los proveedores de hipervínculos por la información vinculada en caso de que "retiren o inhabiliten inmediatamente el acceso a dicha información cuando la autoridad competente se lo ordene"[26]. En el contexto de los derechos de autor, en virtud de la Ley de Derechos de Autor del Milenio Digital de los Estados Unidos de América se exime a los proveedores de "servicios en línea y acceso a la red" de responsabilidad por el contenido de terceros siempre que "eliminen con prontitud el material que se afirme que infringe la ley o que podría ser objeto de una actividad infractora o inhabiliten el acceso" tras recibir la notificación[27]. Esos marcos de notificación y retirada de contenido han sido objeto de críticas por incentivar denuncias cuestionables y por no ofrecer la protección adecuada a los intermediarios que procuran aplicar a la reglamentación de contenidos normas equitativas que tengan en cuenta los derechos humanos.

44. Otro elemento importante de preocupación es que los intermediarios privados no suelen disponer de medios suficientes para determinar la ilegalidad de los contenidos. La

[24] Sentencia del Tribunal de Justicia de la Unión Europea (Gran Sala), asunto C -131/12 (13 de mayo de 2014).

[25] Presentación del artículo 19.

[26] Párr. 43 a).

[27] Código de los Estados Unidos, título 17, art. 512 c) 1) C).

Comisión Interamericana de Derechos Humanos ha observado que los agentes privados "no tienen la capacidad de ponderar derechos e interpretar la ley de conformidad con los estándares en materia de libertad de expresión y otros derechos humanos"[28]. Ello puede deberse a la limitación de recursos, la falta de supervisión y de rendición de cuentas, o posibles conflictos de intereses. En vista de la posible responsabilidad, las empresas pueden verse inclinadas a practicar la autocensura o a la censura excesiva.

Restricciones extralegales

45. Los Estados también procuran limitar el contenido digital fuera de la ley. Algunos Estados han promovido que las empresas de medios de comunicación social y otros prestadores de servicios de alojamiento de contenidos generados por los usuarios vigilen y retiren contenido por iniciativa propia, en lugar de esperar a recibir una solicitud gubernamental basada en la legislación sobre la materia. Los funcionarios públicos también han intentado persuadir a las empresas para que aprueben iniciativas de reacción contra ese discurso a través de foros públicos, campañas y debates privados. Los Gobiernos también se ocupan cada vez más de identificar qué contenidos de los medios de comunicación social resultan inapropiados con arreglo a las condiciones de servicio, a fin de inducir a la empresa a que los retire o desactive la cuenta responsable.

Filtrado

46. Los Estados suelen bloquear y filtrar contenido con la ayuda del sector privado. Los proveedores de servicios de Internet pueden bloquear el acceso a determinadas palabras clave, páginas o sitios web enteros. El tipo de técnica de filtrado de las plataformas que alojan contenidos digitales depende de la naturaleza de la plataforma y del contenido en cuestión. Los registradores de nombres de dominio puede negarse a registrar los dominios que figuren en la lista negra del Gobierno; las empresas que están detrás de las redes sociales pueden retirar mensajes o suspender cuentas; los buscadores pueden retirar los resultados de búsquedas que remitan a contenidos ilícitos. El método de restricción exigido por los Gobiernos o empleado por las empresas puede plantear problemas tanto de necesidad como de proporcionalidad, en función de la validez de las razones citadas para la retirada y del riesgo de que el contenido retirado sea lícito o protegido.

47. La combinación de las ambigüedades en las normas estatales y las obligaciones concernientes a la responsabilidad onerosa del intermediario podrían dar lugar a un filtrado excesivo. Incluso si las disposiciones relativas al contenido se hubieran promulgado y aplicado de forma válida, los usuarios podrían seguir experimentando restricciones innecesarias en el acceso. Por ejemplo, el filtrado de los contenidos en una jurisdicción puede afectar a la expresión digital de los usuarios en otras jurisdicciones. Aunque las empresas pueden configurar filtros de aplicación exclusiva en una jurisdicción o región determinada, ha habido casos en los que, pese a todo, esos filtros se extendieron a otras zonas o redes de la plataforma. Por ejemplo, en 2013, el filtrado ordenado por el Estado y llevado a cabo por la empresa Airtel en la India dio lugar a restricciones del mismo contenido en varias redes de Omán pertenecientes a su socia Omantel[29].

Bloqueo de redes o corte de servicios

48. El corte de servicios y las restricciones conexas son formas particularmente perniciosas de hacer cumplir las disposiciones relativas al contenido. Esas medidas se suelen justificar apelando a la seguridad nacional, el mantenimiento del orden público o la

[28] Comisión Interamericana de Derechos Humanos, *Freedom of Expression and the Internet*, págs. 47 y 48.

[29] Citizen Lab, "Routing gone wild: documenting upstream filtering in Oman via India" (2012).

prevención de desórdenes públicos. En 2015, el Relator Especial y representantes de la Organización para la Seguridad y la Cooperación en Europa, la Organización de los Estados Americanos y la Comisión Africana de Derechos Humanos y de los Pueblos condenaron los "interruptores remotos"[30] de Internet por ser contrarios a derecho. En un solo año se recibieron informes de cortes en Bangladesh, el Brasil, Burundi, la India, el Pakistán y la República Democrática del Congo[31]. El Relator Especial confirmó casos de desconexión de los proveedores de servicios de telecomunicaciones y cortes de servicio en Tayikistán, durante su visita oficial en marzo de 2016[32].

Redes no neutrales

49. Además de abstenerse de imponer restricciones innecesarias y desproporcionadas al acceso a los contenidos digitales, los Estados también tienen el deber de velar por una Internet libre y abierta. El principio de neutralidad de la red establece que todos los datos, contenidos y servicios de Internet sean tratados de forma equitativa y sin discriminación indebida. Sin embargo, los proveedores de servicios de Internet pueden utilizar tecnologías que aceleren o favorezcan de otro modo el acceso a determinados contenidos y servicios, mientras disminuyen la velocidad de acceso a otros (esa práctica se conoce como "*throttling*"). El creciente número de colaboraciones entre los proveedores de servicios de Internet y las plataformas de alojamiento de contenidos que ofrecen datos inalámbricos gratuitos para poder acceder a contenidos en línea o a servicios prestados por esas plataformas (también conocido como prestación de servicios sin costo) ha sido objeto de controversia. Si bien esas medidas menoscaban el principio de neutralidad de la red, sigue siendo objeto de debate si pueden permitirse en las zonas que carecen de acceso a Internet.

50. La reglamentación estatal en esa esfera es desigual e incierta. Unos pocos Estados han reconocido la importancia general de la neutralidad en la red. Rumania, por ejemplo, ha señalado que está "a favor de las iniciativas orientadas a garantizar que toda la población tenga acceso de manera efectiva a la información en línea"[33]. Aún son menos los Estados que han brindado protección jurídica específica[34]. A comienzos de 2016, la Autoridad de Regulación de las Telecomunicaciones de la India publicó un reglamento por el que se prohibía a los proveedores de servicios ofrecer o cobrar "tarifas discriminatorias por servicios de datos ofrecidos o cobrados al consumidor sobre la base del contenido"[35]. En varios países, como el Brasil, Chile, los Estados Unidos y los Países Bajos, se han aprobado leyes o medidas que incluyen alguna forma de defensa de la neutralidad en la red.

2. Políticas y prácticas internas

51. Las políticas y normas de los intermediarios pueden tener importantes efectos sobre la libertad de expresión. Si bien las condiciones de servicio son la fuente primaria de la reglamentación, las opciones de diseño e ingeniería pueden afectar también a la presentación de contenido.

[30] Declaración conjunta sobre la libertad de expresión y las repuestas ante situaciones de conflicto (2015).

[31] Comunicación del Institute for Human Rights and Business at 3.

[32] 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 (9 de marzo de 2016).

[33] Comunicación del Gobierno de Rumania.

[34] Mackinnon y otros, *Fostering Freedom Online*, pág. 80.

[35] Reglamento por el que se prohíben las tarifas discriminatorias por la prestación de servicios de datos, 2016.

Condiciones de servicio

52. Las condiciones de servicio, que deben ser aceptadas por los particulares como requisito para acceder a una plataforma, a menudo incluyen restricciones sobre el contenido que se puede compartir. Esas restricciones se formulan con arreglo a leyes y reglamentos locales y reflejan prohibiciones similares, en particular contra el acoso, el discurso del odio, la incitación a la delincuencia, la violencia gratuita y las amenazas directas[36]. Las condiciones de servicio suelen formularse de forma tan general que puede resultar difícil predecir de manera clara qué tipo de contenido puede restringirse. La aplicación irregular de las condiciones de servicio también ha sido objeto de críticas. Hay quienes afirman que las plataformas más populares del mundo no responden adecuadamente a las necesidades e intereses de los grupos vulnerables; por ejemplo, se han formulado acusaciones de renuencia "a afrontar directamente la violencia contra la mujer relacionada con la tecnología, hasta que se convierte en una cuestión de relaciones públicas"[37]. Al mismo tiempo, algunas plataformas han sido criticadas por exceso de celo en la censura de una amplia gama de expresiones que, siendo legítimas, quizá puedan resultar "incómodas" para cierto público[38]. A esas preocupaciones se añaden la falta de un procedimiento de recurso, la escasa comunicación por parte de la empresa acerca de las razones por las que se retiró cierto contenido o se desactivó la cuenta. Las condiciones de servicio que exigen que el registro consigne el nombre real de una persona o pruebas que demuestren el uso válido de un seudónimo también pueden inhibir de forma desproporcionada, en sociedades cerradas, la capacidad de los grupos vulnerables o los agentes de la sociedad civil para utilizar plataformas en línea con fines de expresión, asociación o promoción.

53. Asimismo, a la hora de retirar contenidos que consideren censurables, los Estados dependen cada vez más de las condiciones de servicio. El Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo ha observado que varios Estados han establecido mecanismos para la retirada de contenido que con frecuencia pretenden la retirada de algunos que, siendo lícitos, podrían considerarse como extremistas (véase A/HRC/31/65). La Unidad de Lucha contra la Divulgación del Terrorismo en Internet del Reino Unido, por ejemplo, se dedica a retirar los contenidos en línea "de naturaleza extremista violenta o terrorista", mediante métodos que incluyen el "uso de mecanismos para identificar el contenido cuestionable de sitios web y denunciarlo por vulnerar las condiciones de servicio de esos sitios"[39]. Esas prácticas plantean la posibilidad de que los Estados puedan recurrir a unas condiciones de servicio de carácter privado para eludir las leyes o las normas de derechos humanos contrarias a las restricciones de contenido.

54. La labor de censura privada se complica por la gran cantidad de denuncias y de contenido sospechoso que los intermediarios identifican diariamente. Las plataformas de mayor tamaño también pueden subcontratar la gestión del contenido, lo que distancia más aún a los moderadores del contenido de las decisiones internas en materia de formulación de políticas e intensifica las incoherencias en el cumplimiento de la ley. Los intermediarios que operan en una amplia gama de mercados se enfrentan inevitablemente a "complejos

[36] Véanse, por ejemplo, las condiciones de servicio de Facebook, art. 3, párr. 7; las condiciones de servicio de Twitter; las Normas de la comunidad de YouTube; y Reddit.

[37] Véase https://ourinternet-files.s3.amazonaws.com/publications/no24_web_2.pdf.

[38] Véase onlinecensorship.org.

[39] Consejo de Jefes de la Policía Nacional, Unidad de Lucha contra la Divulgación del Terrorismo en Internet; presentación del Centro para la Tecnología y la Democracia;

juicios de valor", problemas relacionados con la sensibilidad cultural y la diversidad y "difíciles decisiones sobre conflictos de legislaciones"[40].

Opciones de diseño e ingeniería

55. La manera en que los intermediarios gestionan, categorizan y clasifican contenidos determina la información a la que los usuarios pueden acceder y pueden consultar en sus plataformas. Las plataformas, por ejemplo, utilizan predicciones algorítmicas de las preferencias del usuario y orientan con arreglo a ellas la publicidad que puede ver, cómo se organiza el contenido de sus redes sociales y en qué orden aparecen los resultados cuando efectúa una búsqueda[41]. Otras medidas de autorregulación, como las iniciativas "de reacción" en apoyo a la lucha contra el terrorismo o el acoso[42], también afectan a la forma en que los usuarios pueden consumir y procesar contenidos de Internet sobre temas delicados. Queda pendiente la cuestión de cómo pueden compatibilizarse las preocupaciones que plantean las decisiones en materia de diseño e ingeniería con la libertad de las entidades privadas para diseñar las plataformas y adaptarlas a su gusto.

B. Vigilancia y seguridad digital

56. La vigilancia del Estado y la recopilación y retención de datos empresariales plantean cuestiones sustanciales relacionadas con la libertad de expresión. Por ejemplo, ¿cómo llevan a cabo los Estados actividades de vigilancia con la cooperación del sector privado, y cómo repercute esa cooperación en la libertad de expresión? ¿Cuáles son las responsabilidades de los agentes privados cuando descubren que los Estados acceden de forma encubierta a datos de Internet y de telecomunicaciones transmitidos o almacenados en sus redes o plataformas? ¿Cuáles son las responsabilidades del sector privado en relación con la protección de la seguridad y el anonimato en línea?

57. Las comunicaciones digitales y los datos transmitidos o almacenados en redes privadas y plataformas son, cada vez más, objeto de vigilancia y de otras formas de injerencia, ya sea por el Estado o por agentes privados. La vigilancia innecesaria y desproporcionada puede socavar la seguridad en línea y el acceso a la información y las ideas (véase A/HRC/23/40). La vigilancia puede crear un efecto disuasorio sobre la expresión en línea de los ciudadanos corrientes, que pueden autocensurarse por temor a ser objeto de seguimiento constante. La vigilancia ejerce un efecto desproporcionado en la libertad de expresión de una amplia gama de grupos vulnerables, incluidas las minorías raciales, religiosas, étnicas, de género y sexuales, los miembros de ciertos partidos políticos, la sociedad civil, los defensores de los derechos humanos, profesionales como los periodistas, los abogados y los sindicalistas, las víctimas de la violencia y el maltrato, y los niños (véase A/HRC/29/32). La capacidad del Estado para llevar a cabo la vigilancia puede depender de la medida en que las empresas cooperen o se resistan a esa vigilancia.

1. Solicitudes de datos de clientes

58. A medida que los proveedores de servicios de Internet, las plataformas de las redes sociales, los buscadores, los proveedores de servicios en la nube y otras empresas han ido transmitiendo o almacenando en cantidades cada vez más ingentes datos de sus clientes, el volumen de solicitudes de información del Gobierno acerca de los usuarios en virtud de las

[40] Emily Taylor, *The Privatization of Human Rights: Illusions of Consent, Automation and Neutrality*, documento núm. 24 de la GCIG (2016).

[41] Presentación del Centro de Tecnología y Sociedad; Ranking Digital Rights.

[42] Véase, por ejemplo, Comité para Asuntos de Interior, declaración oral de Anthony House, Google Europa, Oriente Medio y África (2 de febrero de 2016).

leyes y reglamentos locales también ha comenzado a aumentar. Varias de las principales empresas de Internet han informado de un aumento de las solicitudes[43]. Muchas de ellas corresponden a las fuerzas del orden y los servicios de inteligencia. La supervisión de esas solicitudes por parte de los Estados puede variar desde la autorización judicial previa[44] a la aprobación de altos cargos del poder ejecutivo[45], o puede no existir. Los acuerdos de concesión de licencias y la ley pueden limitar la capacidad del sector privado para oponerse a esas solicitudes o imponer la rendición de cuentas. Incluso las plataformas de almacenamiento de contenidos, que carecen de presencia física en algunas de las jurisdicciones en las que operan, pueden enfrentar el bloqueo de sus servicios y los intentos de las empresas subsidiarias de intimidar a sus empleados. No obstante, las empresas de todas las esferas de la industria de la tecnología de la información y las comunicaciones son capaces de establecer y ejercer diversos grados de influencia en sus relaciones con los Estados para resistirse a la aplicación abusiva de la ley o, cuando menos, mitigar el daño causado. Entre las estrategias de resistencia eficaces cabe citar la inclusión de garantías de respeto de los derechos humanos en los acuerdos de concesión de licencias y otros contratos pertinentes; la interpretación restrictiva de las solicitudes de los Gobiernos; la negociación con funcionarios gubernamentales sobre el alcance de esas solicitudes; el recurso judicial ante solicitudes o leyes de alcance demasiado amplio; la facilitación de la información pertinente a las personas afectadas, los medios de comunicación o el público; y la suspensión o retirada del servicio en un mercado concreto o la decisión de no entrar en él.

2. Venta de equipo de vigilancia y de censura

59. El sector privado proporciona equipo físico, programas informáticos y otras tecnologías que permiten a los Estados interceptar, almacenar o analizar las comunicaciones y otra información. Los proveedores de infraestructura, los fabricantes de equipos físicos y los desarrolladores de programas informáticos pueden diseñar o adaptar productos en nombre de los Estados, o proporcionar equipos y tecnología de doble uso que los Estados pueden adaptar posteriormente a sus propias necesidades. Los proveedores de servicios de telecomunicaciones y de Internet también pueden adquirir equipos o programas informáticos de esas empresas para instalar en su red componentes que les permitan cumplir con los protocolos de interceptación que disponen las leyes de los Estados en los que operan. Los Estados pueden recurrir a estos productos y servicios para atacar, acosar o intimidar a miembros de grupos vulnerables.

3. Interceptación de las comunicaciones

60. Los Estados también pueden intervenir de manera encubierta la infraestructura técnica perteneciente a los proveedores de servicios y plataformas de contenido a fin de interceptar una gran variedad de información, incluidas comunicaciones, información sobre cuentas de usuarios, y los registros telefónicos y de Internet. Al parecer, los Estados manipulan los equipos informáticos durante el proceso de entrega a los clientes, se infiltran en plataformas y redes privadas gracias a programas malignos, piratean dispositivos específicos y explotan otras lagunas de la seguridad digital. Cuando las empresas tienen conocimiento de esa vigilancia, pueden surgir cuestiones relativas a sus responsabilidades en materia de derechos humanos, como la notificación a los clientes o la mitigación de esos daños mediante medidas de seguridad. Las empresas que venden equipos y servicios a los Gobiernos para aplicar técnicas de vigilancia encubierta pueden estar cometiendo violaciones de los derechos humanos con motivo de sus ventas.

[43] Véanse los recientes informes de transparencia de Google, Facebook, Dropbox, Twitter y Microsoft.
[44] Suecia, Ley sobre Interceptación de Señales en Operaciones de Defensa, art. 3, párr. 2.
[45] Australia, Ley de Telecomunicaciones (Interceptación y Acceso) de 1979, art. 9, párr. 1.

4. Tratados de asistencia judicial recíproca y localización de datos

61. Es importante señalar que la vigilancia se ve afectada por otras exigencias relativas a la información que se encuentra en manos privadas. Por ejemplo, la incapacidad del régimen de tratados de asistencia judicial recíproca para adaptarse al ritmo de exigencia de datos transfronterizos puede inducir a los Estados a recurrir a medidas invasivas de vigilancia extraterritorial. Las leyes que exigen a las empresas que conserven los datos de los clientes o que los almacenen en los centros de datos locales también pueden alentar esa vigilancia.

5. Cifrado y anonimato

62. Desde que el Relator Especial informó sobre la importancia del cifrado y el anonimato para proteger la libertad de opinión y de expresión ha aumentado la presión de los Gobiernos sobre las sociedades para debilitar la seguridad de los dispositivos digitales, así como de la información y las comunicaciones de sus clientes. Una serie de entidades privadas, que va desde los fabricantes de equipos informáticos a los proveedores de servicios de correo electrónico, ha tomado medidas para desarrollar y aplicar tecnologías que mejoren la seguridad, el anonimato y la privacidad de los usuarios. Esas medidas incluyen el cifrado de extremo a extremo para las comunicaciones digitales, el cifrado de discos y las actualizaciones de los programas informáticos a tiempo para cerrar las brechas de seguridad. Como respuesta, los Estados están tratando de obligar a las empresas a incorporar o aprovechar deficiencias técnicas en sus productos y servicios en lugar de hacerlo ellos mismos. En los Estados Unidos, por ejemplo, el Buró Federal de Investigaciones solicitó a un tribunal federal que obligara a Apple a crear programas informáticos que facilitasen el acceso al iPhone de un sospechoso en una investigación en la esfera de la lucha contra el terrorismo. Con el proyecto de ley de regulación de las facultades de investigación, presentado ante el Parlamento británico el 1 de marzo de 2016, se prende facultar a los servicios de inteligencia para solicitar una orden que exija a las entidades privadas que “garanticen la injerencia en todos los equipos con el fin de obtener datos del equipo de comunicaciones […] y cualquier otra información”[46].

C. Transparencia

63. La transparencia puede ayudar a asegurar que las cuestiones relacionadas con la regulación de Internet puedan predecir significativamente sus obligaciones jurídicas y a oponerse a ellas cuando proceda. Las deficiencias en el cumplimiento de esas normas ponen en peligro la capacidad de las personas para comprender los límites impuestos a su libertad de expresión en línea y obtener la reparación adecuada cuando se vulneren sus derechos. Se plantean problemas de transparencia en el contexto del Estado y en el del sector privado, como las alianzas público-privadas, la participación del sector privado en las negociaciones comerciales y la carrera de armamento digital.

64. A pesar de los múltiples intentos de reforma, sigue faltando transparencia con respecto a las solicitudes de los Gobiernos. Si bien se han producido algunas mejoras en la presentación de informes de transparencia relativos a las solicitudes de información sobre los usuarios formuladas por los Gobiernos, hay mucha menos información disponible sobre el volumen y la naturaleza de las solicitudes de los Gobiernos para restringir o retirar contenidos[47]. No está claro si esas estadísticas quedan incluso almacenadas. Las restricciones estatales privadas relativas a la divulgación de información pertinente pueden

[46] Proyecto de ley de regulación de las facultades de investigación (2015), disp. 88, párr. 2.

[47] Comunicaciones del Grupo de Trabajo sobre Privacidad y Transparencia en Línea de la Freedom Online Coalition; y el Grupo de Diálogo de la Industria de las Telecomunicaciones.

suponer un obstáculo importante para la transparencia de las empresas. Varios Estados prohíben la divulgación de solicitudes gubernamentales de retirada de contenidos o de acceso a los datos de los usuarios. La India, por ejemplo, prohíbe a los intermediarios de servicios en línea la divulgación de detalles de las órdenes del Gobierno sobre el bloqueo de acceso a contenidos de Internet, así como de las medidas que se adopten en respuesta a tales órdenes[48]. Con el proyecto de ley de regulación de las facultades de investigación se pretende prohibir a los proveedores de servicios de telecomunicaciones que revelen, entre otras cosas, "la existencia y los contenidos" de las órdenes gubernamentales para la conservación de los datos de las comunicaciones de los clientes[49]. En otros Estados, la ambigüedad de las leyes y los reglamentos hace que resulte difícil para las empresas determinar qué tipos de información se les permite revelar. En Sudáfrica, por ejemplo, está prohibida la divulgación de información sobre las solicitudes formuladas por el Gobierno para acceder a datos de los clientes[50], aunque no queda claro si esa misma restricción se aplica a las solicitudes de retirada de contenidos[51].

65. En el contexto del sector privado, los proveedores de servicios y las plataformas de alojamiento de contenidos a menudo divulgan al menos alguna información sobre las circunstancias en las que se retiran contenidos o se cumple con las solicitudes gubernamentales de datos de los clientes. Hay una amplia variación, no obstante, con respecto a la difusión de interpretaciones o explicaciones de las normas estatales y las condiciones de servicio, y a los procesos internos para su aplicación y cumplimiento. También hay lagunas en materia de divulgación de estadísticas sobre el volumen, la frecuencia y los tipos de solicitud de datos de los usuarios y de retirada de contenido, a causa de las restricciones que impone el Estado o de decisiones de política interna. En cualquier caso, es más probable que las empresas den a conocer estadísticas sobre solicitudes gubernamentales que sobre solicitudes privadas. También ha habido mucha menos investigación sobre la medida en que otros intermediarios de servicios en línea (por ejemplo, de carácter financiero o de comercio electrónico) y empresas divulgan información relativa a las solicitudes de datos de los clientes y de retirada de contenido.

66. El actual debate sobre las normas mínimas para la divulgación de la información empresarial y las prácticas óptimas pertinentes refleja incertidumbre acerca del equilibrio adecuado entre la transparencia y los valores contrapuestos, como la seguridad individual y el secreto comercial. Si bien existe un consenso cada vez mayor en torno al hecho de que las empresas deberían divulgar información sobre cómo se interpretan y aplican las restricciones, hay discrepancias sobre la forma en que debería hacerse. Asimismo, hay un acuerdo generalizado sobre la importancia de la transparencia cuantitativa, pero no está tan claro cómo se debe contextualizar, presentar y poner a disposición esa información.

D. Vías de recurso

67. Las restricciones a la libertad de expresión en línea se producen diariamente, y a menudo por intervención de las empresas, obligadas por la ley o en aplicación de sus políticas y prácticas (reflejadas, por ejemplo, en las condiciones de servicio). Los ejemplos más comunes de esas restricciones incluyen la retirada de contenido ilícito o cuestionable, las restricciones de servicios y suspensiones de la cuenta de usuario, y las infracciones de la seguridad de los datos.

[48] La India, Reglamento sobre la Tecnología de la Información (Procedimientos y Salvaguardias para el Bloqueo del Acceso Público a la Información) de 2009, art. 16.

[49] Proyecto de ley de regulación de las facultades de investigación (2015), disp. 84, párr. 2.

[50] Sudáfrica, Regulación de la Interceptación de las Comunicaciones y Provisión de Información Relacionada con la Comunicación, Ley núm. 70/2002, art. 42, párr 1.

[51] Sudáfrica, Ley de Lugares de Importancia Estratégica (Ley núm. 102/1980), art. 10, párr. c).

68. En virtud del artículo 2, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos, los Estados partes deben velar por que toda persona cuyos derechos reconocidos en el Pacto hayan sido vulnerados disponga de un recurso efectivo. En los Principios Rectores sobre las Empresas y los Derechos Humanos se prevé que las empresas deberían proporcionar mecanismos de reparación y de reclamación legítimos, accesibles, previsibles, equitativos, compatibles con los derechos, transparentes, basados en el diálogo y la participación y que sean una fuente de aprendizaje continuo[52]. No obstante, hay muy poca información sobre la forma en que esos elementos deben ponerse en práctica o evaluarse en el contexto de la tecnología de la información y las comunicaciones. Por ejemplo, la retirada indebida de determinados enlaces web de los resultados de una búsqueda podría requerir que el buscador restableciera esos enlaces. No obstante, no queda claro cómo deben concebirse y aplicarse los mecanismos de queja o de recurso para asegurar que esas retiradas se identifiquen, evalúen y reparen eficazmente. La base de clientes enormemente dispersa de los buscadores complica aún más dicha concepción. Tampoco está claro si las empresas deben proporcionar reparaciones adicionales, como indemnizaciones económicas por lucro cesante durante el período de retirada, o garantías de no repetición.

69. Para hacer cumplir las condiciones de servicio, las empresas no siempre cuentan con suficientes procedimientos para que los usuarios puedan oponerse a las decisiones de retirada de contenidos o desactivación de una cuenta cuando consideren que esa acción es un error o el resultado de campañas de identificación abusivas. También pueden resultar útiles otras investigaciones que examinan las mejores prácticas relativas a la forma en que las empresas comunican decisiones sobre la aplicación de las condiciones de servicio y a la manera de aplicar mecanismos de recurso.

70. También se cuestiona el alcance de la responsabilidad de la empresa en la reparación. ¿En quién recae la carga de reparar las retiradas incorrectas o las solicitudes de datos cuando las empresas interpretan o aplican de forma demasiado estricta las leyes nacionales pertinentes? Cuando los productos o servicios de una empresa se utilizan para cometer abusos de derechos humanos, ¿qué grado de causalidad desencadena la obligación de ofrecer una reparación? Cuando las empresas se enfrentan a denuncias de irregularidades, ¿existe la obligación de realizar investigaciones internas y, en ese caso, deben efectuarse esas investigaciones con arreglo a determinadas normas? Cuando una restricción afecta a personas en distintos países, ¿cuál es la jurisdicción competente para examinar las vías de recurso? Esas preguntas reflejan la incertidumbre que enfrentan las víctimas de violaciones de los derechos humanos en situaciones en que la conducta del Estado y las empresas están interrelacionadas.

71. La función que corresponde al Estado a la hora de completar o regular los mecanismos de reparación que ofrecen las empresas también requiere un análisis más detenido. A menudo, los consumidores perjudicados por la actividad empresarial tienen a su disposición procedimientos civiles y formas de reparación judicial, pero suelen resultar engorrosos y onerosos. Las alternativas pueden incluir los mecanismos de denuncia y reclamación establecidos y gestionados por organismos de protección del consumidor y reguladores del sector. Varios Estados también han establecido mecanismos internos de reparación o de reclamación: la India, por ejemplo, exige que las empresas que posean, traten o manejen datos personales confidenciales nombren empleados que se ocupen de "las discrepancias y reclamaciones […] con respecto al procesamiento de la información"[53].

[52] Principios Rectores, cap. III, párr. 31, apdo. a).

[53] La India, Ley de Tecnología de la Información, 2008, art. 43. a); Reglamento sobre la Tecnología de la Información (Prácticas de seguridad y procedimientos razonables e información o datos personales confidenciales) de 2011, art. 5, apdo. 9.

V. Desarrollo temático ulterior

72. Habida cuenta de la variedad de actividades privadas relativas a las tecnologías de la información y las comunicaciones que delimitan el ejercicio de la libertad de opinión y de expresión en línea e influyen en él, el Relator Especial se centrará en las obligaciones de los Estados y las responsabilidades de las empresas en esferas concretas de interés. Las cuestiones jurídicas y políticas planteadas anteriormente orientarán la presentación de informes temáticos, las comunicaciones con los Gobiernos, las visitas a países y empresas, las consultas regionales y de expertos y otros trabajos.

73. Entre las prioridades del Relator Especial para el estudio temático y la orientación cabe citar las siguientes.

Restricciones a la prestación de servicios de telecomunicaciones e Internet

74. Cada vez es más frecuente que los Gobiernos exijan a las entidades privadas que prestan servicios de telecomunicaciones e Internet que cumplan con sus exigencias de censura. Además de las prácticas de filtrado de contenidos en la red, los Estados obligan o presionan a las empresas para que cierren redes o bloqueen servicios completos. Esa tendencia requiere más documentación y examen. La labor futura se concentrará en examinar leyes, políticas y medidas extralegales que posibilitan a los Gobiernos imponer tales restricciones, así como sus costos y consecuencias. El Relator Especial también examinará las responsabilidades de las empresas de responder a esas medidas de manera que se respeten los derechos, se mitiguen los daños y se proporcionen vías de reparación cuando se produzcan abusos.

Restricciones de contenido con arreglo a las condiciones de servicio y las normas de la comunidad

75. Los agentes privados se enfrentan a presiones considerables de los Gobiernos y las personas para restringir las manifestaciones que se consideren como extremismo u odio, hostilidad o acoso. Los agentes privados también pueden tener por objeto fomentar en sus plataformas lo que consideran el discurso civil, reglamentar el acceso mediante requisitos como el de facilitar el nombre real y otras políticas de registro, mostrar determinados contenidos o darles prioridad por razones comerciales. La labor futura evaluará las posibilidades de que se produzca un abuso de las iniciativas privadas por parte del Estado, el efecto de medidas privadas sobre la libertad de expresión, y las obligaciones y responsabilidades pertinentes en materia de derechos humanos. Esa información no solo se centrará en las funciones de las redes sociales y los buscadores, sino también en agentes menos conocidos como el comercio electrónico y los intermediarios financieros.

Responsabilidad derivada del alojamiento de contenidos

76. Cada vez se responsabiliza más a los intermediarios del contenido que permiten alojar a terceros, ya sea a través de los regímenes de responsabilidad de los prestadores de servicios de intermediación o de los requisitos de censura. Las razones comúnmente citadas para esas restricciones incluyen la ciberseguridad, el derecho de autor, la difamación y la protección de los datos. En el futuro, se examinará el alcance legítimo de esas justificaciones, la necesidad de acompañarlas de restricciones, y la falta de garantías procesales en los marcos existentes para retirar el contenido de terceros. También se examinarán las fuentes y modalidades de responsabilidad de los intermediarios en determinados contextos y regiones y se tratará de extraer los principios y prácticas fundamentales aplicables a fin de asegurar la capacidad de los intermediarios para promover y proteger la libertad de expresión.

Censura y vigilancia del sector

77. Las empresas privadas contribuyen en gran medida al desarrollo, la producción y la transferencia de equipo físico y programas informáticos que los Gobiernos pueden utilizar para potenciar cumplimiento de la ley, los servicios de inteligencia y la seguridad pública. Si bien esos instrumentos pueden tener fines legítimos, con frecuencia son utilizados por los Gobiernos para fines de censura y vigilancia excesiva. Los trabajos futuros examinarán esas cuestiones a través del marco de derechos humanos y promoverán la diligencia debida a la hora de determinar la utilización de esas tecnologías con fines que menoscaben la libertad de expresión.

Intentos de socavar la seguridad digital

78. Las empresas que transmiten, almacenan o generan comunicaciones y otros tipos de datos de los usuarios, en particular los proveedores de servicios de Internet y de telecomunicaciones y las plataformas para alojar contenidos, se enfrentan a crecientes exigencias de las fuerzas del orden y de seguridad en cuanto al acceso a la información de sus clientes. La labor futura tratará de encontrar enfoques que puedan maximizar el alcance de la libertad de expresión al tiempo que abordan los intereses gubernamentales legítimos en materia de seguridad nacional y orden público.

Acceso a Internet

79. Los miles de millones de personas que están conectadas en línea disfrutan del acceso a información e ideas que se niegan a otros tantos que carecen de la infraestructura o del entorno político, de seguridad, jurídico o social necesarios para la conectividad. A medida que el sector privado redoble sus esfuerzos para empoderar a esos miles de millones de personas dándoles acceso a la información y las ideas, será fundamental asegurar que ese acceso sea libre, abierto y seguro. La labor futura examinará cuestiones relacionadas con el acceso y la participación del sector privado y la inversión destinada a garantizar la asequibilidad y la accesibilidad, teniendo en cuenta, en particular, a los grupos marginados.

Gobernanza de Internet

80. Los resultados de la Cumbre Mundial sobre la Sociedad de la Información demostraron el constante y amplio apoyo de que goza la idea de poner la gobernanza de Internet en manos de múltiples interesados. No obstante, el modelo existente se enfrenta a un aumento de la presión en forma de políticas nacionales específicas (tales como la localización de datos) y estrategias como la "cibersoberanía". Además, existe una necesidad persistente de mantener o aumentar la participación de los derechos humanos en todos los niveles de la gobernanza, incluido el establecimiento de normas técnicas, y de velar por que los marcos de gobernanza de Internet y las iniciativas de reforma tengan en cuenta las necesidades de las mujeres, las minorías sexuales y otras comunidades vulnerables.

81. Durante la labor futura, el Relator Especial prestará especial atención al desarrollo jurídico (legislativo, normativo y judicial) a nivel nacional y regional. En ese contexto, el Relator Especial insta a todas las partes interesadas a que, por su propio interés, recopilen esos materiales para futuras comunicaciones y presentaciones de informes, y las alienta a que reúnan y presenten ese material en el curso de esa labor.

VI. Conclusiones y recomendaciones

82. **El sector de la tecnología de la información y las comunicaciones está envuelto en un rápido y permanente desarrollo, actualizando constantemente la tecnología y digitalizando la vida cotidiana. Como resultado, abordar las cuestiones jurídicas y de**

política centrándose en las actuales lagunas normativas entraña un cierto riesgo de ignorar tendencias incipientes o que aún no se han manifestado. Esa es una característica natural de la era digital, pero incluso con los rápidos cambios tecnológicos, el entorno digital seguirá estando animado por persistentes amenazas contra la libertad de opinión y de expresión. Esas amenazas incluyen el control, o los intentos por lograrlo, de las fuentes de información por los Gobiernos, mediante el uso de herramientas de censura contra los servicios y la infraestructura en línea; la lucha de las empresas para promover sus productos y servicios en entornos hostiles a la libertad de expresión; la incapacidad de muchas empresas para garantizar la promoción y la protección de los derechos en su búsqueda de intereses comerciales; y las exigencias, a menudo contradictorias, de las personas a las que las empresas no solo proporcionan seguridad, sino también conveniencia, conectividad e integración en una comunidad. Conforme avance el proyecto que explora las responsabilidades de la tecnología de la información y las comunicaciones, el Relator Especial necesitará expertos sobre el terreno —en el Gobierno, el sector privado, la sociedad civil, la comunidad técnica y el mundo académico— para que le ayuden a realizar análisis y presentar informes que respondan a los problemas actuales en la zona en que la tecnología y de la libertad de expresión entran en contacto y a las características a largo plazo de la era digital.

83. **El Relator Especial alienta enérgicamente a todos los interesados, ya sean agentes estatales, empresas del sector privado u organizaciones de la sociedad civil y particulares, a que participen activamente en la elaboración de los próximos proyectos. En particular, alienta a las partes interesadas de los países menos adelantados y las comunidades vulnerables a que compartan perspectivas sobre el impacto que el sector de la tecnología de la información y las comunicaciones puede tener en el disfrute de los derechos y la función que pueden desempeñar los Estados a la hora de obstaculizar o promover esos derechos.**

84. **Aunque el proyecto está en sus etapas iniciales, es fundamental que los Estados y los agentes del sector privado adopten medidas para asegurar el respeto por la libertad de opinión y de expresión. Esas medidas deberían incluir, como mínimo, las siguientes, con un análisis más detenido a lo largo de todo el mandato del Relator Especial.**

Estados

85. **Los Estados tienen la responsabilidad primordial de proteger y respetar el derecho a ejercer la libertad de opinión y de expresión. En el contexto de la tecnología de la información y las comunicaciones, eso significa que los Estados no deben exigir o presionar al sector privado para que adopte medidas que interfieran de manera innecesaria o desproporcionada en la libertad de expresión, ya sea mediante leyes, políticas o medios extralegales. Las exigencias, solicitudes y otras medidas encaminadas a retirar contenido digital o acceder a la información de los clientes deben basarse en leyes promulgadas de forma válida, estar sujetas a supervisión externa e independiente, y demostrar que son medios necesarios y proporcionales para alcanzar uno o más objetivos en virtud del artículo 19, párrafo 3, del Pacto Internacional de Derechos Civiles y Políticos. En el contexto concreto de la regulación del sector privado, las leyes y políticas del Estado deben ser aprobadas y aplicadas de manera transparente.**

86. **Los Gobiernos también deben adoptar y aplicar leyes y políticas que protejan el desarrollo del sector privado y el desarrollo de medidas técnicas, productos y servicios que promuevan la libertad de expresión. Deben asegurar la adopción de medidas legislativas, la formulación de políticas y otros procesos de establecimiento de normas**

relativas a los derechos y las restricciones de Internet para proporcionar al sector privado, la sociedad civil, la comunidad técnica y el mundo académico oportunidades significativas para participar y realizar aportaciones.

Sector privado

87. **Es innegable que los Estados someten a presiones al sector de la tecnología de la información y las comunicaciones privadas que, a menudo, suelen conducir a graves restricciones de la libertad de expresión. No obstante, el sector privado también desempeña funciones independientes que pueden promover o restringir los derechos, una cuestión que el Consejo de Derechos Humanos reconoció con la aprobación de los Principios Rectores sobre las Empresas y los Derechos Humanos en 2011 como orientación general en esa esfera. La evaluación de las empresas privadas debería basarse en las medidas que adopten tanto para promover como para menoscabar la libertad de expresión, incluso en entornos hostiles, desfavorables para los derechos humanos.**

88. **Entre las medidas más importantes que deberían adoptar los agentes del sector privado está la elaboración y aplicación de procedimientos transparentes de evaluación de los derechos humanos. Deberían elaborar y aplicar políticas que tengan en cuenta las posibles repercusiones de sus actividades sobre los derechos humanos. En esas evaluaciones se debería analizar de forma crítica la amplia gama de actividades del sector privado en las que esos actores participan, como la formulación y aplicación de las condiciones de servicio y las normas de la comunidad sobre la libertad de expresión de los usuarios, incluida la externalización de esa aplicación; la repercusión de los productos, servicios y otras iniciativas comerciales sobre la libertad de expresión de los usuarios a medida que se están elaborando, incluidas las opciones de diseño e ingeniería, y planes para la fijación de precios diferenciales o para el acceso a los contenidos y servicios de Internet; y los efectos que tiene sobre los derechos humanos la realización de transacciones con posibles clientes gubernamentales, como operar la infraestructura de telecomunicaciones o transferir tecnologías de regulación de contenido o de vigilancia.**

89. **También es fundamental que las entidades privadas garanticen la mayor transparencia posible en las políticas, normas y medidas que afectan a la libertad de expresión y otros derechos fundamentales. Las evaluaciones de los derechos humanos deberían ser objeto de un examen transparente en lo que se refiere a sus metodologías, su interpretación de las obligaciones jurídicas y el peso que esas evaluaciones tienen en las decisiones empresariales. La transparencia es importante en todos los ámbitos, incluso en el contexto de la regulación del contenido, y debería comprender información sobre la presentación de solicitudes gubernamentales para la retirada de contenido.**

90. **Más allá de la adopción de políticas, las entidades privadas también deberían alcanzar compromisos en pro de la libertad de expresión en la formulación de políticas internas, la gestión de productos, el desarrollo empresarial, la capacitación del personal y otros procesos internos pertinentes. El Relator Especial procurará estudiar las políticas y toda la gama de medidas de aplicación de diversas maneras, incluidas las visitas a empresas.**

Organizaciones internacionales y procesos de múltiples interesados

91. **Como se ha demostrado en el presente informe, muchas organizaciones internacionales contribuyen a los procesos de gobernanza de la tecnología de la información y las comunicaciones. Es fundamental que esas organizaciones ofrezcan un acceso público efectivo a las políticas, las normas, los informes y cualquier otra**

información relativa a la gobernanza de Internet creada o generada por la organización y sus miembros, entre otras cosas facilitando el acceso gratuito a los recursos en línea y las iniciativas de educación pública. De manera más general, el proceso de gobernanza de Internet por parte de múltiples interesados ha sido un motor importante para las políticas de apoyo a la libertad de expresión. Teniéndolo presente, las organizaciones internacionales deberían garantizar la participación efectiva de la sociedad civil en la formulación de políticas y otros procesos de elaboración de normas, incluso mediante el aumento de la presencia de expertos técnicos que tengan en cuenta las preocupaciones en materia de derechos humanos.