



Asamblea General

Distr. general
17 de mayo de 2019
Español
Original: inglés

Consejo de Derechos Humanos

41^{er} período de sesiones

24 de junio a 12 de julio de 2019

Tema 3 de la agenda

**Promoción y protección de todos los derechos humanos,
civiles, políticos, económicos, sociales y culturales,
incluido el derecho al desarrollo**

Derechos a la libertad de reunión pacífica y de asociación

Informe del Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación*

Resumen

En el presente informe, el Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación, Clément Nyaletsossi Voule, expone las oportunidades y los problemas que hay en el ámbito de esos derechos en la era digital. El Relator Especial pretende ofrecer orientación sobre las mejores fórmulas para mantener y aprovechar al máximo estas oportunidades y hacer frente a los riesgos.

El Relator Especial concluye que el derecho internacional protege los derechos a la libertad de reunión pacífica y de asociación con independencia de que se ejerzan personalmente, con los medios técnicos contemporáneos o con los que se inventen en el futuro. Las normas y los principios de derechos humanos vigentes no solo deberían dictar el comportamiento de los Estados, sino también constituir el marco por el que se rigieran las empresas de tecnología digital en lo tocante al diseño, el control y la gestión de las tecnologías digitales.

* Se acordó publicar el presente informe tras la fecha de publicación prevista debido a circunstancias que escapan al control de quien lo presenta.



I. Introducción

1. El Relator Especial sobre los derechos a la libertad de reunión pacífica y de asociación presenta este informe al Consejo de Derechos Humanos en su 41^{er} período de sesiones, en cumplimiento de las resoluciones del Consejo 15/21 y 32/32. En la sección II, el Relator Especial reseña algunas de las actividades que ha realizado en el tiempo transcurrido desde que presentó su informe al Consejo, el 18 de junio de 2018. En las secciones III y IV, trata el ejercicio de los derechos a la libertad de reunión pacífica y de asociación en la era digital. Las conclusiones y las recomendaciones se detallan en la sección V.

2. La era digital ha abierto un nuevo espacio para el disfrute de los derechos a la libertad de reunión pacífica y de asociación. Hay numerosos ejemplos de todo el mundo que demuestran el poder que tiene la tecnología digital en manos de personas que desean unirse para promover la democracia, la paz y el desarrollo. Sin embargo, la revolución digital también ha traído una serie de riesgos y amenazas nuevos para esos derechos.

3. El Relator Especial ha observado que, en el último decenio, los Estados han utilizado la tecnología para silenciar, vigilar y acosar a los disidentes, la oposición política, los defensores de los derechos humanos, los activistas y los manifestantes, y para manipular a la opinión pública. Los gobiernos ordenan interrupciones del servicio de Internet con más frecuencia y bloquean sitios web y plataformas antes de momentos democráticos decisivos, como elecciones y manifestaciones. El auge de las leyes y las políticas dirigidas a combatir la ciberdelincuencia también ha dado pie a que se castigue y vigile a los activistas y los manifestantes en muchos países del mundo. Aunque el empleo que se pueda dar a esa tecnología para promover el terrorismo, incitar a la violencia y manipular elecciones es un problema mundial auténtico y grave, esas amenazas se suelen aducir como pretextos para reprimir a la nueva sociedad civil digital.

4. Entretanto, las plataformas digitales dominantes, como Facebook, Twitter y YouTube, han pasado a controlar la capacidad que tiene la población de disfrutar de los derechos a la libertad de reunión pacífica y de asociación y poseen un poder inmenso para decidir si los particulares y los agentes de la sociedad civil pueden acceder al espacio democrático y participar en él.

5. Las oportunidades y las amenazas que entrañan las tecnologías digitales para el ejercicio de la libertad de reunión pacífica y de asociación aumentarán a medida que las tecnologías emergentes, como la Internet de las cosas y la inteligencia artificial, se desarrollen y se hagan más comunes. Habiéndose inspirado en otros informes elaborados por otros titulares de mandatos de procedimientos especiales competentes¹, el Relator Especial pretende, en el presente informe, proporcionar orientación sobre las mejores fórmulas para mantener y aprovechar al máximo las oportunidades que ofrecen esas tecnologías y hacer frente a sus riesgos. El presente informe no aspira a ser exhaustivo. Su finalidad es, más bien, ofrecer una síntesis introductoria de los problemas más acuciantes, que se trataran con más detenimiento en informes y comunicaciones futuros.

6. Durante la redacción del presente informe, el Relator Especial se benefició de un proceso público de aportación de ideas y de consulta. En noviembre de 2018, solicitó que se le aportaran ideas para el informe. En la fecha de publicación de este, había recibido 10 comunicaciones de organizaciones de la sociedad civil, 2 de empresas de tecnología digital y otras 2 de gobiernos. El Relator Especial organizó una reunión de expertos que se celebró en Ginebra, los días 11 y 12 de octubre de 2018. También mantuvo consultas regionales con organizaciones de la sociedad civil en Bangkok (21 de diciembre de 2018), Beirut (18 de enero de 2019), Ciudad de México (24 y 25 de enero de 2019), Silicon Valley (California (Estados Unidos de América)) (27 a 30 de enero de 2019) y Nairobi (21 y 22 de febrero de 2019). Mantuvo reuniones con expertos en Copenhague (6 de marzo de 2019) y organizó una consulta con diversos gobiernos en Ginebra (20 de marzo de 2019). Además, celebró una consulta conjunta con el Relator Especial sobre la promoción y protección del

¹ Véanse, por ejemplo, A/HRC/17/27, A/71/373, A/HRC/23/40 y A/HRC/38/47.

derecho a la libertad de opinión y de expresión, David Kaye, los días 18 y 19 de noviembre de 2108, en Bangkok.

II. Actividades del Relator Especial

A. Visitas a los países

7. El Relator Especial visitó Túnez, del 17 al 28 de septiembre de 2018 (véase A/HRC/41/41/Add.3), y Armenia, del 7 al 16 de noviembre de 2018 (A/HRC/41/41/Add.4). Da las gracias a ambos Gobiernos por la cooperación que le han brindado antes de las visitas y en el curso de ellas.

B. Comunicaciones

8. El Relator Especial envió un total de 130 comunicaciones a 60 Estados entre el 1 de abril de 2018 y el 25 de abril de 2019. Sus observaciones sobre las comunicaciones enviadas a los Estados, y las respuestas recibidas, figuran en una adición del presente informe (A/HRC/41/41/Add.1).

C. Participación en actos diversos

9. El Relator Especial participó en los siguientes actos, entre muchos otros:

- a) Una visita académica al Brasil, del 16 al 20 de julio de 2018;
- b) La Conferencia de Cooperación Suiza para el desarrollo sobre la disminución del espacio cívico y la creación de un entorno propicio para la sociedad civil, celebrada en Berna, los días 13 y 14 de septiembre de 2018;
- c) El 63^{er} período de sesiones de la Comisión Africana de Derechos Humanos y de los Pueblos, celebrado en Banjul, del 24 al 26 de octubre de 2018, y su 64^o período de sesiones, celebrado en Sharm El Sheikh (Egipto), el 24 de abril de 2019;
- d) La sesión de la Cumbre Mundial de Defensores de los Derechos Humanos titulada “Volver a ampliar nuestro espacio: hacer frente a la disminución del espacio, las leyes restrictivas y las limitaciones de financiación – situación actual y cuestiones principales para los próximos 20 años”, que tuvo lugar en París, el 30 de octubre de 2018;
- e) La conferencia “Civic Space under Attack” (“El ataque contra el espacio cívico”), celebrada en el Centre for Global Challenges de la Universidad de Utrecht (Países Bajos), el 21 de noviembre de 2018;
- f) El Foro sobre las Empresas y los Derechos Humanos, celebrado en Ginebra, del 26 al 28 de noviembre de 2018;
- g) El acto que celebró la Organización Internacional de la Francofonía para conmemorar el 70^o aniversario de la Declaración Universal de Derechos Humanos, en Nueva York, el 10 de diciembre de 2018;
- h) Los diálogos regionales con la sociedad civil y los gobiernos de la región de Asia y el Pacífico sobre las secuelas que tiene, en las elecciones, la restricción del espacio cívico y de la libertad de opinión, expresión y reunión, organizados por el Foro Asiático sobre Derechos Humanos y Desarrollo y celebrados en Bangkok, los días 20 y 21 de diciembre de 2018;
- i) La conferencia anual de Frivillighet Norge, la asociación noruega de organizaciones no gubernamentales (ONG), sobre el tema “¿Pueden las ONG salvar la democracia?”, celebrada en Oslo, el 14 de febrero de 2019;
- j) La Conferencia Internacional de Reivindicación Común del Espacio Cívico, celebrada en Copenhague, los días 4 y 5 de marzo de 2019;

k) El 172º período de sesiones de la Comisión Interamericana de Derechos Humanos, celebrado en Kingston, del 6 al 10 de mayo de 2019.

III. Los derechos a la libertad de reunión pacífica y de asociación en la era digital: marco jurídico internacional

A. Obligaciones de los Estados

10. Los derechos a la libertad de reunión pacífica y de asociación están amparados por el artículo 20 de la Declaración Universal de Derechos Humanos y los artículos 21 y 22 del Pacto Internacional de Derechos Civiles y Políticos. El Consejo de Derechos Humanos ha recalcado que los Estados tienen la obligación de respetar esos derechos y protegerlos plenamente, tanto en línea como fuera de línea². Asimismo, la Asamblea General ha exhortado a todos los Estados “a que velen por que los mismos derechos que tienen las personas cuando no están conectadas, incluidos los derechos a la libertad de expresión, de reunión pacífica y de asociación, estén plenamente protegidos también cuando estén en línea, de conformidad con el derecho de los derechos humanos”³.

11. En informes anteriores, el titular del mandato ha reconocido que la tecnología digital es esencial para ejercer los derechos a la libertad de reunión pacífica y de asociación⁴. La tecnología sirve tanto de medio que facilita el ejercicio de esos derechos sin estar conectado como de espacio virtual en el que se los puede ejercer activamente⁵. Ciertamente, esas tecnologías son instrumentos importantes para los organizadores que desean movilizar a un grupo grande de personas de manera rápida y eficaz, y con poco gasto, y también sirven de espacios en línea a los grupos de personas que están marginadas por la sociedad y sufren limitaciones para actuar en los espacios materiales⁶. El titular del mandato ha exhortado a los Estados a que velen por que todos tengan acceso a Internet y puedan usarla para ejercer esos derechos, y a que faciliten la constitución de asociaciones⁷ y la realización de reuniones⁸ en línea con arreglo a las normas de derechos humanos. El Consejo de Derechos Humanos ha reconocido que aunque, en general, suele entenderse por reunión una agrupación física de personas, la protección de los derechos humanos, incluidos los derechos a la libertad de reunión pacífica, puede extenderse a agrupaciones análogas en Internet⁹.

12. Si bien esos derechos no son absolutos, la libertad de acceso a las tecnologías digitales y de uso de estas para ejercer los derechos a la libertad de reunión pacífica y de asociación se debería considerar la regla, y las limitaciones, la excepción. La regla general debería ser la de permitir el uso abierto y libre de Internet y otras herramientas digitales¹⁰. En la resolución 15/21 del Consejo de Derechos Humanos se aclara que, para ser admisibles, las limitaciones deberían estar “prescritas por la ley [y ser] necesarias en una sociedad democrática en razón de la seguridad nacional, el orden público, la protección de la salud o de la moral públicas o la protección de los derechos y libertades de los demás”¹¹. Cuando se apliquen restricciones, “los Estados deben demostrar su necesidad y adoptar únicamente las medidas que resulten proporcionales a la consecución de los legítimos objetivos para lograr una protección constante y eficaz de los derechos del Pacto. En ningún

² Véase la resolución 38/7 del Consejo de Derechos Humanos.

³ Véase la resolución 73/173 de la Asamblea General.

⁴ Véanse A/HRC/20/27 y A/HRC/38/34.

⁵ Véase A/HRC/29/25/Add.1, párr. 53.

⁶ Véase A/HRC/35/28.

⁷ Véase A/HRC/20/27, párr. 52.

⁸ Véase A/HRC/29/25/Add.1, párr. 34.

⁹ Véase la resolución 38/11 del Consejo de Derechos Humanos.

¹⁰ Véase A/HRC/23/39, párr. 76.

¹¹ Véase la resolución 15/21 del Consejo de Derechos Humanos.

caso se deben aplicar las restricciones o invocarse de una manera que menoscabe la esencia de un derecho del Pacto”¹².

13. Los Estados no solo tienen la obligación negativa de no injerirse indebidamente en el ejercicio de los derechos a la libertad de reunión pacífica y de asociación sino la obligación positiva de favorecer y proteger el ejercicio de esos derechos con arreglo a las normas internacionales de derechos humanos¹³. A tal fin, velarán por que todos disfruten de los derechos a la libertad de reunión pacífica y de asociación sin discriminación alguna por motivos de raza, color, sexo, idioma, religión, opinión política o de otra índole, origen nacional o social, posición económica, nacimiento o cualquier otra condición social (artículo 2, párrafo 1, del Pacto Internacional de Derechos Civiles y Políticos)¹⁴.

14. En la era digital, la obligación positiva de favorecer el ejercicio de los derechos a la libertad de reunión pacífica y de asociación incluye las iniciativas destinadas “a cerrar las brechas digitales, especialmente la existente entre los géneros, y a aumentar el uso de la tecnología de la información y las comunicaciones, para promover el pleno disfrute de los derechos humanos para todos”¹⁵. La obligación de proteger los derechos a la libertad de reunión pacífica y de asociación requiere que se adopten medidas positivas para prevenir las actividades de agentes no estatales, como las empresas, que se pudieran injerir indebidamente en el ejercicio de esos derechos¹⁶.

15. Cuando se limiten indebidamente los derechos a la libertad de reunión pacífica y de asociación, la(s) víctima(s) debería(n) poder ejercer su derecho a un recurso eficaz y obtener reparación. El Consejo de Derechos Humanos ha exhortado a los Estados a que garanticen “recursos eficaces en los casos de violaciones de los derechos humanos, en particular las relacionadas con Internet, de conformidad con sus obligaciones internacionales”¹⁷.

16. Las vulneraciones de los derechos a la libertad de reunión pacífica y de asociación también pueden estorbar el disfrute, tanto en línea como fuera de línea, de otros derechos humanos; entre ellos, el derecho a la privacidad y el derecho a la libertad de opinión y de expresión, que están íntimamente ligados al disfrute de los derechos a la libertad de reunión pacífica y de asociación. También se pueden ver perjudicados otros derechos, particularmente los económicos, sociales y culturales.

B. Función y responsabilidades de las empresas

17. En la era digital, el ejercicio de los derechos a la libertad de reunión pacífica y de asociación ha pasado a depender, en gran medida, de empresas, cuyas obligaciones jurídicas, política, normativa técnica, modelo económico y algoritmos pueden afectar a esas libertades. Las empresas propietarias de las plataformas en línea y las redes sociales, en particular, poseen un poder considerable para influir en la manera en que se disfrutaban y ejercen el derecho a la libertad de reunión pacífica y el derecho a la libertad de asociación, sobre todo en los países donde se coarta gravemente el ejercicio “fuera de línea” de estos derechos. Sin embargo, esas plataformas se han convertido en nuevos instrumentos para intimidar y vigilar a los agentes de la sociedad civil.

¹² Comité de Derechos Humanos, observación general núm. 31 (2004), sobre la índole de la obligación jurídica general impuesta a los Estados partes en el Pacto, párr. 6.

¹³ Véanse A/HRC/17/27, párr. 66, y A/HRC/29/25/Add.1.

¹⁴ Véase también el artículo 26 del Pacto.

¹⁵ Véase la resolución 38/7 del Consejo de Derechos Humanos, párr. 5. Esta idea figura también en la Agenda 2030 para el Desarrollo Sostenible, en la que se enuncian los compromisos de “aumentar significativamente el acceso a la tecnología de la información y las comunicaciones y esforzarse por proporcionar acceso universal y asequible a Internet en los países menos adelantados de aquí a 2020” (objetivo 9.c) y de “mejorar el uso de la tecnología instrumental, en particular la tecnología de la información y las comunicaciones, para promover el empoderamiento de las mujeres” (objetivo 5.b). Véase también A/HRC/35/9.

¹⁶ Véanse el artículo 2, párrafo 2, del Pacto y la observación general núm. 31 del Comité de Derechos Humanos.

¹⁷ Véase la resolución 38/7 del Consejo de Derechos Humanos.

18. Los Principios Rectores sobre las Empresas y los Derechos Humanos constituyen el marco mundial para analizar las responsabilidades que tienen las empresas de tecnología digital de respetar los derechos humanos¹⁸. En los Principios Rectores 11 a 24 se reconoce que las empresas “deben respetar los derechos humanos”, por lo que deben abstenerse de infringir los derechos humanos de terceros, y hacer frente a las consecuencias negativas en los derechos humanos en las que tengan alguna participación. A fin de cumplir esa obligación, las empresas deben tener unas políticas y unos procedimientos de derechos humanos, que incluyan el compromiso oficial de cumplir su deber de respetar estos derechos; un procedimiento que garantice la diligencia debida en cuestiones de derechos humanos y permita determinar, prevenir y mitigar las consecuencias que tenga su actividad en los derechos humanos y rendir cuentas por la manera en que se traten esas consecuencias; y procedimientos que permitan reparar¹⁹ todas las consecuencias negativas en los derechos humanos que provoque o que favorezca su actividad.

19. En relación con lo anterior, el titular del mandato suscribe la opinión del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, según la cual “el derecho de los derechos humanos ofrece a las empresas los instrumentos necesarios para que puedan expresar sus posiciones de manera que se respeten los principios democráticos y oponerse a las exigencias autoritarias”²⁰. Asimismo, el Consejo de Derechos Humanos ha reconocido que “el derecho internacional de los derechos humanos debe guiar a los actores del sector privado y constituir la base de sus políticas”²¹.

20. Los Estados, por su parte, tienen la obligación de proteger los derechos humanos y prevenir que se los vulnere como consecuencia de la acción o la omisión de terceros, como las empresas. Según el primer principio rector, los “Estados deben proteger contra las violaciones de los derechos humanos cometidas en su territorio y/o su jurisdicción por terceros, incluidas las empresas. A tal efecto deben adoptar las medidas apropiadas para prevenir, investigar, castigar y reparar esos abusos mediante políticas adecuadas, actividades de reglamentación y sometimiento a la justicia”²².

IV. Ejercicio de los derechos a la libertad de reunión pacífica y de asociación en la era digital: oportunidades y problemas

A. Oportunidades digitales

21. Las tecnologías digitales han creado oportunidades notables de ejercer los derechos a la libertad de reunión pacífica y de asociación. Al ser tanto instrumentos mediante los cuales se pueden ejercer esos derechos “fuera de línea” como espacios donde las personas pueden actuar para celebrar reuniones y constituir asociaciones en línea²³, las tecnologías digitales han ampliado enormemente la capacidad que tienen los particulares y los grupos de la sociedad civil de organizarse y movilizarse, promover los derechos humanos e innovar en materia de transformación social.

22. Es bien sabida la función que pueden cumplir las redes sociales de movilizar a la población para que salga a la calle. Durante su visita a Armenia en 2018, por ejemplo, el Relator Especial oyó varios relatos sobre la función decisiva que habían desempeñado las plataformas de redes sociales, los instrumentos de emisión en directo y en continuo y las aplicaciones de comunicación en la revolución “de terciopelo” de dicho año, que había provocado la dimisión del Primer Ministro. Se habían utilizado las etiquetas #MyStep y #MerzhirSerzhin para intercambiar información, movilizar a los ciudadanos y obtener su

¹⁸ Véase A/HRC/17/31.

¹⁹ Véase A/72/162, párr. 86 c).

²⁰ Véase A/HRC/38/35.

²¹ Véase la resolución 38/7 del Consejo de Derechos Humanos.

²² Véase A/HRC/17/31.

²³ Véase A/HRC/29/25/Add.1.

apoyo, eludiendo los medios de difusión controlados por el Gobierno. El movimiento #BlackLivesMatter, que lucha por la igualdad racial, empezó con el uso de esa etiqueta para movilizar a diversos segmentos de población, tanto en los Estados Unidos como en otras partes del mundo, para que se unieran a unas grandes manifestaciones de protesta contra la violencia policial y el racismo sistémico que sufrían los afrodescendientes. Muchos movimientos juveniles del mundo se apoyan en las redes sociales, como ejemplifican el #RoadSafetyMovement de Bangladesh, la campaña #FeesMustFall de Sudáfrica y el movimiento global #FridaysForFuture y #ClimateStrikes.

23. Los particulares ya pueden usar los espacios en línea para participar en una sociedad civil conectada virtualmente. Las activistas, por ejemplo, usan Internet para conectarse e intercambiar estrategias, incluso más allá de sus respectivas fronteras, y como espacio de organización²⁴. El movimiento #MeToo es, quizá, el ejemplo reciente más notable. En 2017, unas mujeres que habían sido víctimas de violencia sexual usaron las redes sociales para difundir su historia personal de acoso y abusos sexuales y para reclamar la igualdad de género en el trabajo, con la etiqueta #MeToo. Al parecer, transcurrido un año desde el inicio, la etiqueta ha sido utilizada más de 19 millones de veces²⁵, tanto por las víctimas como por quienes simpatizaban con su causa. Aunque el movimiento empezó en los Estados Unidos, también se unieron a él mujeres de Francia (#BalanceTonPorc), del mundo árabe (#AnaKaman), de la India (#MeTooIndia), de Ucrania (#IAmNotAfraidToSayIt) y de México (#MeTooMexico).

24. Las tecnologías de cifrado y de seudonimización y otros medios de seguridad ha permitido a las personas pertenecientes a grupos minoritarios encontrarse y crear una comunidad. El Consejo de Derechos Humanos ha puesto de relieve que “las soluciones técnicas para asegurar y proteger la confidencialidad de las comunicaciones digitales, en particular las medidas de codificación y anonimato, pueden ser importantes para garantizar el disfrute de los derechos humanos, en particular los derechos a la privacidad, a la libertad de expresión y a la libertad de reunión pacífica y de asociación”²⁶. El Relator Especial afirma que lo mismo sucede en el caso de la organización y el funcionamiento de las asociaciones. Esos instrumentos ofrecen a los particulares y a los agentes de la sociedad civil un espacio en línea seguro para reunirse y conectarse con otros miembros de su grupo, así como para organizar y coordinar actividades, sin injerencias indebidas de terceros ni de los gobiernos²⁷.

25. Mediante el uso de las redes sociales, las peticiones en línea y las plataformas de financiación popular, las organizaciones de la sociedad civil han podido llegar a nuevos públicos, difundir información, atraer miembros y obtener fondos por medios que antiguamente resultaban imposibles o extremadamente caros. Por ejemplo, a raíz del terremoto que hubo en México en 2018, un grupo de ciudadanos se movilizaron en línea mediante la etiqueta #Verificado19S²⁸ para facilitar información fiable y ayudar a las víctimas que necesitaban recursos. En Turquía, organizaciones como Oy ve Ötesi usaron las redes sociales para captar a más de 60.000 voluntarios que se encargarían de vigilar más de 130.000 urnas durante las elecciones generales de noviembre de 2015. En los Estados Unidos, la American Civil Liberties Union recaudó millones de dólares mediante donaciones en línea en un fin de semana para sufragar su labor de defensa de los derechos de los inmigrantes. Asimismo, después de que la Federación de Rusia hubiera impuesto restricciones rigurosas a la sociedad civil para obtener recursos del extranjero, la organización de derechos humanos OVD-Info recurrió a la financiación popular para obtener ayuda y recaudar pequeñas donaciones privadas a nivel nacional²⁹. Además, las tecnologías digitales han cobrado cada vez más importancia para los sindicatos, que

²⁴ Véase A/HRC/35/9, paras. 23 y 24.

²⁵ Pew Research Center, “How social media users have discussed sexual harassment since #MeToo went viral”, 11 de octubre de 2018.

²⁶ Véase la resolución 38/7 del Consejo de Derechos Humanos.

²⁷ Véanse A/HRC/29/32 y A/HRC/38/35/Add.5.

²⁸ #Verified19S.

²⁹ Véase A/HRC/35/28, párr. 62.

recurren a ellas para realizar sus funciones principales, como organizar manifestaciones, mantener el contacto con los afiliados y ofrecer espacios para debatir y tomar decisiones³⁰.

26. Muchos grupos de la sociedad civil han aprovechado la tecnología para innovar en el tratamiento de los problemas sociales. Por ejemplo, el proyecto Landmark³¹ ofrece planos y otros datos fundamentales de dominio público sobre las tierras que poseen y usan colectivamente los pueblos indígenas y las comunidades locales de todo el mundo para garantizar su protección. El proyecto Eyewitness ha ideado tecnologías que incrementan la capacidad que tienen los agentes de la sociedad civil y los particulares de documentar abusos contra los derechos humanos y dejar constancia de ellos³². La elaboración de programas informáticos de código abierto y la concesión de licencias de utilización gratuita de bienes comunes han sido impulsadas, en gran medida, por organizaciones de la sociedad civil como la Fundación Mozilla y Wikimedia. Se han ideado plataformas como Signal y Crabgrass para potenciar la seguridad de las comunicaciones digitales de los grupos de la sociedad civil. Las redes comunitarias de los asentamientos de refugiados o de las poblaciones indígenas son otro ejemplo de innovaciones introducidas por la sociedad civil para hacer frente a los problemas sociales.

27. Las autoridades deberían considerar las tecnologías digitales como “una oportunidad excelente para interactuar con un público amplio y diversificado antes y durante las reuniones pacíficas, con el fin de darle a conocer su papel y funciones, y en definitiva, generar o reforzar la confianza en la población”³³. Asimismo, los Estados deberían reconocer el valor que tiene la tecnología para favorecer el ejercicio de los derechos de la población a la participación en los asuntos públicos. El Relator Especial acoge con agrado las iniciativas que han adoptado muchos gobiernos para crear plataformas en línea mediante las cuales los interesados puedan presentar y recoger firmas para peticiones relativas a políticas gubernamentales y medidas legislativas.

28. Esos ejemplos demuestran que la tecnología digital tiene una amplia gama de usos que favorecen el disfrute de los derechos a la libertad de reunión pacífica y de asociación y la interacción entre las esferas digital y material. El Relator Especial observa que los derechos a la libertad de reunión pacífica y de asociación se suelen ejercer, sin solución de continuidad, tanto en línea como fuera de línea. Por ejemplo, muchas asociaciones tienen oficinas y sus afiliados tratan entre sí cara a cara; pero, al mismo tiempo, usan la tecnología digital para realizar sus actividades cotidianas y como espacio para organizar debates y reuniones en línea. Asimismo, las asociaciones que funcionan principalmente en línea también celebran debates y reuniones presenciales. La proporción de actividades en línea y fuera de línea depende de la composición de la asociación, sus estrategias y sus objetivos. Por expresarlo en términos sencillos, el derecho internacional protege los derechos a la libertad de reunión pacífica y de asociación, con independencia de que se ejerzan personalmente o mediante las tecnologías contemporáneas o las que se inventen en el futuro³⁴.

B. Tendencias de las limitaciones impuestas por los Estados

29. Al Relator Especial le preocupa la variedad de medidas y tácticas que emplean los Estados para controlar e impedir el acceso a la tecnología digital, así como el uso de esta, para ejercer los derechos a la libertad de reunión pacífica y de asociación. Siguen proliferando las leyes que penalizan los contenidos digitales, lo que tiene un efecto sumamente disuasorio en las actividades de defensa de derechos y movilización. Muchas autoridades han recurrido a la interrupción del acceso a las redes y los servicios de

³⁰ Véanse Jeffrey M. Hirsch, “Worker collective action in the digital age”, *West Virginia Law Review*, vol. 117 (2015), págs. 921 a 959, y Klaus Schoemann, “Digital technology to support the trade union movement”, *Open Journal of Social Sciences*, vol. 6, núm. 1 (2018), págs. 67 a 82.

³¹ Véase www.landmarkmap.org.

³² Véase www.eyewitnessproject.org.

³³ Véase A/HRC/23/39, párr. 74.

³⁴ Véase Douglas Rutzen y Jacob Zenn, “Assembly and association in the digital age”, *International Journal of Not-for-Profit Law*, vol. 13, número 4 (diciembre de 2011), pág. 67.

comunicaciones durante las elecciones y manifestaciones públicas, y al bloqueo de sitios web pertenecientes a grupos de la sociedad civil, entre ellos organizaciones de derechos humanos. En una demostración del uso refinado que hacen de los nuevos instrumentos técnicos, algunos Estados, así como terceros con intenciones malévolas, han incrementado la vigilancia digital y el acoso en línea contra los agentes de la sociedad civil, los defensores de los derechos humanos, los dirigentes de la oposición política y los planificadores de reuniones públicas pacíficas. Todo ello ha reducido considerablemente el espacio que tiene la población para defender y promover sus intereses comunes. En concreto, el Consejo de Derechos Humanos se ha declarado preocupado ante “la tendencia emergente a la desinformación y a la imposición de restricciones indebidas que impiden a los usuarios de Internet obtener o difundir información en momentos políticos clave, lo que repercute en la capacidad para organizar y celebrar reuniones”³⁵.

30. En la presente sección se examinan esas actividades de los Estados para determinar si se ciñen a los artículos 21 y 22 del Pacto y a los criterios de análisis pertinentes que se enuncian en ellos.

1. Legalidad

31. Como ya se ha señalado, toda restricción de los derechos a la libertad de reunión pacífica y de asociación debe tener un fundamento jurídico (es decir, debe estar “en conformidad con la ley” o “prescrita por la ley” respectivamente)³⁶, como lo deben tener el mandato y las facultades de la autoridad que imponga la restricción. La propia ley debe ser lo suficientemente precisa como para que una persona pueda determinar si su conducta sería o no contraria a la ella y prever también las posibles consecuencias de una eventual vulneración³⁷.

32. Se aprueban cada vez más leyes en las que se penaliza el acceso a los instrumentos digitales y su utilización, en países diversos. En esas leyes la responsabilidad penal se suele enunciar en términos vagos y mal definidos, que permitan aplicarlas de manera arbitraria o discrecional y dan lugar a inseguridad jurídica. Por ello, incumplen las disposiciones jurídicas relativas a las restricciones admisibles según los artículos 21 y 22 del Pacto. Cabe citar, como ejemplos, las leyes contra la ciberdelincuencia, las leyes antiterroristas, las leyes de vigilancia y las leyes contra las manifestaciones.

Leyes contra la ciberdelincuencia

33. Por ejemplo, la prohibición de usar dispositivos electrónicos para destruir la armonía social o provocar inestabilidad o desorden o alterar o intentar alterar el orden jurídico y el orden público³⁸ que se impone en la Ley de Seguridad Digital de Bangladesh confiere a los funcionarios unas potestades discrecionales excesivas para determinar qué constituye una conducta ilegal y emprender actuaciones penales contra particulares aduciendo razones arbitrarias y subjetivas. Las autoridades podrían calificar las convocatorias de reuniones pacíficas en las redes sociales de intentos de provocar inestabilidad o destruir la armonía social. En otras leyes contra la ciberdelincuencia se confiere a los gobiernos facultades amplísimas para bloquear los sitios web que se consideren críticos con las autoridades, como los pertenecientes a defensores de los derechos humanos³⁹, recurriendo a unos conceptos de seguridad nacional definidos de manera imprecisa.

³⁵ Véase la resolución 38/11 del Consejo de Derechos Humanos.

³⁶ En el artículo 21 del Pacto se dispone que el ejercicio del derecho de reunión pacífica solo podrá estar sujeto a las restricciones previstas por la ley. Y en el artículo 22, párrafo 2, se dispone que “[e]l ejercicio de tal derecho solo podrá estar sujeto a las restricciones previstas por la ley”.

³⁷ Véanse A/HRC/20/27, párr. 16, y A/HRC/31/66, párr. 30.

³⁸ Véase BGD 4/2018, que se puede consultar en <https://spcommreports.ohchr.org/Tmsearch/TMDocuments>.

³⁹ Véase, por ejemplo, EGY 13/2017.

Leyes antiterroristas

34. Los titulares de mandatos han expresado, en varias ocasiones, su preocupación ante la terminología excesivamente vaga que se suele emplear en las leyes antiterroristas⁴⁰. Aunque el Relator Especial es consciente de que los Estados están interesados en proteger la seguridad nacional y el orden público, que son motivos legítimos para limitar la libertad de reunión y de asociación, esas leyes se suelen redactar en unos términos que dan pie a los abusos. Por ejemplo, en muchas de ellas se define el terrorismo con términos imprecisos y subjetivos, como los de “terror generalizado provocado mediante el extremismo político”, “trastornos sociales graves”⁴¹, “la alteración de los servicios públicos”, “la incitación a la violencia en manifestaciones” y “el infundir temor a la población para menoscabar la solidaridad” de un país⁴². La vaguedad de los términos dificulta mucho el determinar, con certeza razonable, qué conducta (en línea y fuera de línea) se considerará “terrorismo”. Las organizaciones y las personas que se considera que promueven o divulgan unas opiniones o convicciones que no comparte la mayoría de la población o que son contrarias a las autoridades son particularmente vulnerables, lo que tendrá un efecto disuasorio considerable sobre ellas y las excluirá, aún más, del espacio digital.

Leyes de vigilancia

35. Los titulares de mandatos han subrayado que las leyes de vigilancia demasiado amplias y generales no suelen servir para acusar a personas concretas a partir de una sospecha razonable⁴³. Por ejemplo, la Ley de Facultades de Investigación de 2016 del Reino Unido de Gran Bretaña e Irlanda del Norte se había redactado con una terminología vaga que permitía a las autoridades investigar a un grupo o categoría de personas sin tener que identificar individualmente a cada uno de los investigados⁴⁴. Otras normas jurídicas de vigilancia otorgan a los Estados muchísima libertad para vigilar las actividades en línea de los ciudadanos, por ejemplo el proyecto de ley de reforma de la Ley de Telecomunicaciones y otras leyes de Australia, que contiene disposiciones en las que se concederá a las autoridades facultades ilimitadas para obligar a las empresas a que faciliten a los organismos de seguridad el acceso a datos cifrados de usuarios y a que debiliten las tecnologías de cifrado⁴⁵. Los riesgos de abusos aumentan, dado que muchas leyes y muchos reglamentos vigentes que regulan la vigilancia no siguen el ritmo de las veloces transformaciones que experimenta la tecnología de vigilancia y de sus posibles usos.

Leyes de medios de difusión y de lucha contra las noticias falsas

36. Durante las consultas con la sociedad civil, se expresaron inquietudes acerca de la terminología imprecisa que se emplea en el decreto interministerial (*prakas*) núm. 170 de Camboya, de 28 de mayo de 2018, en el que se prohíben las actividades en línea dirigidas a crear trastornos en la sociedad. En esa disposición se confieren a las autoridades potestades discrecionales excesivas para prohibir una amplia gama de actividades en línea, como el intercambio de fotografías y de vídeos de abusos policiales contra manifestantes, la difusión de mensajes de convocatoria de manifestaciones pacíficas, y las campañas políticas. También se imponen sanciones rigurosas, y las organizaciones de la sociedad civil corren peligro de que las clausuren por difundir contenidos prohibidos, lo que es desproporcionado y contraviene el derecho a la libertad de asociación. Además, estas restricciones se imponen mediante decreto gubernamental, lo que agrava las inquietudes acerca de su legalidad⁴⁶.

⁴⁰ Véase A/HRC/26/29, párr. 59.

⁴¹ Véase BRA 8/2015.

⁴² Asian Forum for Human Rights and Development (Forum-Asia), *Instruments of Repression: A Regional Report on the Status of Freedoms of Expression, Peaceful Assembly, and Association in Asia*, págs. 84 y 89.

⁴³ Véase A/HRC/35/28/Add.1.

⁴⁴ *Ibid.*

⁴⁵ Véase AUS 5/2018.

⁴⁶ Comisión Interamericana de Derechos Humanos, “Segundo informe sobre la situación de las defensoras y los defensores de los derechos humanos en las Américas” (OEA/Ser.L/V/II. Doc. 669, párr. 165).

Leyes sobre las manifestaciones

37. En la Federación de Rusia, por ejemplo, se introdujeron, mediante la “Ley Yarovaya”, unas enmiendas demasiado generales al Código Penal en las que se prohibía inducir, captar o implicar del modo que fuere a otras personas para que organizaran desórdenes colectivos⁴⁷. La publicación de declaraciones en Internet se considera circunstancia agravante. Por su parte, en Kazajstán, el Código Penal prohíbe prestar asistencia para celebrar reuniones ilegales, incluso mediante dispositivos de comunicación⁴⁸. La redacción imprecisa de esas disposiciones limita indebidamente los derechos a la libertad de reunión pacífica, de asociación y de expresión, al convertir en posible delito la divulgación de información sobre una protesta, el debate sobre ella, la búsqueda de dicha información o la conexión con las páginas donde figure.

2. Fines legítimos

38. Las limitaciones de los derechos a la libertad de reunión pacífica y de asociación deben tener un fin legítimo. En el Pacto se reconocen solo como legítimos los siguientes fines: la seguridad nacional o la seguridad pública, el orden público, la protección de la salud o la moral públicas o la protección de los derechos y las libertades de los demás. Los Estados no pueden invocar justificaciones admisibles para ocultar fines ilegítimos.

Penalización de las actividades en línea

39. La penalización de las actividades en línea de particulares y organizaciones constituye una tendencia creciente en muchos países del mundo⁴⁹. Se suele acusar a los particulares de delitos mal definidos que figuran en las leyes de represión del terrorismo, la ciberdelincuencia y las manifestaciones. En Viet Nam, por ejemplo, se detuvo y acusó de delito a un defensor de los derechos humanos por unos comentarios en Internet en los que, al parecer, criticaba al Gobierno⁵⁰. En la República Bolivariana de Venezuela se ha condenado, por delitos de incitación a la violencia, a un dirigente de la oposición política que ha convocado protestas contra el Gobierno en las redes sociales⁵¹. En los Emiratos Árabes Unidos se ha detenido y procesado a unos defensores de los derechos humanos acusados de difundir información falsa y engañosa en Internet, con miras a propagar el odio y el sectarismo⁵², y de emplear las redes sociales para poner en peligro la seguridad del Estado e injuriar a los gobernantes, en virtud de la Ley de Ciberdelincuencia⁵³. En Egipto se ha detenido y procesado a unos activistas acusándolos de haberse afiliado a una organización cuya fundación atentaba contra la Constitución y de haber pretendido socavar las instituciones del Estado, como represalia por unos comentarios que habían formulado en las redes sociales⁵⁴. En la Arabia Saudita, según parece, uno de los fundadores de la Asociación Saudita de Derechos Civiles y Políticos ha sido condenado a ocho años de cárcel y a una prohibición de viajar durante ocho años por haber infringido el artículo 6 de la Ley de Lucha contra la Ciberdelincuencia, al haber instigado a la opinión pública en contra de los gobernantes del país, haber firmado declaraciones publicadas en línea en las que se convocaba a la población a manifestarse y haberse resistido a acatar la resolución judicial de clausurar la Asociación⁵⁵. A las defensoras saudíes de los derechos humanos que se oponen a la prohibición de conducir se las ha juzgado en causas de terrorismo, por delitos como la incitación a la protesta, el intento de soliviantar a la opinión pública y la filmación de manifestaciones y la subsiguiente publicación de lo filmado en las redes sociales⁵⁶.

⁴⁷ Véase RUS 7/2016.

⁴⁸ A/HRC/29/25/Add.2, párr. 57.

⁴⁹ A/71/373, paras. 29 a 35

⁵⁰ Véase VNM 1/2017.

⁵¹ Véase la opinión núm. 26/2014 del Grupo de Trabajo sobre la Detención Arbitraria.

⁵² Véase ARE/1/2018.

⁵³ Véase ARE 5/2013.

⁵⁴ Véase EGY 4/2017.

⁵⁵ Véase SAU 4/2016.

⁵⁶ Véanse SAU 11/2018 y SAU/1/2017.

40. Aunque los Estados suelen invocar razones de seguridad nacional y orden público al acusar a esas personas, lo cierto es que los juicios penales a los que se las somete se suelen utilizar, con demasiada frecuencia, para ahogar la disensión y controlar el espacio digital, lo que no es un fin estatal legítimo, y contraviene directamente los artículos 21 y 22 del Pacto. No se debería suscitar la responsabilidad penal, civil o administrativa de ninguna persona por organizar o fomentar protestas pacíficas o participar en ellas⁵⁷, ni por crear o gestionar una asociación con fines legítimos. La disensión es una parte legítima de los derechos a la libertad de reunión pacífica y de asociación y se la debería proteger, en línea y fuera de línea⁵⁸.

Bloqueo arbitrario de contenidos digitales

41. Cada vez es más frecuente que se bloqueen sitios web enteros de organizaciones de derechos humanos y partidos de la oposición política en muchas partes del mundo, como en países del Oriente Medio y de la región del África Septentrional. Por ejemplo, en los Emiratos Árabes Unidos y la Arabia Saudita, las autoridades bloquean habitualmente sitios web en los que figuran críticas. Son víctimas de ello, sobre todo, los sitios web pertenecientes a organizaciones de la sociedad civil y grupos de derechos humanos, como la campaña saudita #Women2Drive, que se bloqueó en 2013. Por su parte, las autoridades egipcias han bloqueado varios sitios web de organizaciones de derechos humanos⁵⁹. El cortafuego que se emplea en China bloquea sistemáticamente el acceso a miles de sitios web y de contenidos digitales que están radicados fuera del país y contienen términos clave como “democracia” y “derechos humanos”⁶⁰.

42. El sitio web de una persona o de una asociación es un medio importante que tienen estas de promover una causa; plantear cuestiones de interés público y contribuir al debate público; denunciar vulneraciones de los derechos humanos; publicar investigaciones; obtener, recibir y divulgar información e ideas de toda clase; construir coaliciones y redes con otras organizaciones, también del extranjero; recaudar fondos; captar miembros y voluntarios, y tratar con los órganos internacionales y regionales de derechos humanos. En general, el bloqueo de sitios web enteros es una medida extrema y desproporcionada que limita gravemente la capacidad de llevar a cabo esas actividades y, por tanto, socava el ejercicio de la libertad de reunión y de asociación. En muchos casos, parece que esas medidas se dirigen indebidamente contra quienes disienten y, así pues, no se pueden justificar como medidas con un fin legítimo. El Relator Especial considera que prohibir a una persona o una asociación que publiquen material en línea “por el solo hecho de criticar al gobierno o al sistema político o social al que se adhiere”⁶¹ lesiona los derechos a la libertad de reunión pacífica, de asociación y de expresión.

Troleo y ciberataques patrocinados por el Estado

43. Algunos Estados han aprovechado la tecnología para vigilar y entorpecer la labor de los defensores de los derechos humanos y los agentes de la sociedad civil. Sus tácticas varían. Muchos hackean teléfonos y ordenadores, lanzan amenazas de muerte y violación, divulgan imágenes manipuladas, suspenden temporalmente las cuentas de sus víctimas, secuestran etiquetas, propagan teorías sobre conspiraciones, vierten acusaciones de traición y promueven sentimientos discriminatorios virulentos. Si bien el Relator Especial es consciente de que los Estados no son los únicos que cometen actos de esa índole, lo cierto es que también incurren en responsabilidad al encargar o alentar a terceros a que los cometan.

44. Esos ataques son una vulneración directa de los derechos a la libertad de reunión pacífica y de asociación de las personas, ya que no se pueden justificar como actos con

⁵⁷ Véase A/HRC/31/66, párr. 27.

⁵⁸ Véase A/HRC/20/27, párr. 84.

⁵⁹ Véase EGY 13/2017.

⁶⁰ Freedom House, “Freedom on the Net 2018”, que se puede consultar en <https://freedomhouse.org/report/freedom-net/freedom-net-2018>. Véase también Rebecca MacKinnon, *Consent of the Networked: The Worldwide Struggle for Internet Freedom* (Basic Books, 2012), págs. 31 a 47.

⁶¹ A/66/290, párr. 39.

finés legítimos en una sociedad democrática. Su objetivo es el contrario: intimidar a los agentes de la sociedad civil, destruir su credibilidad y legitimidad y negarles la atención necesaria para movilizarse en el espacio digital. Esos ataques minan la capacidad que tienen las organizaciones de la sociedad civil y los activistas de difundir o recibir información y comunicarse con los demás. Incentivan la autocensura y amenazan la seguridad y la integridad personales.

45. Por ejemplo, los trolls reciben instrucciones para difundir propaganda, aislar o ahogar las opiniones críticas e inhibir los movimientos contrarios al Gobierno, y para amplificar los mensajes de las autoridades públicas y aumentar su número de seguidores⁶². Por ejemplo, las autoridades de Omán, de manera sistemática, hackean y secuestran cuentas en línea e inundan las redes sociales, como Twitter, con un torrente interminable de referencias a etiquetas y, así, desarticulan el debate sobre determinados temas⁶³.

46. Otro ejemplo de esa tendencia es el uso de programas espía comerciales, como la tecnología de vigilancia FinFisher y el paquete de aplicaciones de espionaje Pegasus, para lanzar ataques contra agentes de la sociedad civil. Unos informes bien documentados han relacionado Pegasus con los ataques de programas espía contra activistas y defensores de los derechos humanos en la Arabia Saudita, Bahrein, los Emiratos Árabes Unidos, Kazajstán, Marruecos y México, entre otros países⁶⁴. Esos ataques permiten hackear las cuentas de esas personas y vigila, en tiempo real, sus comunicaciones, localización y actividades⁶⁵, y pueden ir dirigidos contra blancos situados en el propio Estado o blancos extraterritoriales⁶⁶.

47. Otra técnica que se usa es la de infiltrarse en grupos o foros de las redes sociales y hacer un seguimiento de las actividades en línea de la sociedad civil “haciéndose amigos” de los activistas. Asimismo, los datos obtenidos de fuentes de acceso público por los servicios de inteligencia pueden servir para desarticular, de antemano, manifestaciones pacíficas deteniendo a los organizadores, que se comunican y planifican sus actividades en línea.

48. Las mujeres y las personas lesbianas, gais, bisexuales, transgénero e intersexuales corren peligro particular de sufrir ataques de esa índole. Por ejemplo, según parece, el Gobierno de Egipto ha identificado y detenido a activistas de orientación sexual lesbiana, gai, bisexual, transgénero e intersexual infiltrándose en la red social Grindr y vigilando sus actividades en ella⁶⁷. Las autoridades del Brasil han usado Tinder para entablar relaciones con mujeres activistas que estaban implicadas en protestas y vigilarlas⁶⁸. En Tailandia, las defensoras de los derechos humanos han sufrido fuertes campañas de descrédito y acoso y amenazas de muerte en blogs y redes sociales⁶⁹. Esos ataques adoptan formas particulares, entre ellas la difusión de imágenes manipuladas, que tienen habitualmente contenido sexual o de género; la propagación de información encaminada a desacreditar a las personas, que suele estar llena de estereotipos de género perjudiciales y negativos; la difusión de mensajes de odio violentos y mensajes amenazadores en las redes sociales, que incluyen llamamientos a la violación colectiva y al asesinato; y las intrusiones en la intimidad, como el hackeo de los números telefónicos y los ordenadores de familiares y la divulgación del número telefónico de la víctima, de su domicilio y de fotografías personales y familiares. El titular del mandato suscribe las conclusiones de la Relatora Especial sobre la violencia contra la mujer, sus causas y consecuencias de que los abusos en línea contra las mujeres

⁶² Institute for the Future, “State-sponsored trolling: how governments are deploying disinformation as part of broader digital harassment campaigns” (2018).

⁶³ A/HRC/29/25/Add.1, párr. 34.

⁶⁴ Véase, por ejemplo, Citizen Lab, “Hide and seek: tracking NSO Group’s Pegasus spyware to operations in 45 countries”.

⁶⁵ Véase LBN 2/2018.

⁶⁶ Información presentada por los *amici curiae* en la causa *John Doe a.k.a. Kidane v. Federal Democratic Republic of Ethiopia*, que se dirimió en el Tribunal de Apelación de Circuito del Distrito de Columbia, de los Estados Unidos.

⁶⁷ Article 19, “Apps, arrests and abuse in Egypt, Lebanon and Iran”, febrero de 2018.

⁶⁸ Privacy International, “State of privacy Brazil”.

⁶⁹ Véase, por ejemplo, THA 6/2017.

son un ataque directo contra la visibilidad de estas y su participación plena en la vida pública y de que se deberían investigar y castigar debidamente⁷⁰

3. Limitaciones necesarias y proporcionadas para proteger un objetivo legítimo

49. En los artículos 21 y 22, párrafo 2, del Pacto se requiere que las limitaciones de la libertad de reunión o de asociación sean necesarias y proporcionadas en una sociedad democrática, en interés de la seguridad nacional, de la seguridad pública o del orden público, o para proteger la salud o la moral públicas o los derechos y libertades de los demás. El Relator Especial ha señalado, en otro lugar, que el término “necesarias” expresa que tienen que existir razones sociales acuciantes “para una injerencia”. Cuando surja una necesidad social acuciante, los Estados tendrán que asegurar que toda medida restrictiva adoptada se circunscriba a los límites de lo aceptable en una sociedad democrática, que “exist[e] únicamente donde hay ‘pluralismo, tolerancia y una mentalidad abierta’”⁷¹. El deber de justificar esa necesidad recae siempre en el Estado.

50. Los Estados suelen impedir el ejercicio de las libertades de reunión y de asociación en línea mediante restricciones que no son necesarias ni proporcionadas, habida cuenta de las amenazas concretas que se aducen. Algunos ejemplos de ello son la perturbación del funcionamiento de las redes digitales, el bloqueo de contenidos digitales ordenado por el Estado, la aplicación de impuestos por el uso de las redes sociales y la vigilancia mediante tecnologías digitales.

Perturbación de las redes digitales

51. Según ciertos datos⁷², se documentaron, al menos, 40 perturbaciones del funcionamiento de las redes digitales relacionadas con manifestaciones públicas y protestas pacíficas en 2018, 37 perturbaciones en 2017 y 27 en 2016. Las regiones más afectadas son Asia y África, donde se han registrado casos de interrupción de los servicios de Internet o de prohibición de las redes sociales en la India⁷³, la República Islámica del Irán⁷⁴, el Chad⁷⁵, el Camerún⁷⁶ y el Togo⁷⁷. Ya solo en la India se dieron 64 perturbaciones del funcionamiento de las redes digitales relacionadas con manifestaciones públicas entre 2016 y 2018. Se han registrado perturbaciones análogas con ocasión de reuniones pacíficas en otras regiones del mundo, lo que demuestra que estas perturbaciones se han convertido en una tendencia mundial peligrosa. También ha aumentado el número de perturbaciones del funcionamiento de las redes digitales y de prohibiciones contra las redes sociales en época de elecciones desde 2016, lo que ha perjudicado gravemente a la visibilidad que tienen los partidos de la oposición política y los movimientos sociales y a su capacidad de movilizar apoyo en momentos decisivos. Esas medidas merman la capacidad que tienen los defensores de los derechos humanos de llevar a cabo su labor y de documentar los atentados contra esos derechos⁷⁸.

52. El Relator Especial opina que las interrupciones del servicio de las redes digitales contravienen claramente el derecho internacional y no se pueden justificar en ninguna circunstancia. Las interrupciones del servicio incumplen el criterio de imposición de limitaciones al derecho de reunión pacífica que se enuncia en el artículo 21 del Pacto y el criterio de imposición de limitaciones al derecho a la libertad de asociación que se enuncia en el artículo 22, párrafo 2, de este instrumento. En la mayoría de los casos, las órdenes de interrupción del servicio de las redes digitales carecen de fundamento jurídico. Cuando carecen de tal fundamento, las órdenes se suelen remitir a disposiciones generales y vagas y no son objeto de una supervisión independiente adecuada⁷⁹. Aunque estas medidas se

⁷⁰ Véase A/HRC/38/47.

⁷¹ Véase A/HRC/20/27, párr. 17.

⁷² Access Now, #KeepitOn campaign, and Shutdown Tracker Optimization Project (STOP).

⁷³ Véanse IND 5/2016, IND 3/2017 e IND 7/2017.

⁷⁴ Véase IRN 1/2018.

⁷⁵ Véase TCD 3/2016.

⁷⁶ Véase CMR 1/2018.

⁷⁷ Véase TGO 1/2017.

⁷⁸ Véase A/68/299, párr. 28.

⁷⁹ Véase A/HRC/29/25/Add.2.

justifican, por lo común, con razones de seguridad nacional y orden público, son un medio desproporcionado, y generalmente ineficaz, de lograr esos fines legítimos.

53. Esas medidas extremas ocasionan a los derechos humanos, la actividad económica, el orden público y los servicios de emergencia unos perjuicios muy variados, que superan los pretendidos beneficios. Las perturbaciones del funcionamiento de las redes digitales suelen resultar contraproducentes y provocar caos y agitación. En los momentos en que tienen lugar protestas y elecciones, que es cuando las tensiones alcanzan su grado máximo, se requieren esos instrumentos para prevenir la desinformación y disipar los rumores, así como para proteger los derechos a la libertad y la integridad personal, permitiendo el acceso a ayuda urgente y el contacto con la familia y las amistades⁸⁰. El Consejo de Derechos Humanos ha expresado, de manera inequívoca, su preocupación ante las medidas que, en violación del derecho internacional de los derechos humanos, pretenden impedir o perturbar el acceso a la información en línea o su difusión, o los impiden o perturban intencionadamente⁸¹.

Impuestos por el uso de las redes sociales

54. Al Relator Especial le inquieta que la imposición reciente de impuestos por el uso de las redes sociales en algunos países, pueda perjudicar desproporcionadamente la capacidad que tienen las personas vulnerables de ejercer los derechos a la libertad de reunión pacífica y de asociación, y que esos “impuestos a las redes sociales” puedan suscitar dudas respecto de su necesidad o proporcionalidad. Por ejemplo, el impuesto a las redes sociales de Uganda repercute desproporcionada y negativamente en la capacidad que tienen los usuarios de acceder a Internet de manera asequible, por lo que limita indebidamente su derecho a la libertad de expresión y sus derechos a la libertad de reunión pacífica y de asociación, sobre todo en el caso de los ciudadanos de renta baja, a quienes 1 GB mensual de datos les cuesta casi el 40% de su renta mensual media⁸². Aunque puede haber justificaciones económicas legítimas para esos impuestos, los Estados deben adoptar medidas para procurar que no menoscaben, de manera desproporcionada, las posibilidades que tienen las personas de comunicarse con otros miembros de la sociedad, y no agranden las brechas digitales.

Vigilancia mediante dispositivos digitales

55. Durante el último decenio han aumentado las medidas de vigilancia innecesarias y desproporcionadas en todo el mundo. El requisito de necesidad obliga a demostrar cómo cumplirá la vigilancia un objetivo previsto, cumplimiento que suele verse amenazado por la propia actividad de vigilancia. Estados como Australia y el Reino Unido, por ejemplo, afirman que la seguridad nacional o el orden público justifican el que se debiliten los dispositivos de cifrado⁸³. Como ha declarado el Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, hay un amplio consenso entre los especialistas en seguridad informática de que esas vulnerabilidades de cifrado obligan a hacer, en general, unos gastos considerables en seguridad digital, ya que dichas vulnerabilidades pueden ser aprovechadas por terceros no autorizados, aun cuando estén previstas para uso exclusivo de los gobiernos⁸⁴.

56. El principio de proporcionalidad requiere que se pruebe que la medida aplicada es la opción menos invasora. La vigilancia colectiva, esto es, la recogida y el análisis de grandes volúmenes de metadatos de todas las comunicaciones⁸⁵, con la intención expresa de averiguar las relaciones de asociación que mantienen las personas, es inherentemente

⁸⁰ Véase Jan Rydzak, Global Network Initiative, “Disconnected: a human rights-based approach to network disruptions”.

⁸¹ Véase la resolución 38/7 del Consejo de Derechos Humanos.

⁸² Véase UGA 3/2018.

⁸³ Véase A/HRC/35/28/Add.1.

⁸⁴ Véase A/HRC/38/35/Add.5.

⁸⁵ Los metadatos son la información relativa a una comunicación, como la geolocalización de esta, la duración y los interlocutores.

desproporcionada⁸⁶. Asimismo, los requisitos jurídicos que se imponen a los proveedores de servicios de comunicaciones de que almacenen los datos personales y sensibles localmente y registren las tarjetas SIM de manera indiscriminada permiten a las autoridades acceder a información que no atañe, de manera pertinente ni sustancial, a ningún delito grave o amenaza específica⁸⁷. Las leyes de registro obligatorio de las tarjetas SIM, en particular, “exigen que la mayor parte de la población divulgue datos personales de identificación” al Estado de que se trate⁸⁸. La tecnología de reconocimiento facial que se emplea en los grandes actos culturales, las competiciones deportivas importantes, los festivales de música y las reuniones políticas también suscita inquietudes acerca de su proporcionalidad. Asimismo, los dispositivos de captura del número de Identificación Internacional de Abonados Móviles (receptores de IMSI)⁸⁹ permiten a los países recopilar datos de miles de teléfonos móviles en una zona determinada o en actos públicos como manifestaciones políticas. Esos dispositivos se usan para identificar y vigilar a todos quienes participan en determinado acto o se hallan en determinado espacio público⁹⁰. Estas formas de identificación y recopilación de datos atentan contra el anonimato de la persona en los espacios públicos y ejercen unos “efectos disuasorios” considerables en la decisión de participar en reuniones públicas⁹¹.

57. Se debería prohibir el empleo de tecnologías de vigilancia para vigilar, de manera indiscriminada y general, a quienes ejercen sus derechos a la libertad de reunión pacífica y de asociación, tanto en el espacio material como en el digital. La vigilancia de los particulares que ejercen esos derechos suyos solo se puede llevar a cabo de manera específica, cuando haya una sospecha razonable de que están implicados en delitos penales graves o prevén implicarse en ellos y aplicando las normas más estrictas y los principios de necesidad y proporcionalidad, bajo supervisión judicial rigurosa.

C. Empresas de tecnología digital: preocupaciones principales

58. En virtud del control que ejercen sobre las plataformas y los dispositivos en línea, estas empresas se exponen a que los Estados les soliciten acceso a los datos de los usuarios. En ocasiones, estas solicitudes pueden adoptar la forma de peticiones oficiosas o presiones. Cuando las leyes nacionales incumplen los principios y las normas internacionales de derechos humanos, las empresas se ven sujetas a unas obligaciones jurídicas contradictorias que amenazan tanto sus posibilidades de respetar los derechos humanos como sus posibilidades de operar en ciertas jurisdicciones. Ello las puede inducir a lesionar los derechos a la libertad de reunión pacífica y de asociación de los usuarios, y suscita interrogantes sobre la transparencia y la rendición de cuentas. Empresas de todo el mundo no suelen revelar como debieran la información sobre recopilación de datos y las solicitudes de los gobiernos⁹². Los informes de transparencia que publican las empresas de tecnología digital estadounidenses y europeas más importantes del mundo son ejemplos positivos que se deberían extender y perfeccionar.

59. La manera en que las plataformas digitales moderan la publicación de contenidos según sus propias reglas de comunidad también suscita preocupaciones acerca de los derechos humanos, por ejemplo acerca de los derechos a la libertad de reunión pacífica y de asociación. En particular, las políticas que aplican las empresas propietarias de las redes sociales en materia de contenido responden a interpretaciones heterogéneas de lo que constituye una expresión o una conducta admisible, que puede no estar en consonancia con

⁸⁶ Véase la resolución 34/7 del Consejo de Derechos Humanos.

⁸⁷ Véanse A/HRC/29/32, párr. 51, y A/HRC/35/22, párr. 20.

⁸⁸ *Ibid.*

⁸⁹ Véase A/HRC/35/28/Add.1.

⁹⁰ The Human Rights, Big Data and Technology Project, “The Universal Declaration of Human Rights at 70: putting human rights at the heart of the design, development and deployment of artificial intelligence”, 20 de diciembre de 2018, pág. 31.

⁹¹ Véase Daragh Murray y Pete Fussey, “Bulk surveillance in the digital age: rethinking the human rights law approach to bulk monitoring of communications data”, *Israel Law Review*, vol. 52, núm. 1.

⁹² Ranking Digital Rights, The Ranking Digital Rights 2018 Corporate Accountability Index, cap. 3, “Inadequate disclosure”.

los principios y las normas internacionales de derechos humanos. Además, la manera en que se aplican esas políticas de contenidos, mediante la moderación de estos, también puede contravenir las normas de derechos humanos y suscitar cuestiones de injerencia arbitraria, a pesar de los intentos de mejora que se han hecho. Asimismo, parece que la aplicación de las políticas de contenido afecta a quienes tienen una personalidad pública de manera desproporcionada. Es más, al descargar en los usuarios la responsabilidad de denunciar las infracciones de las normas de la comunidad (esto es, al recurrir a la vigilancia comunitaria), la aplicación de las políticas de contenidos pone, a los activistas y a quienes convocan movilizaciones colectivas, en peligro de que se supriman arbitrariamente sus contenidos y se suspendan o cancelen sus cuentas. Las personalidades públicas no solo tienen más probabilidades de ser denunciadas que los usuarios menos populares (dada su visibilidad), sino que también suelen ser víctimas de campañas dirigidas expresamente a lograr que se retiren sus contenidos y se cancelen sus cuentas. El uso de la inteligencia artificial para moderar la publicación de contenidos agrava el problema, ya que las plataformas utilizan, cada vez más, procedimientos automatizados para marcar los contenidos que se deben retirar.

60. También se usan sistemas algorítmicos para influir en la facilidad de búsqueda, la visibilidad y la accesibilidad de los materiales, esto es, qué contenidos ven las personas, con quiénes se conectan y qué grupos encuentran. Ello significa que el suministro de contenidos se puede basar en el historial de afiliaciones políticas, en las afiliaciones políticas supuestas o en otros lazos de asociación, lo que puede constituir una ventaja para quienes pretenden llegar a determinado público y comunicarse con personas de mentalidad afín, pero también un inconveniente. Los sistemas algorítmicos tienen el poder de silenciar historias y movimientos, impedir que los agentes de la sociedad civil lleguen a un público más amplio y potenciar las cajas de resonancia o propagar los sesgos y la discriminación, en detrimento del desarrollo democrático. Asimismo, estas medidas pueden tener un efecto desproporcionado en grupos que ya están marginados o en situación de riesgo, sobre todo las mujeres⁹³. Los sistemas algorítmicos son opacos y varían constantemente, y afectan a la visibilidad en línea de particulares y grupos, sin que ellos “puedan investigar o entender por qué, cómo o sobre qué base”⁹⁴.

61. Las políticas y las herramientas de privacidad y seguridad de las comunicaciones de los usuarios también pueden afectar al disfrute de los derechos a la libertad de reunión pacífica y de asociación. Solo unas pocas empresas de tecnología digital permiten emplear seudónimos u otros medios de disfrazar la identidad de una persona, o facilitan comunicaciones cifradas. Al Relator Especial le complacen los esfuerzos que ha hecho la red social Grindr por idear y aplicar unas herramientas de seguridad en su plataforma, a fin de proteger a las personas lesbianas, gais, bisexuales, transgénero e intersexuales en Egipto, la República Islámica del Irán y el Líbano, que sufren acoso político, torturas y encarcelamiento.

62. El Relator Especial observa que, si bien algunas empresas de tecnología digital se han esforzado por incluir el derecho a la libertad de expresión y el derecho a la privacidad en las evaluaciones de los riesgos y los procedimientos de diligencia debida, no han incluido, en cambio, los derechos a la libertad de reunión pacífica y a la libertad de asociación. En sus reuniones con las empresas de tecnología digital, ha averiguado que muchas de ellas reconocen el valor y la importancia que tienen esos derechos en una sociedad democrática, pero aún no han asumido un compromiso político de alto nivel en relación con ellos.

63. El Relator Especial pide a las empresas de tecnología digital que cumplan su obligación de respetar las normas de derechos humanos aceptadas internacionalmente, sobre todo las que atañen a los derechos a la libertad de reunión pacífica y de asociación. A tal fin, estas empresas deberían otorgar prioridad a la aplicación efectiva de los Principios Rectores sobre las Empresas y los Derechos Humanos. Se deberían fomentar los modelos en que se prevea una supervisión independiente de los análisis del impacto, como los

⁹³ Véase A/HRC/35/9, párr. 41.

⁹⁴ Véase A/73/348, párr. 32.

modelos propuestos por la Global Network Initiative⁹⁵. Las empresas de tecnología digital deberían comprometerse, en sus políticas, a respetar los derechos a la libertad de reunión pacífica y de asociación (además de cumplir sus compromisos vigentes de respetar la libertad de expresión y el derecho a la privacidad), mostrar la diligencia debida en relación con esas libertades fundamentales, por ejemplo realizando análisis periódicos del impacto que tienen esas políticas en los derechos humanos, e instituir unos mecanismos de reparación eficaces para ofrecer indemnizaciones y otras formas de resarcimiento cuando se produzcan vulneraciones. Los Estados deberían aprobar y aplicar unas leyes y políticas encaminadas a fijar unos requisitos obligatorios para que las empresas de tecnología digital muestren la diligencia debida en lo tocante a determinar el impacto que tengan sus actividades y productos en los derechos humanos, prevenirlos y mitigarlos, explicar cómo afrontarán ese impacto e instituir unos mecanismos sólidos que garanticen la transparencia y la reparación. Esas leyes y políticas deben tener “como objetivo principal el acceso universal y el disfrute de los derechos humanos”⁹⁶ y ceñirse a las directrices que emanan de los principios y las normas internacionales. Se deberían aprobar solo después de un proceso plenamente inclusivo y participativo de consulta con los interesados pertinentes.

64. El Relator Especial opina que la normativa internacional de derechos humanos debería regir la respuesta de las empresas de tecnología digital a las solicitudes de los gobiernos, así como sus decisiones sobre moderación de los contenidos y modelos técnicos, lo que incluye la edición de contenidos por medios digitales. Ello significa que los criterios de legalidad, necesidad y legitimidad se deberían aplicar a las decisiones de las empresas que afectaran a los derechos a la libertad de reunión pacífica y de asociación. El Relator Especial se remite a unos informes recientes del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión sobre el tema de la moderación del contenido de las plataformas digitales y la inteligencia artificial, en los que se expone detalladamente la complejidad y la magnitud de esos problemas y se formulan recomendaciones importantes⁹⁷.

V. Conclusiones y recomendaciones

65. **Aunque la era digital ha abierto un nuevo espacio para ejercer los derechos a la libertad de reunión pacífica y de asociación, también ha traído consigo una serie de amenazas y peligros nuevos para estos derechos fundamentales. Por ejemplo, las limitaciones jurídicas graves y las actividades estatales de vigilancia digital amenazan con destruir el espacio en el que la sociedad civil puede promover o defender colectivamente un asunto de interés común. La acción y la omisión de las empresas de tecnología digital han exacerbado esos riesgos o creado problemas nuevos y complejos para las personas y las organizaciones que pretenden ejercer los derechos a la libertad de reunión pacífica y de asociación en línea y fuera de línea. Es probable que estos problemas se intensifiquen en un futuro cada vez más digitalizado.**

66. **El derecho internacional protege los derechos a la libertad de reunión pacífica y de asociación, con independencia de que se los ejerza personalmente, con los medios técnicos contemporáneos o con los que se inventen en el futuro. Las normas y los principios de derechos humanos vigentes no solo deberían dictar el comportamiento de los Estados, sino también constituir el marco por el que se rigieran las empresas de tecnología digital en lo tocante al diseño, el control y la gestión de las tecnologías digitales.**

67. **Los Estados deberían velar por que los derechos a la libertad de reunión pacífica y de asociación se respetaran, protegieran e hicieran efectivos en los**

⁹⁵ La Global Network Initiative es una plataforma de interesados múltiples que entró en funcionamiento en 2018, con miras a proteger y fomentar la libertad de expresión y el derecho a la privacidad en el sector de la tecnología de la información y las comunicaciones fijando unos principios globales para que las empresas tomaran decisiones de manera responsable. Véase <https://globalnetworkinitiative.org/team/our-mission/>.

⁹⁶ Véase la resolución 38/7 del Consejo de Derechos Humanos, párr. 18.

⁹⁷ Véase A/HRC/38/35, párr. 61.

ordenamientos jurídicos, las políticas y las prácticas nacionales, con arreglo al derecho internacional. Las empresas de tecnología digital se deben comprometer a respetar las libertades de reunión pacífica y de asociación y ejercer la diligencia debida para no ocasionar vulneraciones de esos derechos, contribuir a ellas o tener complicidad en ellas. En el ejercicio de sus responsabilidades respectivas, los Estados y las empresas de tecnología digital deberían atenerse a los principios acreditados de no discriminación, pluralismo de opiniones, transparencia, participación de múltiples interesados y acceso a la justicia.

68. A tal fin, el Relator Especial formula las siguientes recomendaciones.

A. Recomendaciones a los Estados

69. Los Estados deberían velar por que todas las injerencias en los derechos a la libertad de reunión pacífica y de asociación estuvieran “prescritas por la ley” y fueran “necesarias en una sociedad democrática en razón de la seguridad nacional, el orden público, la protección de la salud o de la moral públicas o la protección de los derechos y libertades de los demás”⁹⁸. Las restricciones por razones de “seguridad nacional”, “orden público” y “protección de la moral” se deberían definir de manera clara y precisa, para evitar que las autoridades abusaran de ellas.

70. Los Estados deberían promover y facilitar el acceso a las tecnologías digitales y no deberían limitar su uso para ejercer los derechos a la libertad de reunión pacífica y de asociación. En las políticas y las prácticas se deberían tener en cuenta la igualdad de acceso a Internet y a las tecnologías digitales, la asequibilidad de estos servicios y la participación de todas las personas en la era digital, para cerrar la brecha digital.

71. Las reuniones y asociaciones en línea desempeñan un papel particularmente importante para los grupos marginados, y la injerencia en los derechos a la libertad de reunión pacífica y de asociación puede tener repercusiones desproporcionadas en las personas y los grupos que se hallen en posición vulnerable. En el cumplimiento de sus obligaciones, los Estados deberían prestar particular atención a los efectos dispares que tuvieran las limitaciones del acceso a las tecnologías digitales y de su uso en las minorías raciales y religiosas, los opositores y los activistas políticos, y las personas lesbianas, gais, bisexuales, transgénero e intersexuales.

72. Los Estados deberían velar por que todos dispusieran de un recurso eficaz contra la vulneración de sus derechos a la libertad de reunión pacífica y de asociación y por que dicho recurso les resulte accesible. Los recursos deberían ser accesibles, asequibles, adecuados y oportunos, desde la perspectiva de los titulares de derechos afectados. Los Estados deberían ofrecer reparación por conducto de unas autoridades judiciales, administrativas o legislativas independientes o de cualquier otra autoridad independiente y competente prevista en el ordenamiento jurídico.

73. Los Estados deberían instaurar un marco jurídico que favoreciera el ejercicio de los derechos a la libertad de reunión pacífica y de asociación en la era digital, por los siguientes medios:

a) Derogar las leyes que limiten o menoscaben indebidamente los derechos a la libertad de reunión pacífica y de asociación, incluidas las leyes de prohibición de las protestas, o abstenerse de aprobar tales leyes;

b) Derogar y reformar todas las leyes y las políticas en las que se autoricen las perturbaciones y la interrupción del funcionamiento de las redes digitales, y abstenerse de aprobar tales leyes y políticas;

c) Revisar y reformar las leyes de lucha contra la ciberdelincuencia y el terrorismo y las leyes de vigilancia y ajustarlas a las normas y los principios internacionales de derechos humanos que rigen el derecho a la privacidad, el derecho

⁹⁸ Véase la resolución 15/21 del Consejo de Derechos Humanos, párr. 4.

a la libertad de opinión y de expresión, el derecho a la libertad de reunión pacífica y el derecho a la libertad de asociación;

d) Promover y proteger un cifrado y un anonimato fuertes, por ejemplo aprobando leyes, reglamentos y políticas en los que se confiera exclusivamente a los tribunales la potestad de revocar el derecho al anonimato, en lugar de conferírsela a los órganos policiales.

74. Los Estados deberían abstenerse de adoptar medidas como la supresión del acceso a los servicios de Internet y de telecomunicaciones, y deberían poner fin a esas medidas. El acceso a los servicios de Internet y de telefonía móvil se debería mantener siempre, incluso en épocas de desórdenes públicos. Se deberían respetar, proteger y promover especialmente el acceso a las tecnologías digitales y su uso durante las épocas de elecciones, con fines de reunión y asociación.

75. Se debería poner fin a todas las prácticas de bloqueo de sitios web de las organizaciones de la sociedad civil y los defensores de los derechos humanos.

76. Se debería prohibir el empleo de tecnologías de vigilancia para vigilar, de manera indiscriminada y general, a quienes ejercieran los derechos a la libertad de reunión pacífica y de asociación, tanto en espacios materiales como en línea.

77. Habría que abstenerse de realizar actividades indebidas de vigilancia específica mediante dispositivos digitales contra los agentes de la sociedad civil, los organizadores de manifestaciones, las minorías y otras personas que pretendieran ejercer sus derechos a la libertad de reunión pacífica y de asociación. Para ser admisibles, las actividades de vigilancia específica solo se pueden realizar cuando sean abiertas, tengan un plazo definido, se ajusten a los criterios fijados internacionalmente de prescripción legal, finalidad legítima, necesidad y proporcionalidad y estén sujetas a una supervisión independiente y continua mediante mecanismos de autorización previa, supervisión operativa y examen. Se debería cursar la notificación correspondiente a las personas y los grupos cuando se hubieran lesionado sus derechos mediante la vigilancia, y se les deberían garantizar recursos eficaces.

78. Asimismo, toda aplicación de las nuevas formas de vigilancia tecnológica se debería ceñir a los citados principios y normas, incluida la vigilancia extraterritorial. Los Estados deberían abrir investigaciones independientes para examinar el uso de todas las tecnologías de vigilancia, para que la ciudadanía juzgue la índole y la frecuencia de dicho uso, sus justificaciones y su necesidad y proporcionalidad, y juzgue también si esas tecnologías se están usando de manera inapropiada o demasiado amplia.

79. Se debería poner fin a todas las actividades de troleo, intimidación y desinformación en línea patrocinadas por los gobiernos y dirigidas contra los agentes de la sociedad civil. Los Estados deberían investigar esas actividades, ofrecer recursos eficaces y aprobar y aplicar medidas preventivas. En este sentido, los Estados deberían determinar cuáles son las formas específicas de violencia en línea y las barreras que impiden a las mujeres acceder a la justicia, y hacer frente a esas formas de violencia.

80. Los Estados deberían cumplir como corresponde su deber de proteger a la población contra las vulneraciones de los derechos a la libertad de reunión pacífica y de asociación por parte de las empresas tomando medidas apropiadas para prevenir, investigar, castigar y reparar esos abusos mediante políticas adecuadas, actividades de reglamentación y sometimiento a la justicia. Ese deber incluye la aprobación y la aplicación de leyes y políticas encaminadas a fijar unos requisitos obligatorios para que las empresas de tecnología digital muestren la diligencia debida en lo tocante a determinar el impacto que tengan sus actividades y productos en los derechos humanos, prevenirlo y mitigarlo, explicar cómo afrontarán ese impacto e instituir unos mecanismos sólidos que garanticen la transparencia y la reparación. Esas leyes se deberían aprobar solo después de un proceso plenamente inclusivo y participativo de consulta con todos los interesados.

81. Los Estados deberían renovar su compromiso de adoptar un enfoque de interesados múltiples que constituyera la piedra angular de los procedimientos de gestión de Internet. La cooperación efectiva en cuestiones relacionadas con la esfera digital depende de las posibilidades que tengan las personas y los grupos de ejercer sus derechos a la libertad de reunión pacífica y de asociación.

B. Recomendaciones a las empresas de tecnología digital

82. Las empresas deberían cumplir su deber de respetar los derechos humanos aceptados internacionalmente, en particular los derechos a la libertad de reunión pacífica y de asociación, tomando todas las medidas necesarias y legales para no ocasionar vulneraciones de los derechos humanos, contribuir a ellas o tener complicidad en ellas.

83. Las empresas deberían comprometerse, al más alto nivel político, a respetar la libertad de reunión pacífica y de asociación y reconocer la importancia del papel que desempeña la sociedad civil en la democracia y el desarrollo sostenible.

84. Las empresas deberían procurar prevenir o mitigar los efectos perjudiciales que tuviera, en los derechos humanos, la colaboración que dispensaran a los gobiernos, en la medida en que lo autorizara la ley, cuando estos les solicitaran que censuraran, vigilaran o controlaran a personas o grupos o facilitaran los datos que recopilan, tratan o retienen.

85. Las empresas deberían reconocer que el derecho internacional de los derechos humanos es el marco acreditado que garantiza que sus productos y servicios respeten los derechos a la libertad de reunión pacífica y de asociación y deberían analizar sus políticas conforme a este marco. Las empresas deberían velar por que sus políticas y sus reglas de comunidad fueran lo suficientemente claras, accesibles y ajustadas a las normas internacionales de derechos humanos. Asimismo, deberían aportar ejemplos o estudios de casos más detallados sobre la manera en que se aplican sus reglas de comunidad en la práctica, para que los usuarios entendieran en qué circunstancias se podría acceder a sus datos o información personales, se podrían limitar los contenidos o se podría bloquear o limitar el acceso al servicio.

86. Las empresas deberían mostrar la diligencia debida en el ámbito de los derechos humanos para determinar las vulneraciones de los derechos a la libertad de reunión pacífica y de asociación, prevenirlas, mitigarlas y hacerles frente, por los siguientes medios:

a) Realizar análisis del impacto en los derechos humanos, teniendo en cuenta los derechos a la libertad de reunión pacífica y de asociación, al idear o modificar sus productos y servicios. El proceso de análisis del impacto debería incluir siempre consultas con los agentes de la sociedad civil y otros especialistas y ser corroborado por un tercero externo acreditado y con experiencia en el ámbito de los derechos humanos; y

b) Poner en práctica las conclusiones de los análisis del impacto tomando medidas dirigidas a los fines siguientes: aumentar el conocimiento de los derechos a la libertad de reunión pacífica y de asociación y la sensibilidad hacia ellos impartiendo formación y directrices a la dirección, los empleados y otros agentes del sector empresarial, como los contratistas; adoptar políticas y procedimientos en los que se defina cómo analizará, la empresa, las solicitudes gubernamentales de que limite las comunicaciones o el acceso a contenidos y cómo responderá a ellas; incorporar sistemas de alerta temprana en los procesos empresariales para determinar los riesgos en materia de derechos humanos, y reaccionar oportunamente; ejercer su influencia para rechazar las solicitudes gubernamentales que pretendan limitar indebidamente los derechos a la libertad de reunión pacífica y de asociación; fomentar la investigación y el desarrollo de soluciones tecnológicas apropiadas para el acoso, la desinformación y la propaganda en línea, entre ellas instrumentos para descubrir e identificar cuentas y *bots* ligados a los Estados; adoptar unos indicadores de

supervisión en los que se tengan en cuenta cuestiones relacionadas específicamente con la libertad de reunión pacífica y de asociación.

87. Las empresas deberían tomar medidas eficaces para que sus políticas y prácticas fueran transparentes, entre ellas la de aplicar sus condiciones de servicio y unos procedimientos de examen informatizados, y respetar las debidas garantías jurídicas. A tal fin, deberían publicar periódicamente, en su sitio web oficial, información sobre el fundamento jurídico de las solicitudes que hubieran formulado los gobiernos y demás terceros y sobre el número o el porcentaje de solicitudes a las que hubieran accedido las empresas, así como sobre el contenido o las cuentas que se hubieran limitado o suprimido en virtud de la política o las directrices de comunidad de las propias empresas.

88. Las empresas deberían instaurar unos mecanismos de supervisión independientes para vigilar el resultado de las decisiones de moderación de contenidos, y los Estados deberían estudiar la posibilidad de aprobar una reglamentación en la que se exigiera esa supervisión independiente.

89. Las empresas deberían instituir, consultando como correspondiera con las comunidades afectadas, unos mecanismos operativos de reclamación cuya disponibilidad y accesibilidad fueran claras, y que fueran eficaces tanto a efectos procedimentales como de reparación.

90. Las empresas deberían sumarse a las iniciativas de múltiples interesados que están en curso y aumentar la calidad de la participación en ellas y la calidad de su ejecución. Las empresas participantes deberían incrementar su respeto por los derechos a la libertad de reunión pacífica y de asociación en el seno de esas iniciativas.

91. Las empresas deberían colaborar con los gobiernos y la sociedad civil para desarrollar una tecnología que promoviera y afianzara los derechos humanos.

C. Recomendaciones a la sociedad civil

92. Los agentes de la sociedad civil deberían seguir innovando y colaborando con los gobiernos, las empresas y los círculos científicos para desarrollar una tecnología que favoreciera el ejercicio de los derechos a la libertad de reunión pacífica y de asociación.

93. Los agentes de la sociedad civil deberían velar por que la seguridad y la alfabetización digitales ocuparan un lugar principal en las actividades de su organización.

94. Los agentes de la sociedad civil deberían ampliar y perfeccionar la recopilación de datos acerca de los derechos a la libertad de reunión pacífica y de asociación, y la documentación de las amenazas digitales que pesan sobre estos derechos, sobre todo en relación con las novedades en materia jurídica, las perturbaciones del funcionamiento de las redes digitales, la vigilancia, el acoso en línea y las campañas de desinformación. Deberían intercambiar conocimientos, promover unas normas de recopilación de datos y colaborar con otros interesados en estas iniciativas.

95. Todos los grupos de la sociedad civil, y no solo las organizaciones defensoras de los derechos digitales, deberían favorecer el proceso de comprensión de las amenazas digitales que se ciernen sobre el espacio cívico, colaborar en este proceso e idear respuestas eficaces a estas amenazas.

D. Recomendaciones al Comité de Derechos Humanos

96. Tomar en consideración el presente informe al elaborar la observación general sobre el artículo 21 del Pacto Internacional de Derechos Civiles y Políticos.