Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios

Consideración prioritaria del ámbito digital 2015

Ediciones UNESCO

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios

Consideración prioritaria del ámbito digital 2015

Ediciones UNESCO

Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

Publicado en 2015 por
la Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura,
7, Place de Fontenoy, 75352 París 07 SP, Francia

ISBN 978-92-3-300053-7

Las designaciones empleadas y la presentación del material no entrañan la expresión de opinión alguna, cualquiera esta fuere, por parte de UNESCO, a propósito del estatuto jurídico de cualquier país, territorio, ciudad o zona, o de sus autoridades, fronteras o límites. Las ideas y opiniones expresadas en esta obra son las de los autores y no reflejan necesariamente el punto de vista de la UNESCO ni comprometen a la Organización.

La presente publicación se inspira en otros tres estudios, y en ella se resumen las cuestiones fundamentales tratadas y se hace hincapié en las tendencias consideradas:

1. Gagliardone, I. y cols. 2015. Countering Online Hate Speech (Contrarrestar la incitación al odio en Internet) UNESCO Series on Internet Freedom (Serie de la UNESCO sobre la libertad en Internet). París: UNESCO. http://unesdoc.unesco.org/images/0023/002332/233231e.pdf
2. Posetti, J. (de próxima publicación). *Protecting Journalism Sources in the Digital Age* (Protección de las fuentes periodísticas en la era digital) París: UNESCO
3. MacKinnon, R. y cols. 2014. Fomento de la libertad en la Red: El papel de los intermediarios en Internet) UNESCO Series on Internet Freedom (Serie de la UNESCO sobre la libertad en Internet). París: UNESCO / Internet Society. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

Esta publicación ha recibido el apoyo del Gobierno de Suecia.

También contribuyeron The Internet Society, las Open Society Foundations, el Center for Global Communication Studies de la Annenberg School for Communication de la Universidad de Pensilvania, la Universidad de Oxford, y el World Editors Forum de la Asociación Mundial de Periódicos y Editores de Noticias (WAN-IFRA).

Editor: Rachel Pollack Ichou
Diseño gráfico: UNESCO
Diseño de tapa: UNESCO
Ilustraciones: UNESCO
Composición: UNESCO
Impreso por: UNESCO

Impreso en Francia

Job 3181.15

Tendencias mundiales en libertad de expresión y desarrollo de los medios: consideración prioritaria del ámbito digital 2015

Editor: Rachel Pollack Ichou, Especialista de Proyecto, Sección de la Libertad de Expresión, División de la Libertad de Expresión y el Desarrollo de los Medios de Comunicación, UNESCO

Contrarrestar la incitación al odio en Internet

Autores:

Iginio Gagliardone, investigador docente en nuevos medios de comunicación y derechos humanos, Centro de Estudios Sociojurídicos, y miembro del Programa de políticas y derecho comparativo sobre medios de comunicación, Universidad de Oxford.

Danit Gal, candidato al título de máster en ciencias sociales de Internet, Universidad de Oxford.

Thiago Alves Pinto, candidato al doctorado en derecho, Universidad de Oxford.

Gabriela Martínez Sainz, candidata al doctorado en pedagogía, Universidad de Cambridge.

Bitange Ndemo, ex Secretario Permanente, Ministerio de Información y Comunicación, Kenya.

Nicole Stremlau, Director del Programa de políticas y derecho comparado sobre medios de comunicación, Universidad de Oxford.

Protección de las fuentes periodísticas en la era digital

Autor e investigador principal: Julie Posetti, antigua investigadora docente de la Asociación Mundial de Periódicos y Editores de Noticias (WAN-IFRA) y editora en el World Editors Forum (Foro Mundial de Editores de Noticias); profesora de radiodifusión y periodismo convergente en la Universidad de Wollongong.

Investigadores académicos:

Ying Chan, Director Fundador del Centro de Estudios de Periodismo y Medios de Comunicación de la Universidad de Hong Kong.

Marcus O'Donnell, profesor titular de periodismo, Facultad de Derecho, Humanidades y Bellas Artes de la Universidad de Wollongong.

Carlos Affonso Pereira de Souza, Vicecoordinador, Centro de Tecnología y Sociedad (CTS), Fundación Getulio Vargas (FGV), Facultad de Derecho, Río de Janeiro.

Doreen Weisenhaus, Directora del Proyecto sobre el derecho de los medios de comunicación y profesora asociada del Centro de Estudios de Periodismo y Medios de Comunicación de la Universidad de Hong Kong.

Ayudantes de investigación de postgrado y colaboradores de investigación de pregrado

Federica Cherubini, gestora de programas, WAN-IFRA.

Jake Evans, antiguo miembro en prácticas de periodismo en WAN-IFRA-Universidad de Wollongong; colaborador de la Australian Broadcasting Corporation (ABC).

Emma Goodman, responsable de investigación, LSE, Proyecto sobre políticas en materia de medios de comunicación, LSE.

Angelique Lu, periodista, BBC; y antigua miembro en prácticas de periodismo de WAN-IFRA-Universidad de Wollongong.

Alice Matthews, periodista, Australian Broadcasting Corporation (ABC) News; antigua ayudante de investigación, WAN-IFRA.

Alexandra Sazonova-Prokouran, estudiante, Universidad de Oxford; antigua miembro en prácticas de WAN-IFRA.

Jessica Sparks, estudiante de periodismo y derecho, Universidad de Wollongong, antigua miembro en prácticas de WAN-IFRA.

Nick Toner, cofundador y editor de VERSA News; antiguo miembro en prácticas de WAN-IFRA.

Farah Wael, coordinador, desarrollo de los medios de comunicación y libertad de prensa, WAN-IFRA.

Alexandra Waldhorn, responsable de comunicaciones, Instituto Internacional de Planeamiento de la Educación, UNESCO; antigua consultora en materia de juventud, WAN-IFRA.

Olivia Wilkinson, estudiante, Universidad de Oxford; antigua miembro en prácticas de WAN-IFRA.

Apoyo administrativo:

Ashleigh Tullis, periodista, Fairfax Media Wollondilly Advertiser; antiguo miembro en prácticas de periodismo en WAN-IFRA.

Comité Consultivo Internacional

Mark Pearson, profesor de periodismo y medios sociales, Griffith University.

Julie Reid, profesora titular de estudios sobre medios de comunicación, Departamento de Ciencias de la Comunicación, UNISA (Universidad de Sudáfrica).

Lillian Nalwoga, Presidenta, División de Uganda de Internet Society; responsable de políticas en Collaboration of International ICT Policy in East and Southern Africa (CIPESA).

Dan Gillmor, Director del Centro Knight para el emprendimiento en medios digitales, en la escuela Walter Cronkite de periodismo y medios de comunicación de masas de la Universidad Estatal de Arizona.

Prisca Orsonneau, miembro del Colegio de Abogados de París, especializada en derecho de los medios de comunicación y derechos humanos; Presidenta de Reporteros Sin Fronteras, Comité de Asuntos Jurídicos.

Gayathry Venkiteswaran, Directora Ejecutiva, Southeast Asian Press Alliance.

Mario Calabresi, Redactor Jefe, La Stampa.

Mishi Choudhary, Directora de Asuntos Jurídicos, Software Freedom Law Centre y SFLC.in.

Fomento de la libertad en la Red: El papel de los intermediarios en Internet

Autores:

Rebecca MacKinnon, Directora, Proyecto de clasificación de derechos digitales, New America Foundation; profesora asociada invitada, Centro de Estudios sobre Comunicación a Escala Mundial, Escuela Annenberg de Comunicación, Universidad de Pensilvania.

Elonnai Hickok, investigadora, Centre for Internet and Society.

Allon Bar, coordinador de investigación, Proyecto de clasificación de derechos digitales.

Hae-in Lim, investigadora, Proyecto de clasificación de derechos digitales.

Investigadores:

Sara Alsherif, investigadora, Programa sobre libertad de información, Centro de Apoyo a las Tecnologías de la Información.

Celina Beatriz Mendes de Almeida Bottino, Instituto de Tecnologia & Sociedade do Río de Janeiro.

Richard Danbury, investigador asociado, Facultad de Derecho, Universidad de Cambridge.

Elisabetta Ferrari, Centro de Medios de Comunicación, Información y Sociedad, Universidad Europea Central, Budapest; alumno de doctorado, Escual Annenberg de Comunicación, Universidad de Pensilvania.

Grace Githaiga, miembro asociado, Red de Acción sobre TIC de Kenya (KICTANet).

Kirsten Gollatz, Directora de Proyectos, Instituto Alexander von Humboldt de Internet y Sociedad.

Elonnai Hickok, investigadora, Centre for Internet and Society.

Hu Yong, Profesor Asociado, producción de películas y documentales, Escuela de Periodismo y Comunicación, Universidad de Pekín.

Tatiana Indina, candidata de ciencias, investigadora docente, Centro para el Estudio de los Nuevos Medios y la Sociedad.

Victor Kapiyo, Director de Programas – Protección de los Derechos Humanos, Sección de Kenya de la Comisión Internacional de Juristas (ICJ Kenya); Red de Acción sobre TIC de Kenya (KICTANet).

Peter Micek, Asesor Principal de Políticas, Access.

Agustín Rossi, candidato al doctorado, Instituto Universitario Europeo; profesor no residente, Instituto de Política Pública Global.

Comité Consultivo Internacional:

Renata Avila, Director Mundial de Campaña, iniciativa "Web We Want", Fundación World Wide Web; colaboradora, Global Voices.

Rasha Abdulla, profesora asociada y antigua presidenta, Periodismo y Comunicación de Masas, Universidad Americana en El Cairo.

Sunil Abraham, Director Ejecutivo, Centre for Internet and Society.

Peng Hwa Ang, profesor, Universidad Tecnológica Nanyang, Escuela de Comunicación Wee Kim Wee.

Eduardo Bertoni: Director del Centro de Estudios sobre Libertad de Expresión y

Acceso a la Información (CELE), Palermo, Facultad Universitaria de Derecho.

Seeta Peña Gangadharan, profesora de programas, New America's Open Technology Institute.

Leslie Harris, Directora, Harris Strategy Group LLC; antigua Presidenta y Primera Ejecutiva,

Centro para la Democracia y la Tencología.

Dunstan Allison Hope, Director Gerente, Servicios de Consultoría, BSR.

Rikke Frank Jørgensen, Consultor Principal, Instituto Danés para los Derechos Humanos.

Jeremy Malcolm, Analista Principal de Políticas Globales, Electronic Frontier Foundation.

Pranesh Prakash, Director Ejecutivo, Centre for Internet and Society.

Lucy Purdon, Directora de Programas: TIC, Institute for Human Rights and Business.

David Sullivan, Director de Políticas y Comunicaciones, Global Network Initiative.

Ben Wagner, Director, Centro de Internet y Derechos Humanos, Universidad Europea Viadrina.

La seguridad de los periodistas

Autor: Ming-Kuok Lim, Especialista Asistente de Programas, Sección de la Libertad de Expresión, División de la Libertad de Expresión y el Desarrollo de los Medios de Comunicación, UNESCO

Índice

Prólogo de Irina Bokova, Directora General de la UNESCO

La UNESCO celebra su 70º aniversario, y nuestro mandato fundacional de promover "la libre circulación de las ideas por medio de la palabra y de la imagen" nunca ha sido tan importante para impulsar el derecho a la libertad de expresión y fomentar la paz y el desarrollo sostenible a través de la libertad, el pluralismo y la independencia de los medios de comunicación, y la seguridad de los periodistas.

A lo largo de la Cumbre Mundial sobre la Sociedad de la Información (CMSI) y su proceso de seguimiento, la UNESCO ha promovido una visión de las sociedades del conocimiento integradoras fundada en los pilares de la libertad de expresión, el acceso universal a la información y el conocimiento, el respeto por la diversidad cultural y lingüística, y la educación de calidad para todos. Las Naciones Unidas revisan los 10 últimos años de CMSI y esperan asistir a los Estados miembros en la consecución de los Objetivos de Desarrollo Sostenible (ODS), y en este contexto, la labor de la UNESCO en tales áreas cobra una enorme relevancia, sobre todo en esta época de cambios tecnológicos revolucionarios y de profunda transformación de todas las sociedades.

El ámbito de la comunicación y la información a escala mundial se ha transformado a consecuencia de la generalización de las tecnologías digitales. En la actualidad, más de 3.000 millones de hombres y mujeres en todo el mundo utilizan Internet, y más de 6.000 millones disponen de acceso a teléfonos móviles. Estas tecnologías han ampliado las posibilidades de progreso hacia unas sociedades del conocimiento sostenibles, aunque también han dado lugar al planteamiento de nuevos desafíos.

En este dinámico panorama, la UNESCO recibió en noviembre de 2013 un llamamiento de sus 195 Estados miembros para la elaboración de un estudio exhaustivo sobre asuntos

relacionados con Internet en el ámbito de su mandato, haciendo hincapié en cuatro áreas: el acceso a la información y el conocimiento, la libertad de expresión, el respeto por la privacidad y el estudio de la ética de la información. En el estudio resultante, *Keystones to foster inclusive Knowledge Societies* (Claves para promover unas sociedades del conocimiento integradoras), se analizan estos temas, así como posibles opciones para la acción futura. Esta iniciativa se basó en el anterior mandato otorgado por los Estados miembros en la Conferencia General de la UNESCO en 2011, relativo al seguimiento de las tendencias mundiales en materia de libertad de expresión y desarrollo de los medios de comunicación. Se inspiró además en el primer informe de *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios*, publicado en 2014.

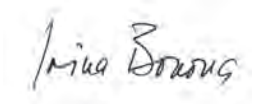
El informe sobre dichas Claves es único en la promoción del concepto de la "universalidad de Internet" para designar una Internet humana, basada en los derechos, abierta, accesible a todos, y gobernada mediante la participación de múltiples interlocutores, mostrando cómo Internet puede impulsar la consecución de diversos objetivos y metas de desarrollo sostenible, desde la erradicación de la pobreza, la realización de la igualdad de género y la garantía de unos patrones de consumo y producción sostenibles, a la lucha contra el cambio climático y el fomento de unas sociedades pacíficas e integradoras.

En este segundo informe sobre las *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios*, se ahonda en el análisis de determinados aspectos esenciales del estudio sobre las *Claves*. De este modo, se actualiza la primera edición de *Tendencias Mundiales*. Mientras que en dicha primera edición se abordaron un amplio número de cuestiones, en esta segunda versión se procura la profundidad con un tratamiento prioritario de cuatro tendencias específicas destacadas en el estudio sobre las Claves, avanzando así en el desempeño del papel de la UNESCO de fomentar el conocimiento y la capacidad de interpretación mediante la investigación de alta calidad que atañe a la construcción de las sociedades del conocimiento.

La investigación acometida para el presente informe no habría sido posible sin el apoyo continuo del Gobierno de Suecia, que agradezco encarecidamente. Deseo trasladar asimismo mi gratitud a la Internet Society, las Open Society Foundations, el Center for Global Communication Studies de la Annenberg School for Communication de la Universidad de Pensilvania, la Universidad de Oxford, y el World Editors Forum de la Asociación Mundial de Periódicos y Editores de Noticias (WAN-IFRA).

Estoy convencida de que *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios - Consideración prioritaria del ámbito digital 2015* se convertirá en una referencia para las administraciones públicas, la sociedad civil, el sector privado y el ámbito académico, así como para los estudiantes, en un período en el que la libertad de expresión nunca ha sido tan importante.

Irina Bokova



I. INTRODUCCIÓN

En 2011, en su 36ª Conferencia General, los 195 Estados Miembros de la UNESCO aprobaron una resolución en la que se encomendaba a la Organización a "vigilar, en estrecha colaboración con otros organismos del sistema de las Naciones Unidas y otras organizaciones competentes que actúan en este campo, la situación de la libertad de prensa y de la seguridad de los periodistas, prestando atención a los casos de impunidad de la violencia ejercida contra los periodistas..., y dar cuenta a la Conferencia General semestral de las novedades a este respecto".

En 2012, con el fin de llevar a cabo este mandato, y con el apoyo del Gobierno de Suecia, la UNESCO se embarcó un proyecto de investigación de gran escala con un grupo consultivo de 27 destacados expertos internacionales. Sobre la base de tal investigación, se elaboró un informe con un resumen de tendencias en el terreno de la libertad de prensa y la seguridad de los periodistas entre 2007 y mediados de 2013, presentado ante la 37ª Conferencia General en noviembre de 2013, bajo la forma de un panorama general que resultaba los principales hallazgos clave. La publicación final sobre las *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios* la puso en marcha la Directora General de la UNESCO en Estocolmo, Suecia, en marzo de 2014, y a continuación se presentó en las cinco regiones de la Organización.

El primer informe sobre las Tendencias Mundiales salvó una importante brecha en la investigación contemporánea sobre medios y comunicación. Aunque otros estudios e informes habían ofrecido instantáneas de dimensiones o regiones específicas, *Tendencias Mundiales* fue el primero en presentar un análisis sistemático de tendencias respecto a los múltiples aspectos de la libertad, el pluralismo, la independencia y la seguridad de los medios de comunicación, prestando especial atención además a las consideraciones relacionadas con el género.

Dado el éxito del primer informe de *Tendencias Mundiales* y la necesidad de una investigación ulterior, la UNESCO emprendió una segunda edición en la serie, en la que se hace hincapié en determinadas tendencias de la era digital. *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios - Consideración prioritaria del ámbito digital 2015* proporciona un análisis significativo de las áreas clave identificadas en la primera edición del informe como de especial relevancia para un estudio ulterior, y en concreto, de la incitación al odio en Internet, la protección de las fuentes periodísticas, y el papel de los intermediarios de Internet en el fomento de la libertad de expresión, así como de la atención prioritaria continuada a la seguridad de los periodistas. Se basa asimismo en los asuntos planteados en el estudio de 2015 de la UNESCO titulado *Keystones to foster inclusive Knowledge Societies* (Claves para promover unas sociedades del conocimiento integradoras).

Por consiguiente, la publicación actual contiene cuatro capítulos temáticos:

1. En **Contrarrestar la incitación al odio en Internet**, se ofrece una visión global de las dinámicas que caracterizan la incitación al odio en la Red, y de algunas de las medidas que se han adoptado para contrarrestar y atenuar tal práctica, subrayando las tendencias en cuanto a buenas prácticas que han surgido a escala local y mundial.

Se realiza un análisis pormenorizado de los marcos normativos internacionales, regionales y nacionales desarrollados para abordar la incitación al odio en Internet, y de sus repercusiones en la libertad de expresión, y se hace especial hincapié en los mecanismos sociales y no regulatorios que pueden considerarse para contribuir a contrarrestar la producción, la divulgación y el impacto de los mensajes de odio en la Red.

2. **Protección de las fuentes periodísticas en la era digital** se inspira en una investigación que abarca a 121 Estados miembros de la UNESCO, y que actualiza un estudio anterior de estos países a cargo de la ONG Privacy International en 2007. En el capítulo se muestra el modo en que los marcos jurídicos que sostienen la protección de las fuentes periodísticas a escala internacional, regional y nacional se han visto sometidos a tensiones significativas en los años transcurridos. Corren un riesgo cada vez mayor de erosión, restricción y de verse comprometidos. Se trata de una tendencia que supone un reto directo para los derechos humanos universales consolidados de libertad de expresión y respeto de la privacidad, y que constituye una amenaza concreta para la sostenibilidad del periodismo de investigación. Una recomendación para su consideración derivada de dicha investigación es la propuesta de una herramienta de 11 puntos concebida para evaluar la eficacia de los marcos jurídicos de protección de las fuentes en la era digital.

3. **Fomento de la libertad en la Red:** el papel de los intermediarios de Internet arroja luz sobre estos agentes: los servicios que actúan como intermediarios en las comunicaciones en línea y posibilitan diversas formas de expresión en la Red. Se muestra como promueven y restringen a la vez la libertad de expresión en diversas jurisdicciones, circunstancias, tecnologías y modelos de negocio. De acuerdo con los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, aunque los Estados tienen la obligación principal de proteger los derechos humanos, las empresas son responsables de respetarlos, y ambos deben desempeñar un papel en la provisión de mecanismos de reparación a aquellos cuyos derechos han sido violados. En este capítulo se aplica el marco de "proteger, respetar y remediar" a las políticas y las prácticas de las empresas que representan a tres tipos de intermediarios (proveedores de servicios de Internet, motores de búsqueda, y plataformas de redes sociales) en 10 países. En los tres estudios de caso se incide en los retos y las oportunidades planteados a los diferentes tipos de intermediarios, en el contexto de la tendencia a su importancia creciente.

4. En **La seguridad de los periodistas** se examinan las tendencias recientes en este campo, se presentan las estadísticas de la UNESCO correspondientes a 2013 y 2014, y se lleva a cabo un seguimiento de otras situaciones hasta agosto de 2015. Se aplica el marco del anterior informe de la UNESCO sobre Tendencias Mundiales, en el que se incluyen la seguridad física, la impunidad, el encarcelamiento de periodistas, y una dimensión de género respecto a las distintas cuestiones consideradas. Por otra parte, en el capítulo se examina la tendencia sin precedentes al refuerzo de las normativas internacionales, así como la reciente evolución de los mecanismos prácticos, la mejora de la cooperación entre organismos de las Naciones Unidas, la

mayor colaboración con el sistema judicial y las fuerzas de seguridad, y el interés en este tema en el ámbito de la investigación.

Además de contribuir al presente informe y al estudio exhaustivo de la UNESCO sobre asuntos relacionados con Internet (véase *UNESCO: Promoting Freedom of Expression and Media Development*), los capítulos sobre la incitación al odio en Internet y el papel de los intermediarios se han presentado como publicaciones independientes de mayor extensión en la Serie emblemática de la Organización sobre la libertad en Internet.

Se presta especial atención a lo largo de este nuevo estudio de las *Tendencias Mundiales* a la igualdad de género, una de las dos prioridades globales de la UNESCO. Como en el primer informe de Tendencias Mundiales, el género se conceptualiza fundamentalmente aquí en referencia a las experiencias de las periodistas y el efecto de las políticas y las prácticas en las mujeres.

Las tendencias identificadas en el presente informe arrojan luz sobre los cambios en el panorama de oportunidades y retos que atañen a la libertad de expresión y al desarrollo de los medios, y en especial sobre los que generan las tecnologías digitales. Mediante la puesta en común de conocimientos y buenas prácticas, la UNESCO trabaja para promover los derechos humanos en la era digital: contrarrestando la incitación al odio en Internet, protegiendo las fuentes periodísticas, fomentando la libertad en línea mediante la puesta en común de buenas prácticas para los intermediarios de Internet, y potenciando la seguridad de los periodistas, tanto en plataformas tradicionales, como en línea.

II. UNESCO: APOYO A LA LIBERTAD DE EXPRESIÓN Y EL DESARROLLO DE LOS MEDIOS

La UNESCO es la agencia de las Naciones Unidas con el mandato específico de defender la libertad de expresión, y según su Constitución debe facilitar "la libre circulación de las ideas por medio de la palabra y de la imagen". Esta misión la refuerza la Declaración Universal de Derechos Humanos, en la que se afirma que "Todo individuo tiene derecho a la libertad de opinión y de expresión". Tanto la libertad de expresión como sus corolarios, la libertad de información y la libertad de prensa, son conceptos que se aplican a todos los medios de comunicación, incluidos los gráficos y de radiodifusión tradicional, y también a los medios digitales, de más reciente desarrollo.

En 2013, la Conferencia General de los 195 Estados Miembros de la UNESCO adoptó la Resolución 52, en la que se recuerda la Resolución A/HRC/RES/20/8 del Consejo de Derechos Humanos, "Promoción, protección y disfrute de los derechos humanos en Internet", y en la que se afirma que los mismos derechos que asisten a las personas al margen de Internet deben protegerse igualmente en la Red. Tales derechos atañen a todas las áreas de competencia de la UNESCO, además de ser críticas para el desarrollo sustentable, la democracia y el diálogo. Los Estados Miembros han dirigido un llamamiento a la UNESCO para que esta se encargue del seguimiento de las tendencias relativas a estos derechos, y en especial, al derecho a la libertad de expresión. En la Resolución 53, convenida en la 36ª sesión de la Conferencia General, se encomendaba a la Organización a "vigilar, en estrecha colaboración con otros organismos del sistema de las Naciones Unidas y otras organizaciones competentes que actúan en este campo, la situación de la libertad de prensa y de la seguridad de los periodistas, prestando atención a los casos de impunidad de la violencia ejercida contra los periodistas, entre otras cosas manteniéndose informada sobre su seguimiento judicial por conducto del Consejo Intergubernamental del Programa Internacional para el Desarrollo de la Comunicación (PIDC), y dar cuenta a la Conferencia General de las novedades a este respecto". En esta Resolución se basó el primer informe de *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios* [1], que se puso en marcha en seis ciudades de todo el mundo, y que comprende seis subestudios regionales. En el presente estudio se da continuidad a dicho mandato, y se utiliza el marco conceptual del primer informe de *Tendencias Mundiales*, en el que se hace hincapié en las cuestiones de libertad, pluralismo, independencia, seguridad y género. El presente estudio también se fundamenta en el mandato de la 37ª Conferencia General de 2013, en cuya Resolución 52 se insta a la elaboración de un estudio consultivo de amplio alcance sobre las cuatro dimensiones de Internet y su relación con la misión de la UNESCO. En dicho estudio, publicado bajo el titulo de *Keystones to foster inclusive Knowledge Societies* (Claves para promover unas sociedades del conocimiento integradoras), se examina el acceso a la información y el conocimiento, la libertad de expresión, el respeto por la privacidad y las dimensiones éticas de la sociedad de la información.

Basándose en estas referencias, la UNESCO reconoce que las tecnologías digitales desempeñan un papel cada vez más destacado en la sociedad, y en este sentido, los asuntos que atañen a la libertad de expresión en Internet y su interfaz con el mundo real "fuera de línea", requieren igualmente la atención de la Organización. Un ejemplo a este

1 http://www.unesco.org/new/en/world-media-trends.

respecto es el de la seguridad de los periodistas y la cuestión de la impunidad, que es objeto de uno de los capítulos del presente informe de *Tendencias Mundiales*. Lo que sucede en este terreno en el mundo real influye de manera notable en lo que ocurre en las dimensiones en línea, y viceversa. La falta de seguridad en uno de los ámbitos repercute en la seguridad existente en el otro. Por este motivo, la UNESCO presta cada vez una mayor atención a las interfaces entre ambos.

En lo que se refiere a los programas, la UNESCO trabaja en todo el mundo para promover la libertad de expresión en todas las plataformas, tanto en Internet, como fuera de línea, así como las interrelaciones entre las dos. Se otorga prioridad a ambas dimensiones, como reflejo de los lados de *salida* y de *entrada* del proceso de comunicación:

La primera dimensión de la libertad de expresión consiste en el derecho a *impartir* información y opinión. Tal es el fundamento del derecho a la libertad de prensa, que se refiere a la libertad para publicar con una audiencia amplia como destinataria de la publicación. En la era digital, este derecho atañe especialmente a todo aquel que utilice medios de comunicación tradicionales o sociales. Para la UNESCO, la libertad de prensa efectiva se basa en la libertad, el pluralismo, la independencia y la seguridad de los medios de comunicación. Y esto se aplica a todos los medios, incluidos los creativos y sociales, y no solo a los dedicados a la difusión de noticias. Con esta perspectiva, el asunto de la independencia reviste especial importancia para aquellos que utilizan la libertad de prensa para ejercer el periodismo. La independencia requiere de libertad y pluralismo, y en el caso del periodismo, ya sea en Internet o fuera de línea, esto se basa en la existencia de estándares profesionales para la producción y la distribución de información verificable en interés del público.

En resumen, la libertad de expresión es la madre de la libertad de prensa, entendida como el uso del derecho a impartir información a gran escala. La libertad, el pluralismo, la independencia y la seguridad de los medios de comunicación constituyen el entorno propicio esencial para el ejercicio de la libertad de prensa. Es en dicho contexto en el que el periodismo profesional, hijo de la libertad de expresión, puede prosperar y contribuir a la construcción de las sociedades del conocimiento.

La segunda dimensión de la libertad de expresión es el derecho a *buscar* y *recibir* información, lo que constituye el fundamento del derecho a la información. A su vez, representa uno de los fundamentos de la transparencia, a la que se le reconoce su carácter esencial para el desarrollo y la democracia. Las tecnologías digitales propician enormes avances en el terreno de la transparencia, en lo que atañe tanto a las instituciones públicas, como a las privadas, dando lugar a una asunción de responsabilidades y a un empoderamiento de los ciudadanos sin precedentes.

Estas dos dimensiones de la libertad de expresión se encuentran cada vez más interrelacionadas con el derecho a la privacidad, con sinergias potenciales, y también con tensiones. Una sólida protección de la privacidad puede reforzar la capacidad del periodismo para servirse de fuentes confidenciales en la obtención de información de interés público, pero también puede menoscabar la transparencia y ocultar información

objeto de un posible interés público legítimo. Una protección débil de la privacidad puede dar lugar a que las fuentes periodísticas retengan la información o practiquen la autocensura por temor a ser víctimas de una vigilancia arbitraria. También puede propiciar una extralimitación en el terreno de la transparencia, y en este sentido, una intrusión injustificada en la vida privada de las personas. La confianza en los beneficios de las comunicaciones digitales puede verse afectada por el modo en el que la sociedad aborda el derecho a la privacidad con las dos dimensiones del derecho a la libertad de expresión.

Gran parte del trabajo de la UNESCO proporciona elementos para la reflexión sobre la manera en que pueden respetarse cada uno de estos dos derechos, tanto en línea, como fuera de ella, y en los ámbitos en los que tales derechos entran en contacto, y sobre el modo en que pueden equilibrarse de forma armoniosa, sirviendo al interés público, cuando resulte necesario. La Organización aborda esta cuestión mediante el desempeño de tareas de investigación, vigilancia, sensibilización, defensa de derechos, refuerzo de capacidades, y asesoramiento técnico. El Programa Internacional para el Desarrollo de la Comunicación (PIDC) de la UNESCO también proporciona apoyo a los proyectos pertinentes a favor de unos medios de comunicación libres, plurales, independientes y seguros, tanto en Internet, como en otras plataformas convencionales.

En lo que se refiere al establecimiento de estándares respecto a la defensa de la libertad de expresión y la privacidad en línea, la UNESCO ha participado activamente en diversos procesos globales y regionales, y ha contribuido a los mismos, entre los que figuran los Principios de gobernanza de Internet y la hoja de ruta para la evolución futura de la gobernanza de la Red de NETmundial, la Recomendación del Consejo de Europa sobre la libertad en Internet, la Declaración africana de derechos y libertades de Internet, y el proyecto del Séptimo Programa Marco de la Unión Europea sobre “Alternativas de gestión para la privacidad, la propiedad y la gobernanza de Internet”.

Por otra parte, la Organización aboga en todo el mundo por la libertad de expresión y el respeto de la privacidad en Internet, y colabora con interlocutores relevantes en el marco de foros, iniciativas y reuniones de escala mundial, regional y nacional. Entre tales foros figuran el Foro para la Gobernanza de Internet (IGF), el proceso de la CMSI, la Iniciativa de NETmundial, la Asociación Internacional de Estudios en Comunicación Social, el Global Media Forum, la Freedom Online Coalition y diversos IGF regionales.

Como resultado de la Resolución 52, y como se señala anteriormente, la UNESCO llevó a cabo el estudio titulado *Keystones to foster inclusive Knowledge Societies* (Claves para promover unas sociedades del conocimiento integradoras), atendiendo la petición formulada por los Estados miembros relativa a la necesidad de priorizar el acceso a la información y el conocimiento, la libertad de expresión, el respeto de la privacidad y las dimensiones éticas de la sociedad de la información. La actividad se refirió a la 38ª Conferencia General en el marco del Informe a cargo del Director General sobre la

aplicación en la práctica de los resultados de la Cumbre Mundial sobre la Sociedad de la Información (CMSI)[2].

Con arreglo a su mandato, la UNESCO elaboró el estudio mediante la puesta en marcha de un proceso incluyente en el que participaron diversos interesados, entre ellos gobiernos, el sector privado, la sociedad civil, distintas organizaciones internacionales y los círculos técnicos. En julio de 2014 se presentó un cuestionario en línea, y se solicitaron aportaciones a través de los medios sociales y foros de relevancia, y también de manera directa a los Estados miembros y a más de 300 expertos y organizaciones, representantes de la sociedad civil, el ámbito académico, el sector privado, la comunidad técnica y varios organismos intergubernamentales. A finales de noviembre de 2014, la UNESCO había recibido 200 respuestas fundadas al cuestionario. También se procuraron las contribuciones al estudio en foros mundiales dedicados a asuntos relacionados con Internet, y en noviembre de 2014, en el marco de la 29ª reunión del Consejo del PIDC, se celebró un debate sobre la libertad de expresión y el respeto de la privacidad en línea. Paralelamente a las consultas con numerosas partes interesadas, la UNESCO encargó una serie de publicaciones sobre determinados subtemas, con el fin de ofrecer un análisis pormenorizado y diversas recomendaciones a sus Estados miembros y a otros interlocutores sobre asuntos relacionados con la libertad en Internet. Estos estudios complementarios contribuyeron al estudio principal sobre Internet, y algunos de ellos también se publicaron de manera independiente en la Serie emblemática de la Organización sobre la libertad en la Red[3].

Además de los estudios complementarios que han contribuido igualmente a la elaboración de los tres capítulos que figuran en la presente publicación (a saber, *Contrarrestar la incitación al odio en Internet*, *Protección de las fuentes periodísticas en la era digital*, y *Fomento de la libertad en la Red: el papel de los intermediarios en Internet*), la UNESCO ha encargado una amplia gama de estudios en el marco de la Serie sobre la libertad en Internet, en el contexto de la Resolución 52 de 2013 adoptada por la Conferencia General:

1. **Building Digital Safety for Journalism: A Survey of Selected Issues:** (El fomento de la seguridad digital para el periodismo: encuesta sobre ciertas cuestiones) A la vista del limitado conocimiento general de las amenazas emergentes para la seguridad asociadas a la evolución en el ámbito digital, la UNESCO encargó este estudio en el marco de las iniciativas en curso de la Organización encaminadas a la ejecución del Plan de acción de las Naciones Unidas sobre la seguridad de los periodistas y la cuestión de la impunidad. Mediante el examen de casos de todo el mundo, la publicación constituye un recurso para diversos agentes, al analizar la evolución de distintas amenazas y evaluar las medidas preventivas, protectoras y prioritarias asociadas. Pone de relieve que la seguridad digital para el periodismo engloba la dimensión técnica, pero también la trasciende. Se proponen varias

2 http://unesdoc.unesco.org/images/0023/002341/234144e.pdf.

3 Véase UNESCO. *UNESCO Series on Internet Freedom* (Serie de la UNESCO sobre la libertad en Internet). http://www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/publications-by-series/unesco-series-on-internet-freedom/.

recomendaciones para su consideración por los Estados miembros, relativas a las administraciones públicas, fuentes y colaboradores periodísticos, medios de comunicación, formadores, corporaciones y organismos internacionales.

2. **Principios para el gobierno de Internet: un análisis comparativo**: Este estudio contiene la revisión de más de 50 declaraciones y marcos específicos de Internet que atañen a los principios para el gobierno de la Red, y se puso en marcha a raíz de la necesidad de emprender un análisis concreto de tales declaraciones y marcos desde la perspectiva del mandato de la UNESCO. La publicación pone de relieve que, aunque cada uno de los documentos examinados tiene su propio valor, ninguno de ellos se ajusta plenamente a las prioridades y el mandato de la Organización. Asimismo, somete a la consideración de los Estados Miembros el concepto de "la universalidad de Internet", como elemento identificador inequívoco de la UNESCO para abordar los diversos ámbitos de los asuntos relacionados con Internet y sus interrelaciones con las cuestiones de interés para la Organización. Dicho concepto atañe a la labor de la UNESCO en numerosas áreas, entre las que figuran la libertad de expresión y el respeto por la privacidad en línea; los esfuerzos dedicados al fomento de la universalidad en la educación, la integración social y la igualdad de género; el plurilingüismo en el ciberespacio; el acceso a la información y el conocimiento; y las dimensiones éticas de la sociedad de la información.

3. **Concesión de licencias en línea y libertad de expresión**: La UNESCO encargó una investigación sobre la cuestión de la concesión de licencias en línea y la libertad de expresión, particularmente en lo que se refiere al periodismo. Restringir el acceso a la utilización de un medio de comunicación es un asunto directamente relacionado con la libertad de prensa. Tal restricción ha surgido como enfoque complementario a las prácticas consolidadas de filtrado y bloqueo, que repercuten especialmente en el derecho a buscar y recibir información. Desde el punto de vista de los estándares internacionales, la libertad de expresión es la norma y las restricciones, la excepción. Cuando el registro equivale a la obtención de una licencia en el sentido de ser tanto obligatorio, como exclusivo, puede percibirse como una forma de restricción previa. Por consiguiente, se requieren pruebas rigurosas para garantizar que el registro pueda justificarse conforme a los estándares internacionales de necesidad, proporcionalidad, procedimiento debido y finalidad legítima. El objeto de esta investigación consiste en proporcionar respuestas contemporáneas y basadas en datos contrastados a las preguntas que rodean a la cuestión de la publicación en línea previa autorización que han planteado diversos regímenes jurídicos, normativos y de formulación de políticas recientes.

4. **Privacidad y alfabetización mediática e informacional:** La UNESCO lleva a cabo un estudio de alcance mundial sobre la privacidad y la alfabetización mediática e informacional (MIL por sus siglas en inglés). Se examina el asunto de los usuarios de Internet que disponen de competencias en materia de MIL relativas a las diversas dimensiones de la privacidad, como las que atañen al conocimiento de los derechos a la privacidad en el ciberespacio, incluidos los regímenes nacionales de protección de datos; a la capacidad para evaluar el modo en que se respeta la privacidad en

los contenidos digitales y las comunicaciones a los que acceden los usuarios; y a la capacidad para evaluar las limitaciones legítimas de la privacidad en Internet. En el estudio se procura información sobre todas estas cuestiones, tanto a través de la ordenación de los datos de disposición pública en determinados países y regiones, como mediante el análisis de la práctica en materia de MAI en esos mismos ámbitos.

5. **El equilibrio de la privacidad y la transparencia:** La UNESCO encargó un estudio de alcance mundial sobre el equilibrio de la privacidad y la transparencia, y esta se evaluó con arreglo a su relación con la libertad de expresión. En el estudio se escudriña la complejidad del asunto a través de la información, tanto normativa, como empírica, y se extiende el análisis a las distintas partes interesadas, entre las que figuran personas físicas, la sociedad civil, el sector privado y la administración pública. También se aborda la cuestión de la confianza del usuario en que los datos personales no devengan transparentes de manera ilegítima. Se esbozarán los riesgos para la privacidad personal derivados de la transparencia, así como los riesgos que plantea el respeto por la privacidad para la transparencia. Se efectuarán análisis de ciertos casos que ponen de relieve los asuntos planteados y las lecciones que se derivan de los mismos. Se identifican además las buenas prácticas en la conciliación de la privacidad y la transparencia, teniendo en cuenta su correspondencia con las normas internacionales pertinentes.

6. **Privacidad y cifrado:** En este estudio se analiza la disponibilidad de diferentes medios de cifrado y sus posibles aplicaciones, y se refiere brevemente la situación existente en el terreno de las tecnologías de cifrado empleadas en Internet y en los sectores de las comunicaciones. Se analiza asimismo la relación entre el cifrado y los derechos humanos en el ámbito internacional, y se incluyen casos pertinentes de escala nacional. El estudio proporciona una visión global de la evolución jurídica respecto a las restricciones impuestas por las administraciones públicas en materia de cifrado en ciertas jurisdicciones, y se revisan las opciones de la política de cifrado en el plano internacional, incluidas diversas ideas para promover la "alfabetización" en este terreno.

Mediante la consulta con diversos interlocutores y los estudios complementarios emprendidos, la UNESCO determinó que cuatro campos de investigación constituyen piedras angulares interdependientes en lo que se refiere a Internet. Publicado bajo el título de *Keystones to foster inclusive Knowledge Societies* (Claves para promover unas sociedades del conocimiento integradoras), el estudio incide en el interés generalizado en un futuro en el que Internet constituya un recurso abierto, fiable y global, accesible para todos de manera equitativa en todo el mundo. Se analizan diversas cuestiones relacionadas con la tecnología y la formulación de políticas en lo que atañe a la provisión de apoyo para un acceso más amplio y equitativo a la información y el conocimiento, para el refuerzo de la libertad de expresión como instrumento de los procesos democráticos y la asunción de responsabilidades, y para el fomento de la privacidad de la información personal.

En *Keystones* se concluye que la libertad de expresión no es un resultado inevitable de las nuevas tecnologías. Se determina más bien que ha de recibir el apoyo de la política y de la práctica, y que requiere confianza en Internet como un canal seguro para la expresión de las opiniones propias. La creciente preocupación por la vigilancia y la práctica del filtrado en Internet, por ejemplo, han dado lugar a la percepción de que la libertad de expresión en la Red se ve cada vez más amenazada, y que se requieren grandes esfuerzos para generar confianza en la privacidad, la seguridad y la autenticidad de la información y el conocimiento accesibles en línea, así como para proteger la seguridad y la dignidad de los periodistas, los usuarios de las redes sociales, y de aquellos que imparten información y opinión en Internet.

Por otra parte, en *Keystones* se establece que la libertad de expresión en línea está vinculada al principio de apertura, particularmente por lo que respecta a las normas internacionales que promueven la transparencia en relación con las restricciones al derecho de expresión. Las oportunidades abiertas para compartir ideas e información en Internet constituyen un elemento esencial de la labor de la UNESCO de promoción de la libertad de expresión, el pluralismo de los medios de comunicación y el diálogo intercultural. Para la UNESCO, la libertad de expresión en línea depende también de cómo utiliza la gente su acceso a Internet y las TIC afines para expresarse. La alfabetización mediática e informacional para todos, hombres y mujeres, atañe a esta cuestión, incluida la implicación de los jóvenes y la lucha contra toda forma de odio, racismo y discriminación, además del extremismo violento, en los contextos digitales, desde el correo electrónico, a los videojuegos en línea.

Para debatir sobre el borrador del estudio de *Keystones*, la UNESCO organizó una conferencia denominada “CONNECTing the Dots: Options for Future Action”, con unos 400 participantes representantes de cinco continentes, celebrada en la sede principal de la UNESCO en París en marzo de 2015. El evento constituyó una plataforma para examinar los resultados del estudio en preparación, de cara a su culminación, y contó con las presentaciones llevadas a cabo por una amplia gama de ponentes de todo el mundo. Tras la consecución de un acuerdo abrumador, esta reunión de múltiples interlocutores adoptó un Documento final en el que se subraya la relevancia de Internet para el progreso humano y su papel en el fomento de unas sociedades del conocimiento integradoras. En dicho Documento se afirman los principios de los derechos humanos que subyacen al enfoque de la UNESCO respecto a los asuntos relacionados con Internet, y se apoyan los principios de universalidad de la Red que promueven una Internet abierta, basada en los derechos, accesible para todos y caracterizada por la participación de múltiples partes interesadas. El análisis contenido en Keystones establece que estos cuatro principios determinan la lógica que rige la contribución al desarrollo ulterior de Internet a través de vías que refuercen el acceso a la información y el conocimiento, la libertad de expresión, el respeto de la privacidad, y la ética.

En una resolución adoptada por la 196º Consejo Ejecutivo de la UNESCO en abril de 2015 se recomienda que el Documento final de la conferencia *CONNECTing the Dots* sea considerado por la 38ª sesión de la Conferencia General y se remita como aportación no vinculante a la Agenda de Desarrollo posterior a 2015, al proceso general de revisión

de la CMSI de la Asamblea General de la ONU, y a la reunión de alto nivel de la Asamblea General establecida con arreglo a la Resolución 68/302 de la Asamblea General. Este Documento final se refleja en las opciones para la acción futura, como se esboza en el estudio de *Keystones*.

Paralelamente, la UNESCO ha contribuido a conformar la agenda de desarrollo sostenible posterior a 2015 mediante la convocatoria de reuniones sobre las Líneas de Acción de la CMSI y los eventos del IGF, con el fin de incidir en el papel primordial de unos medios de comunicación libres, independientes y pluralistas y los principios de universalidad de Internet en los objetivos de desarrollo sostenible. En el foro 2015 de la CMSI, la UNESCO presentó *Keystones* y organizó la 10ª reunión de facilitación de la Línea de Acción C9 Medios de la CMSI. Se aprobaron tres seminarios y un foro abierto para la 10º IGF en Brasil en noviembre de 2015.

Mediante una investigación de vanguardia y sus aportaciones al diálogo entre múltiples partes interesadas, la UNESCO ha conformado su implicación en este ámbito de manera general, con la intención de promover los derechos fundamentales de la libertad de expresión y el respeto de la privacidad, tanto en Internet, como fuera de línea, en una era digital cada vez más consolidada.

III. CONTRARRESTAR LA INCITACIÓN AL ODIO EN INTERNET[4]

4 Este capítulo se basa en Gagliardone, I. y cols. 2015. Countering Online Hate Speech (Contrarrestar la incitación al odio en Internet) UNESCO Series on Internet Freedom (Serie de la UNESCO sobre la libertad en Internet). París: UNESCO. http://unesdoc.unesco.org/images/0023/002332/233231e.pdf.

1. INTRODUCCIÓN

A medida que aumenta el número de participantes en el discurso en Internet, se presta mayor atención a la tendencia a la incitación al odio en la Red. También resulta evidente que, tras el acaecimiento de sucesos dramáticos, es habitual que se realicen llamamientos a favor de medidas más restrictivas o intrusivas para contener el potencial de Internet para la propagación del odio y la violencia, aún cuando los vínculos entre el discurso y la acción, y entre los contenidos en línea y la violencia en el mundo real no se han determinado con claridad. Comprender esta cuestión, y las tendencias de respuesta a la misma, requiere el análisis de diversos asuntos, empezando por el modo en que se conceptualiza el fenómeno. En este capítulo figura tal conceptualización, con referencia a debates recientes, y se evalúa asimismo la evolución de las normativas internacionales. Se reconoce la tendencia de las empresas privadas de Internet a actuar cada vez más en lo que se refiere a la incitación al odio, y se refieren los estándares internacionales que les son aplicables. Por último, se examina la relevancia en términos más generales de las tendencias emergentes en cinco respuestas sociales a la incitación al odio en línea. Se trata en concreto de: i) los esfuerzos dedicados en el terreno de la investigación a vigilar el modo en que surge y se propaga la incitación al odio en Internet, y al desarrollo de sistemas de alerta temprana y de métodos para distinguir entre diferentes tipologías de actos de incitación; ii) las acciones coordinadas por miembros de la sociedad civil con las que se procura la creación de coaliciones nacionales e internacionales; iii) las iniciativas para animar a las plataformas de redes sociales y a los proveedores de servicios de Internet a desempeñar un papel más sólido en la respuesta activa a la incitación al odio en línea; iv) las campañas e iniciativas de alfabetización mediática e informacional encaminadas a preparar a los usuarios para interpretar y reaccionar ante mensajes de odio; y v) la moderación de la expresión del odio en los medios de información. Por último, en el capítulo se indican las cuestiones clave de las tendencias futuras en lo que respecta a las interpretaciones de la incitación al odio y los asuntos jurídicos, con una recapitulación de los puntos esenciales.

1.1 UNA CONCEPTUALIZACIÓN GENERAL

La incitación al odio mantiene relaciones complejas con la libertad de expresión; los derechos individuales, colectivos y de las minorías; y los conceptos de dignidad, igualdad y seguridad personal. Su definición se rebate a menudo. Como se esboza en el apartado 1.2 posterior, en la normativa internacional y en numerosas leyes, la incitación al odio equivale a las expresiones que animan a que se cause daño a una víctima debido a la identificación de esta con un determinado grupo social o demográfico. En el caso del odio por motivos de raza, el Derecho internacional incluye las expresiones afines que podrían propiciar un clima de prejuicio e intolerancia. En el lenguaje coloquial, las definiciones de la incitación al odio tienden a ser aún más amplias, y se extienden para comprender

términos de insulto a los que ejercen el poder, o que resultan despectivos para los que se encuentran en situaciones de especial visibilidad. Que se den tales variaciones en cuanto a los referentes pone de relieve una tendencia actual a la inexistencia de una única interpretación convenida, y que el término "incitación al odio" sigue siendo un "cajón de sastre" cuyo significado puede englobar numerosas formas de manifestación.

Concebido en su sentido más amplio, la "incitación al odio" es motivo de preocupación no solo porque se perciba a menudo como una ofensa en principio, sino también porque suele asumirse que puede alimentar ciertas actuaciones que dan lugar a la violación de derechos en la práctica. La conexión entre la expresión y la acción dista mucho de ser automática, pero, especialmente en momentos críticos como unas elecciones, la sensibilidad es mayor. Al mismo tiempo, el uso del término "incitación al odio" puede dar lugar también a la manipulación: es posible que se intercambien acusaciones de fomentar este tipo de discurso entre los oponentes políticos, o que tales acusaciones sean utilizadas por los que ejercen el poder para contener las disensiones y las críticas.

Con el fin de abarcar el mayor ámbito posible, en este capítulo se utiliza el término "incitación al odio" de manera pragmática, para posibilitar la revisión de diversas definiciones y prácticas reunidas bajo una rúbrica amplia. Así, aunque una conceptualización definitiva de la incitación al odio no resulta sencilla, en el presente capítulo se utiliza el término para cubrir el discurso que sirve a fines de degradación o deshumanización. Sobre la base de la labor del profesor Jeremy Waldron, de la Facultad de Derecho de la Universidad de Nueva York, en el capítulo se reconoce que una expresión que pueda considerarse "de odio" conlleva dos significados. El primero atañe al mensaje dirigido al grupo destinatario que deshumaniza y menoscaba a los miembros asignados a dicho grupo. El segundo consiste en hacer saber a otros con puntos de vista similares que no están solos, y reforzar un sentimiento de pertenencia a un colectivo. La "incitación al odio" en este sentido se basa en las tensiones, que se pretenden reproducir y amplificar, y une y divide al mismo tiempo. Genera una oposición entre "nosotros" y "ellos". En el presente capítulo, el término "incitación al odio" se utiliza en general en este sentido más amplio de identidades de grupos en oposición, sin restringir el significado a los casos en los que existe una incitación específica a causar daño. Se emplea asimismo sin el supuesto de que tal discurso del odio sirva para estimular actuaciones nocivas en la práctica.

Existen claramente varios ejes en torno a los que pueden generarse el odio, como la raza, la etnia, el idioma, el género, la religión, la preferencia sexual o la nacionalidad. Sin embargo, también está claro que unas opiniones firmes respecto a determinadas ideas no deben confundirse *per se* con la incitación al odio. Esta práctica concierne al antagonismo entre personas, y no a las ideas abstractas. No engloba la hostilidad respecto a ideologías políticas, fes o creencias, aún cuando se clasifique con arreglo a las mismas a las víctimas humanas de este tipo de abuso: es necesario tener presente una distinción para evitar que el término "incitación al odio" abarque demasiado.

Dado que la incitación al odio como concepto ha sido rebatida por su excesivo alcance y por ser susceptible de manipulación, ha surgido una tendencia en los últimos tiempos para promover conceptos más restringidos, incluida la limitación de tal denominación a

los casos de incitación que podrían describirse como de "discurso peligroso" o "discurso del miedo". Tales conceptos se han fomentado para hacer hincapié en la capacidad del lenguaje para causar daño en la práctica y dar lugar a consecuencias violentas. Aunque la incitación al odio se observa, en diversas formas y modalidades, en numerosos contextos, el concepto de "discurso peligroso" surgió en torno a 2010. Como avanzó Susan Benesch, del Berkman Center for Internet and Society, con dicho concepto se pretende aislar aquellos actos con una probabilidad significativa de "catalizar o amplificar la violencia ejercida por un grupo contra otro". El concepto de "discurso del miedo" planteado por Antoine Buyse, director del Instituto de los Derechos Humanos de los Países Bajos, también se ha promovido recientemente para incidir en el lenguaje capaz de generar progresivamente una mentalidad de acoso y que, en última instancia, puede dar lugar a la legitimación de actos violentos. Sobre la base del estudio de atrocidades generalizadas, la idea del "discurso del miedo" ofrece una vía para comprender si las condiciones previas para la violencia pueden surgir gradualmente, y para identificar, posiblemente, los momentos críticos en los que las contramedidas puedan resultar más efectivas. Por último, se ha procurado cada vez con mayor ahínco trasladar el debate general sobre la "incitación al odio" más allá de la mera identificación, regulación y distinción de contramedidas, mediante la puesta en marcha de estudios sobre quiénes manifiestan el odio y por qué. Con tales estudios se pretende comprender las características y las causas singulares de un fenómeno en rápida evolución, como condición previa a la consecución de "soluciones". Por tanto, la incitación al odio, tanto en Internet, como fuera de línea, puede evaluarse actualmente con arreglo a estos matices en el desarrollo de respuestas adecuadas al problema concreto considerado.

La proliferación de la incitación al odio en la Red, observada por Rita Izsák, Relatora Especial de la CDHNU sobre cuestiones de las minorías, en su informe A/HRC/28/65, plantea nuevos retos. Aunque no se dispone de estadísticas que ofrezcan una visión global del fenómeno, tanto las plataformas de redes sociales, como las organizaciones creadas para combatir la incitación al odio han reconocido que los mensajes de odio difundidos en línea son cada vez más habituales, y que se presta una atención sin precedentes al desarrollo de respuestas adecuadas. De acuerdo con Hatebase, una aplicación de Internet que recaba casos de incitación al odio en línea en todo el mundo, en la mayoría de tales casos, los destinatarios de este tipo de mensajes lo son por motivos de etnia y nacionalidad, pero las situaciones de incitación al odio asociadas a la pertenencia a una religión o una clase social también han aumentado.

La incitación al odio en Internet da lugar a que ciertas medidas jurídicas elaboradas para otros medios de comunicación resulten ineficaces o inapropiadas, y requiere de planteamientos que permitan tener en cuenta la naturaleza específica de las interacciones que posibilitan las tecnologías de la información y la comunicación (TIC) digitales. Se corre el peligro de meter en el mismo saco una diatriba publicada en Twitter sin pensar en las posibles consecuencias, y una amenaza real que forme parte de una campaña sistemática de odio. Existe una diferencia entre una publicación en un hilo en un medio social que reciba una atención escasa o nula, y otra que devenga "viral". Además, hay que considerar las complejidades que pueden afrontar las administraciones públicas y

los tribunales, por ejemplo, al tratar de aplicar una ley contra una plataforma de redes sociales cuya sede principal se ubica en un país diferente. Por tanto, aunque el contenido del discurso del odio en Internet no difiere de manera intrínseca de expresiones similares que se encuentran fuera de línea, existen retos peculiares y exclusivos de esa forma de incitación.

Tales retos pueden identificarse en función de la permanencia digital, la itinerancia, el anonimato y el carácter interjurisdiccional:

- En primer lugar, el discurso del odio puede permanecer en Internet durante mucho tiempo en diversos formatos y en múltiples plataformas. André Oboler, Primer Ejecutivo del Online Hate Prevention Institute, señaló que: "cuanto más tiempo se encuentre disponible el contenido, más daño podrá infligir a las víctimas y más poder otorgará a sus autores". Las arquitecturas de las plataformas pueden permitir que los temas se mantengan abiertos durante períodos de menor o mayor duración. Las conversaciones en Twitter organizadas en torno a los "trending topics" o temas más comentados pueden facilitar la propagación amplia y rápida de mensajes de odio, pero también brindan la oportunidad para que determinados ponentes con influencia desacrediten tales mensajes y, posiblemente, pongan término a hilos populares. *Facebook*, por el contrario, puede permitir que varios hilos continúen en paralelo y pasen desapercibidos fuera de una comunidad limitada, generando espacios de mayor duración cuando se vilipendia a ciertos grupos.

- En segundo lugar, la incitación al odio en línea también puede ser itinerante. Cuando se elimina un determinado contenido, este puede encontrar una vía de expresión en otro ámbito, posiblemente en la misma plataforma bajo un nombre diferente o en un espacio en Internet distinto. Si se cierra un sitio web, este puede reabrirse utilizando un servicio de hospedaje con una normativa menos rigurosa, o puede reubicarse en un país con una legislación que imponga un umbral superior respecto a la incitación al odio. La naturaleza itinerante también significa que las ideas que no habrían encontrado una expresión pública generalizada en el pasado, ahora pueden exponerse a grandes audiencias a través de diversas plataformas.

- En tercer lugar, la resistencia de los materiales de incitación al odio en Internet es única, debido al escaso coste de conservación y al potencial para una recuperación inmediata, lo que garantiza su relevancia continuada en determinados ámbitos de opinión.

- En cuarto lugar, el anonimato puede plantear asimismo un reto al tratar con la incitación al odio en línea. Las profesoras de derecho Danielle Keats Citron y Helen Norton consideran que: "Internet facilita el discurso anónimo y pseudoanónimo, lo que, con la misma facilidad, puede tanto acelerar las conductas destructivas, como alimentar el discurso público". Algunos gobiernos y plataformas de medios sociales han procurado que se apliquen políticas de revelación del nombre real, pero tales medidas se han enfrentado a una firme oposición, ya que menoscaban tanto el derecho a la privacidad, como la relación de este con la libertad de expresión. Por otra

parte, la mayoría de los "troleos" y ataques de incitación al odio en Internet proceden de cuentas bajo seudónimo, que no son necesariamente anónimas para todos. Las comunicaciones en línea auténticamente anónimas son muy poco habituales, ya que exigen que el usuario aplique medidas técnicas complejas para garantizar que no pueda ser identificado con facilidad. En cualquier caso, el anonimato percibido puede animar a algunas personas a considerar que sus opiniones en línea no se les pueden atribuir.

- En quinto lugar, dado que Internet no está regida por una única entidad, puede que las personas físicas, las administraciones públicas y las organizaciones no gubernamentales a los que atañen estas cuestiones tengan que tratar con los intermediarios de la Red en función de cada caso, dejando que los propietarios de cada espacio en línea específico decidan cómo abordar las acciones de los usuarios. Tales intermediarios corren el riesgo de convertirse en tribunales privados encargados de decidir el modo en que han de regularse los contenidos, una cuestión que se analiza con mayor detenimiento más adelante en el presente informe. Otra complicación tiene que ver con la escala transnacional de Internet, lo que plantea cuestiones de cooperación interjurisdiccional respecto a los mecanismos jurídicos de lucha contra la incitación al odio. Aunque existen tratados de asistencia jurídica mutua vigentes entre numerosos países, se trata de mecanismos caracterizados por su lentitud. La escala transnacional de muchos intermediarios de Internet del sector privado puede proporcionar una vía más efectiva para resolver los problemas en algunos casos, aunque estas entidades también se ven afectadas a menudo por solicitudes de datos interjurisdiccionales. A diferencia de la propagación del discurso del odio a través de canales convencionales, la incitación al odio en Internet conlleva con frecuencia la participación de múltiples escalas de agentes, ya sea con conocimiento de estos o no. Cuando los autores se sirven de una plataforma social en línea para difundir su mensaje de odio, no solo perjudican a sus víctimas, sino que también violan las condiciones de servicio de la plataforma y, en ocasiones, incluso la legislación estatal, dependiendo de su ubicación. Las víctimas, por su parte, se sienten indefensas frente al acoso en Internet, sin saber a quién deben recurrir para obtener ayuda.

Sobre la base del análisis esbozado anteriormente, en el presente capítulo se abordan las tendencias emergentes en el terreno de la incitación al odio en la Red. Se hace hincapié en los países en desarrollo y desarrollados, pero también se reconoce que los mayores problemas en este campo se dan actualmente en países donde existe una elevada conectividad a Internet. En cualquier caso, esta situación puede augurar el desarrollo de una evolución similar en otros lugares, a medida que aumenta el número de personas conectadas a la Red en todo el mundo. Por tanto, algunas de las respuestas evaluadas aquí podrían ser consideradas para su adaptación proactiva y temprana, y no únicamente tras el planteamiento del problema.

1.2 RESPUESTAS JURÍDICAS Y SOCIALES

Las respuestas más debatidas a la incitación al odio en Internet se han centrado fundamentalmente en las definiciones y los medios jurídicos, si bien este enfoque conlleva riesgos y limitaciones.

En primer lugar, la ley se mezcla con el poder y, en ocasiones, puede ser objeto de abusos para limitar el discurso legítimo con la supuesta justificación de sancionar la incitación al odio. Pueden producirse daños colaterales al discurso que, aún cuando resulte altamente objetable para algunos, no transgreda los estándares internacionales en materia de libertad de expresión. La cuestión clave en este caso es determinar cuándo la "incitación al odio" y su regulación pertenece a las tres categorías de expresión identificadas en 2012 por Frank La Rue, entonces Relator Especial de la ONU para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión. En su informe A/66/290 distingue entre:

- la expresión que constituye un delito según el derecho internacional y puede dar lugar a enjuiciamiento penal;
- la expresión que no es punible como delito, pero puede justificar una restricción y una demanda civil; y
- la expresión que no da lugar a sanciones penales o civiles, pero aún así plantea problemas en términos de tolerancia, urbanidad y respeto por los demás.

Es evidente que no todas las categorías anteriores exigen respuestas jurídicas, y además que, las que sí las exigen, pueden conllevar diferencias entre las respuestas del derecho penal y civil. Resulta igualmente evidente que las respuestas sociales pueden desempeñar papeles preventivos o de otra índole en todos los casos. Estas cuestiones influyen en el modo en que se entienden y abordan los diferentes casos de incitación al odio.

En segundo lugar, la Relatora Especial de la ONU sobre cuestiones relativas a las minorías observa que los delitos motivados por el odio rara vez se cometen sin que previamente se dé la estigmatización y deshumanización de los grupos de víctimas y diversos incidentes de incitación al odio. En segundo lugar, señala que: "solo las formas más graves de incitación al odio, a saber, las que constituyen una incitación a la discriminación, la hostilidad y la violencia, se consideran en general ilícitas". Este hecho pone de relieve que, aunque la legislación tiene reservado el desempeño de un papel en esta cuestión, las medidas jurídicas no pueden percibirse como una respuesta apropiada a toda la gama de manifestaciones que pueden contribuir (aunque no necesariamente) a un clima propicio para las acciones motivadas por el odio.

En tercer lugar, en lo que atañe a la incitación al odio, un planteamiento puramente jurídico puede pasar por alto el modo en que las sociedades evolucionan a través de la contestación y el desacuerdo. Aunque la incitación al odio es ofensiva, puede concebirse igualmente como una ventana para apreciar tensiones y desigualdades profundamente

arraigadas, que han de abordarse más allá de las cuestiones de la mera opinión, de la dimensión en línea.

Este análisis pone de relieve por qué es importante efectuar un seguimiento de las tendencias en las dimensiones jurídica y social que rodean a la incitación al odio. Así, en este capítulo se procede a continuación a ofrecer una amplia visión de conjunto de la evolución de los instrumentos jurídicos más relevantes que regulan la incitación al odio y, posteriormente, se hace especial hincapié en las respuestas sociales.

2. METODOLOGÍA

La estrategia de investigación para el presente capítulo se basa en gran medida en un estudio más detallado de la UNESCO titulado *Countering Online Hate Speech* (Contrarrestar la incitación al odio en Internet), en el que, a su vez, se combinan múltiples técnicas de recogida de datos y análisis, comenzando por una extensa revisión bibliográfica en la que se incluye la bibliografía jurídica en la que se examina cómo se aborda la incitación al odio en distintos países y continentes, y varios estudios etnográficos en los que se analiza la conducta de los usuarios en espacios en Internet motivados por el odio. Dada la novedad del fenómeno investigado y su rápida evolución, en dicha revisión también se incluyeron artículos no académicos presentados por diversos expertos en sus blogs y en publicaciones especializadas, así como en importantes periódicos y revistas en línea.

En el capítulo también se utilizan entrevistas semiestructuradas que se llevaron a cabo con interlocutores pertinentes, desde representantes de las plataformas de los medios sociales, incluidas Facebook y Google, a miembros de organizaciones de la sociedad civil, políticos y expertos técnicos Se analizaron asimismo contenidos producidos por organizaciones no gubernamentales que han puesto en marcha diversas iniciativas de alfabetización mediática e informacional (MIL por sus siglas en inglés) para contrarrestar la incitación al odio en línea, además de las condiciones de los acuerdos de servicio de las plataformas de medios en línea, incluidas Facebook, Twitter y YouTube. El objetivo consistía en comprender las tareas de vigilancia y gestión en la práctica de los contenidos en línea. Por otra parte, en la investigación se analizó el modo en que las campañas de MIL se dirigen a distintos destinatarios, y con qué resultados, así como las estrategias adoptadas por los grupos y coaliciones de lucha contra la discriminación para ejercer presión en las organizaciones de los medios sociales. Aunque la gama de puntos de vista y respuestas respecto a la incitación al odio en línea es amplia, se formularon preguntas comunes en cada caso.

3. MARCOS

3.1 MARCOS DE DERECHO INTERNACIONAL

La incitación al odio atañe a cuestiones controvertidas relacionadas con la dignidad, la igualdad, la seguridad de las personas y la libertad de expresión. No se menciona explícitamente en numerosos documentos y tratados internacionales de derechos humanos, pero sí se reclama de manera indirecta en virtud de principios vinculados a la dignidad humana, la igualdad y la libertad de expresión. Es posible que se determine que ciertas expresiones ponen en cuestión la dignidad, también a escala colectiva. En algunos casos, también puede establecerse que una expresión promueve la incitación a la discriminación, lo que conculcaría el derecho a la igualdad (aunque el vínculo entre la expresión y la práctica es otra cuestión diferente). Otro asunto relevante es el derecho a la vida, la libertad y la seguridad de la persona, y si una expresión determinada constituye un menoscabo directo en este sentido, como en los casos de los llamamientos al ataque a personas encuadradas como miembros de un grupo concreto.

Todos estos derechos se recogen en la Declaración Universal de Derechos Humanos de 1948. Teniendo en cuenta todos ellos de manera conjunta, a toda persona le asisten los derechos a la libertad de expresión, a ser protegido frente a las violaciones de la dignidad y la igualdad, y a la vida y la seguridad. En otras palabras, todos tenemos derecho a que se nos proteja frente a la incitación al odio en la medida en que la expresión de este equivalga a la conculcación de esos otros derechos. A tal efecto, se requiere un complejo equilibrio de derechos con el que se mantenga, en la medida de lo posible, la esencia de cada uno de ellos y, por tanto, los procesos y criterios para la consecución de tal equilibrio resultan esenciales. En cualquier caso, lo que es importante tener en cuenta es que la proporcionalidad, la necesidad y la legitimidad, en equilibrio bajo el argumento de contrarrestar la incitación al odio, no den lugar a una extralimitación en el terreno de la libertad de expresión.

La DUDH desempeñó un papel decisivo en el establecimiento de un marco y una agenda para la protección de los derechos humanos, pero no es vinculante. Posteriormente se elaboró una serie de documentos vinculantes para ofrecer una protección más sólida a los distintos derechos. De tales documentos, el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) es el más importante y exhaustivo a la hora de abordar la incitación al odio, aunque no utiliza de manera explícita dicho término. Otros instrumentos jurídicos internacionales más “a la medida” contienen igualmente disposiciones con repercusión en la definición de la incitación al odio y la identificación de las respuestas a este fenómeno, como la Convención para la Prevención y la Sanción del Delito de Genocidio (1951), la Convención Internacional sobre la Eliminación de todas las formas de Discriminación Racial (1969), y la Convención sobre la eliminación de todas las formas de discriminación contra la mujer (1981).

El PIDCP es el instrumento jurídico al que se alude más habitualmente en los debates sobre la incitación al odio y su regulación. En el artículo 19 se dispone el derecho a la libertad de expresión, se establece el derecho en sí y se incluyen las restricciones generales correspondientes a las limitaciones legítimas. No obstante, en el artículo 20 se limita explícitamente la libertad de expresión en casos de "apología del odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia". Consciente de las tensiones respecto al artículo 20, el Comité de Derechos Humanos ha subrayado que este es plenamente compatible con lo dispuesto en el artículo 19.

Para aportar mayor claridad a este respecto cabe señalar que, en el PIDCP, el derecho a la libertad de expresión no es absoluto. Los Estados pueden limitarlo legítimamente en ciertas circunstancias restringidas que deberán estar "expresamente fijadas por la ley y ser necesarias para asegurar el respeto a los derechos o a la reputación de los demás", o "la protección de la seguridad nacional, el orden público o la salud o la moral públicas". En la Observación General 34, el Comité de Derechos Humanos explica que las limitaciones impuestas por los Estados pueden comprender el discurso en línea con arreglo al artículo 19, apartado 3 del PIDCP, y señala que tales restricciones "se deben referir en general a un contenido concreto; las prohibiciones genéricas del funcionamiento de ciertos sitios y sistemas no son compatibles con el párrafo 3".

Entre el artículo 19, apartado 3, y el artículo 20, existe una distinción entre las limitaciones opcionales y obligatorias a la libertad de expresión. En el artículo 19, apartado 3 se establece que las limitaciones a la libertad de expresión "**pueden** estar sujetas a ciertas restricciones", siempre que estas se dispongan en la ley y sean necesarias para atender ciertos fines legítimos. En el artículo 20 se establece que toda apología del odio que constituya una incitación a la discriminación, la hostilidad o la violencia "**estará** prohibida por la ley". A pesar de las indicaciones sobre la gravedad de las ofensas en la expresión que deben quedar prohibidas por la ley con arreglo al artículo 20, sigue existiendo complejidad. En concreto, existe ambigüedad en la conceptualización de una distinción inequívoca entre i) las expresiones de odio, ii) la expresión que equivale a una apología del odio, y iii) la expresión de odio que constituye de manera específica una incitación al daño en la práctica que se deriva de la discriminación, la hostilidad o la violencia. En este sentido, aunque los Estados tienen la obligación de prohibir la expresión concebida como una "apología del odio que constituya una incitación a la discriminación, la hostilidad o la violencia", de conformidad con el artículo 20, apartado 2, el modo de interpretar esta disposición no se ha definido claramente. En consecuencia, las limitaciones de la libertad de expresión, basadas en lo dispuesto en el PIDCP, pueden ser objeto de abuso. En los principios de Camden, un conjunto de normas formuladas por la ONG ARTICLE 19 en consulta con diversos expertos en derechos humanos, se definen criterios específicos para evitar la aplicación errónea del artículo 20, apartado 2. El artículo 20 debe interpretarse de una manera restringida para evitar su abuso.

La Convención Internacional sobre la Eliminación de todas las formas de Discriminación Racial (ICERD por sus siglas en inglés) de 1965 también tiene consecuencias para la conceptualización de las distintas formas de incitación al odio, aunque tampoco utiliza explícitamente este término. La ICERD difiere del PIDCP en tres aspectos. En primer lugar,

su conceptualización de la incitación al odio se limita específicamente a las expresiones que aluden a la raza y la etnia. En segundo lugar, la ICERD impone una obligación a los Estados parte que es más rigurosa que el artículo 20 del PIDCP, y cubre la penalización de las ideas racistas que no incitan necesariamente a la discriminación, la hostilidad o la violencia. En tercer lugar, el concepto de "apología del odio" introducido en el PIDCP es más específico que el de manifestación discriminatoria descrito en la ICERD, ya que en el primero se exige la consideración de la intención del autor, y no de la expresión aislada. La mera difusión de mensajes de superioridad u odio racial, o incluso la incitación a la discriminación o la violencia racial, serán sancionables de conformidad con la ICERD. En el PIDCP, la intención de incitar al odio ha de demostrarse para que se prohíba la expresión de que se trate, con arreglo al artículo 20, apartado 2.

En 2002, el Comité para la Eliminación de la Discriminación Racial abordó activamente la incitación al odio en su Recomendación General 29, A/57/18, en la que recomienda a los Estados parte que adopten medidas contra la divulgación de ideas "por conducto de los medios de información e Internet" de superioridad e inferioridad de castas o que intenten justificar actos de violencia, odio o discriminación contra las comunidades cuya condición se basa en consideraciones de ascendencia. Abogó asimismo por la adopción de medidas estrictas contra toda incitación a la discriminación o a la violencia contra las comunidades, "incluso por conducto de Internet"; y por crear conciencia entre los profesionales de los medios de información respecto de la índole y la incidencia de la discriminación basada en la ascendencia. Estas disposiciones, que reflejan la referencia en la ICERD a la divulgación de declaraciones, tienen especial relevancia para Internet, en cuanto que la expresión de ideas en ciertos contextos en línea puede dar lugar a su difusión inmediata. También atañen a los espacios previamente privados que han comenzado a desempeñar una función pública, como ocurre en el caso de numerosas plataformas de redes sociales.

De modo similar a la ICERD, la Convención sobre el Genocidio se propone proteger a los grupos definidos por la raza, la nacionalidad o la etnia, aunque extiende asimismo sus disposiciones a los grupos religiosos. No obstante, en lo que atañe a la incitación al odio, la Convención sobre el Genocidio se limita únicamente a los actos que incitan de manera pública al genocidio, reconocidos como "actos perpetrados con la intención de destruir, total o parcialmente, a un grupo nacional, étnico, racial, o religioso, como tal".

La incitación al odio basada específicamente en el género (diferenciada de las acciones discriminatorias) no se trata de manera exhaustiva en el derecho internacional. La Convención sobre la eliminación de todas las formas de discriminación contra la mujer (CEDAW), que entró en vigor en 1981, impone a los Estados la obligación de condenar la discriminación contra las mujeres y "prevenir, investigar, procesar y castigar" actos de violencia basada en el género. El Comité de Derechos Humanos ha manifestado asimismo su "profunda inquietud por los actos de violencia y discriminación perpetrados en todas las regiones del mundo contra personas por motivo de su orientación sexual y su identidad de género".

La medida en que la expresión se asocia a tales actuaciones en la práctica es objeto de debate. En cualquier caso, el Comité de Derechos Humanos de la ONU, en su Observación General 28, insta a los Estados a "proporcionar información acerca de las medidas legales que existan para restringir la publicación o difusión" de material pornográfico que presente a mujeres como objetos de un trato degradante.

En resumen, las normas del PIDCP contemplan posibles restricciones debidas al respeto por los derechos o la reputación de terceros, o a motivos de seguridad nacional u orden público, o a razones de salud pública o éticas, cuya disposición en ciertos contextos puede aplicarse a expresiones que podrían catalogarse de "incitación al odio". El PIDCP exige asimismo el establecimiento de restricciones respecto al "odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia". Resulta evidente que estas dos dimensiones constituyen normas para una base condicional, con el fin de limitar ciertas expresiones que podrían clasificarse en la categoría de la "incitación al odio", siempre que tales restricciones figuren en la legislación y sean necesarias. Con arreglo a la ICERD, existe una base normativa para restringir la difusión de ideas de superioridad racial (lo que equivaldría asimismo a la protección del respeto por el derecho humano a la igualdad).

En las últimas tendencias, y como respuesta a esta complejidad y a los riesgos de abuso de las normas internacionales de restricción de la expresión legítima, la ONU ha procurado la creación de espacios para promover una interpretación compartida de lo que constituye incitación al odio, y del modo en que debe tratarse, así como de la pertinencia de los derechos humanos en el ámbito de Internet. También recientemente, los órganos rectores de la Asamblea General de la ONU, la CDHNU y la UNESCO han reconocido de manera definitiva que todos los derechos humanos son aplicables, tanto en Internet, como fuera de línea. Todos estos acontecimientos, combinados, determinan el contexto de la consideración de la incitación al odio en la Red.

Un hito en este proceso ha sido la organización de una serie de reuniones consultivas por parte de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACDH). Tales encuentros dieron lugar en 2012 a la formulación del Plan de acción de Rabat sobre la prohibición del "odio nacional, racial o religioso que constituya incitación a la discriminación, la hostilidad o la violencia". En dicho Plan se reconoce que, a pesar de las obligaciones de los Estados signatarios del PIDCP, muchos marcos jurídicos no contemplan la prohibición legal de tal apología. Además, algunas leyes que sí comprenden la prohibición, utilizan terminología incoherente con la empleada en el artículo 20 del PIDCP. En el Plan se propone asimismo una prueba de umbral en seis partes para identificar mensajes de odio, en la que se considera el contexto, el autor, la intención, el contenido, el alcance de la declaración y la probabilidad de que esta pueda incitar al daño en la práctica. En este sentido, no se asume que todas las expresiones de odio den lugar a un perjuicio real o se traduzcan en un daño efectivo. Por el contrario, lo que se propone es un método para señalar aquellas expresiones que más requieren atención.

No obstante, en el caso de la incitación al odio en línea, el énfasis que se pone en el Plan de Rabat en los agentes de ámbito nacional y, en especial, en los Estados, puede restar importancia a las plataformas de redes sociales del sector privado que actúan a escala transnacional. Estos agentes pueden desempeñar un papel muy significativo en la interpretación de la incitación al odio y en la labor de permitir o restringir este tipo de expresiones. Por otra parte, en el Plan de Rabat no se presta gran atención a las cuestiones del odio por motivos como el género, la preferencia sexual o la lengua hablada.

Además de permitir a los Estados que adopten medidas para limitar la incitación al odio, el derecho internacional comprende ciertas disposiciones relativas a la formulación de reclamaciones al respecto: el Comité de Derechos Humanos recibe quejas individuales respecto al PIDCP, el Comité para la Eliminación de la Discriminación Racial recibe asimismo las reclamaciones derivadas de la ICERD, y de las quejas relacionadas con la CEDAW se encarga el Comité para la Eliminación de la Discriminación contra la Mujer. En cualquier caso, las personas físicas solo pueden formular una reclamación contra un Estado que haya permitido explícitamente tales mecanismos.

Diversas opiniones sobre el equilibrio entre la libertad de expresión y la limitación de la incitación al odio se recogen con profusión en instrumentos regionales de derechos humanos. Estos documentos complementan los tratados internacionales, al reflejar las particularidades regionales que no se especifican en los convenios de alcance universal. Los instrumentos regionales pueden resultar particularmente efectivos para velar por la protección de los derechos humanos, como en el caso del Tribunal Europeo de Derechos Humanos, que resuelve más asuntos relacionados con la incitación al odio que el Comité de Derechos Humanos de las Naciones Unidas. En cualquier caso, los instrumentos regionales de derechos humanos no deben contradecir las normas internacionales establecidas, ni imponer limitaciones más rigurosas sobre derechos fundamentales. La mayoría de los instrumentos regionales carecen de artículos específicos que prescriban la prohibición de la incitación al odio, si bien, en términos más generales, permiten que los Estados limiten la libertad de expresión, estableciendo disposiciones que pueden aplicarse a determinados casos. En los párrafos que siguen se examina cómo se definen el derecho a la libertad de expresión y sus limitaciones a escala regional, y el modo en que los documentos regionales complementan otros textos en los que se recoge una definición y la limitación de la incitación al odio.

En la **Convención Americana sobre Derechos Humanos** se describen ciertas limitaciones de la libertad de expresión de un modo similar al del artículo 19, apartado 3 del PIDCP. En la Convención se añade una cláusula de limitación específica que prohíbe la censura previa; no obstante, con el fin de ofrecer más protección a los menores, permite tal censura para la "protección moral de la infancia y la adolescencia". La Organización de Estados Americanos ha adoptado otra declaración sobre los principios de la libertad de expresión, en la que se incluye una cláusula específica en la que se señala que "condicionamientos previos, tales como veracidad, oportunidad o imparcialidad por parte de los Estados son incompatibles con el derecho a la libertad de expresión reconocido en los instrumentos internacionales". La Corte Interamericana ha advertido de que

las medidas preventivas son incompatibles con la libertad de expresión, y de que los Estados deben emplear en cambio "la imposición ulterior de sanciones para quien haya cometido los abusos". La Corte impone además una prueba para los Estados dispuestos a promulgar restricciones a la libertad de expresión, ya que estos han de satisfacer previamente unos motivos de responsabilidad establecidos, definidos en la legislación, procurados para alcanzar fines legítimos, y "necesarios para garantizar" que se cumplen tales fines. Por último, el Sistema Interamericano cuenta con un Relator Especial sobre la Libertad de Expresión en cuyo estudio exhaustivo sobre la incitación al odio se concluye que el Sistema Interamericano de Derechos Humanos difiere del enfoque europeo y de las Naciones Unidas en una cuestión esencial: el Sistema Interamericano solo se ocupa de la expresión de odio que da lugar en la práctica a la violencia, y únicamente tal expresión puede restringirse.

La **Carta Africana sobre los Derechos Humanos y de los Pueblos** adopta un planteamiento diferente en su artículo 9, apartado 2, al permitir las restricciones sobre los derechos siempre que las primeras "se ajusten a la ley". Este concepto ha dado lugar a ciertas dudas, y existe una amplia doctrina jurídica sobre las cláusulas denominadas de "*claw-back*" o exención y su interpretación. La cuestión apunta fundamentalmente al hecho de que los países pueden manipular su propia legislación y menoscabar la esencia del derecho a la libertad de expresión. No obstante, es importante añadir que en la Declaración de principios sobre la libertad de expresión en África se desarrolla con mayor detenimiento una norma más estricta respecto a las limitaciones de la libertad de expresión. Se declara que el derecho "no debe restringirse por motivos de orden público o seguridad nacional, salvo que exista un riesgo real de perjuicio de un interés legítimo y un vínculo causal estrecho entre el riesgo de perjuicio y la expresión de que se trate".

En 1990, la Organización de la Conferencia Islámica (actualmente, la Organización de Cooperación Islámica (OCI)) aprobó la **Declaración de El Cairo sobre los Derechos Humanos en el Islam**, en la que se establece que los derechos humanos deben ser "conformes con la Shari'ah islámica". Algunos consideran que esta cláusula repercute en el umbral de las limitaciones, y que es la razón por la que algunos Estados miembros de la OCI han realizado un llamamiento a favor de una penalización de la expresión que va más allá de los casos de violencia inminente, para englobar los "actos o declaraciones que denoten una intolerancia y un odio manifiestos".

La **Carta Árabe de Derechos Humanos**, adoptada por el Consejo de la Liga de los Estados Árabes en 2004, incluye en su artículo 32 disposiciones que atañen a la comunicación en línea, y garantizan el derecho a la "libertad de opinión y expresión, y el derecho a buscar, recibir e impartir información e ideas a través de cualquier medio, con independencia de los límites geográficos". En el apartado 2 se dispone que: "Tales derechos y libertades se ejercerán de conformidad con los valores fundamentales de la sociedad". Esta posición difiere de la de la Observación General nº 22 del Comité de Derechos Humanos, en la que se refiere que las "las limitaciones impuestas a la libertad de manifestar la religión o las creencias con el fin de proteger la moral deben basarse en principios que no se deriven exclusivamente de una sola tradición".

La **Declaración de Derechos Humanos de la ASEAN** incluye el derecho a la libertad de expresión en el artículo 23. En el artículo 7 de la Declaración se establecen limitaciones generales y se afirma que "la realización de los derechos humanos debe considerarse en el contexto regional y nacional, teniendo en cuenta los diversos antecedentes políticos, económicos, jurídicos, sociales, culturales, históricos y religiosos". En este sentido, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos ha llamado la atención respecto a la disposición de la Declaración de Viena en la que, a pesar de las diferencias, "es el deber del Estado (cualquiera fuese su sistema político, económico y cultural), promover y proteger todos los derechos humanos y todas las libertades fundamentales".

Algunos textos regionales resultan potencialmente más restrictivos de la libertad de expresión que las normas internacionales. Sin embargo, otros textos de ámbito regional contienen pruebas más rigurosas para evaluar la legitimidad de las limitaciones de la libertad de expresión. La Carta de los Derechos Fundamentales de la Unión Europea, que declara el derecho a la libertad de expresión en su artículo 11, afirma en su artículo 54 que la Carta no debe interpretarse en el sentido de que implique "limitaciones más amplias [...] que las previstas en la presente Carta". El Convenio Europeo de Derechos Humanos conlleva una prueba rigurosa de necesidad y proporcionalidad para las limitaciones a la libertad de expresión. El Tribunal Europeo de Derechos Humanos distingue entre la incitación al odio y el derecho de las personas a expresar sus puntos de vista libremente, aún cuando otros se sientan ofendidos.

En 2000, el Consejo de Europa (CdE) emitió una Recomendación de política general sobre la lucha contra la difusión de materiales racistas, xenófobos y antisemitas a través de Internet. El Convenio sobre la Ciberdelincuencia del CdE de 2001 regula la asistencia mutua respecto a las facultades de investigación, proporcionando a los países suscriptores un mecanismo para tratar los datos informáticos, incluida la incitación al odio en línea a escala transnacional. En 2003, el CdE publicó un protocolo adicional al convenio en el que se abordan las expresiones de racismo y xenofobia en línea, y en el que se impone a los países miembros la obligación de penalizar los insultos racistas y xenófobos en Internet basados en la "raza, color, ascendencia, u origen nacional o étnico, o la religión". Nueve países no europeos han suscrito o ratificado ya el convenio.

Como nota importante relativa a lo anteriormente referido, cabe señalar que en ciertos documentos internacionales recientes, como la mencionada Observación General 34 del Comité de Derechos Humanos (2011), y el Plan de Acción de Rabat (2011), se ha hecho hincapié en la reciprocidad entre la libertad de expresión y la protección contra la incitación al odio. La complejidad en el equilibrio entre la libertad de expresión y las limitaciones en lo que atañe al odio explica la diversidad de concepciones jurídicas de la incitación al odio en todo el mundo, y complica la interpretación de la ley en cualquier caso planteado. No obstante, toda limitación jurídica ha de considerarse siempre teniendo en cuenta el derecho más amplio a la libertad de expresión. Con arreglo a la Observación General 34, "la relación entre el derecho y la restricción, o entre la norma y la excepción, no debe invertirse".

3.2 MARCO PARA AGENTES PRIVADOS

Los instrumentos jurídicos internacionales y regionales examinados anteriormente evolucionan y dan lugar a un marco para que los *Estados* aborden la incitación al odio en el contexto de su obligación de promover y proteger los derechos, que comprende la tarea de equilibrar el derecho a la libertad de expresión con los derechos a la dignidad, la igualdad y la seguridad de la persona. No obstante, al abordar la incitación al odio *en línea*, los distintos Estados no son siempre los agentes que ejercen un mayor impacto. Intermediarios de Internet como las plataformas de redes sociales, los proveedores de servicios de Internet y los motores de búsqueda estipulan en sus condiciones de servicio el modo en que pueden intervenir en la autorización, restricción y canalización de la creación de determinados contenidos y del acceso a los mismos. Un gran número de interacciones en línea ocurren en plataformas de redes sociales que trascienden a las jurisdicciones nacionales y han desarrollado sus propias definiciones de incitación al odio, además de las medidas para responder a estas actuaciones. En el caso de un usuario que infringe las condiciones de servicio, el contenido que haya publicado puede suprimirse de la plataforma, o el acceso al mismo puede restringirse para que no pueda verse en un determinado país.

Los principios que fundamentan los acuerdos sobre condiciones de servicio, y los mecanismos que desarrolla cada empresa para garantizar su ejecución, repercuten de manera significativa en la capacidad de las personas para expresarse en Internet, así como para que se les proteja de la incitación al odio. La mayoría de los intermediarios entablan negociaciones con los gobiernos nacionales en una medida que varía con arreglo al tipo de intermediario, las áreas en las que la empresa se encuentra registrada, y el régimen jurídico aplicable. Los proveedores de servicios de Internet son los agentes que se ven más directamente afectados por la legislación nacional, ya que han de ubicarse en un país concreto para llevar a cabo su actividad. Los motores de búsqueda han tendido cada vez más a adaptarse al régimen de responsabilidades de los intermediarios, tanto de sus jurisdicciones de procedencia y registro, como en otras jurisdicciones en las que prestan sus servicios, ya sea suprimiendo los vínculos a determinados contenidos por iniciativa propia, o a requerimiento de las autoridades. Las empresas de las redes sociales en línea muestran una notable variación en cuanto a sus planteamientos.

Con independencia de la diversidad en el sector, se ha aclarado recientemente que de todos los intermediarios de Internet gestionados por empresas del sector privado también se espera que respeten los derechos humanos. Así se expone en los Principios Rectores sobre las empresas y los derechos humanos de 2011 elaborados por la OACDH. En el documento se hace hincapié en la responsabilidad de las empresas en la defensa de los derechos humanos. En este sentido, los intermediarios de Internet, con arreglo a la actividad en este terreno de otras empresas, deben evaluar “los efectos potenciales y reales sobre los derechos humanos, incorporando los resultados obtenidos y actuando respecto a estos, ocupándose del seguimiento de las respuestas, y comunicando el modo en que se abordan tales efectos”. En los Principios Rectores de la ONU se indica además que, en los casos en que se violan los derechos humanos, las empresas deben

"repararlas o contribuir a su reparación [de las consecuencias negativas] por medios legítimos". En el caso de los intermediarios de Internet y los conceptos de incitación al odio, esto significa que deben asegurarse de que se adopten medidas para identificar los casos de incitación y ofrecer una respuesta proporcional.

En cualquier caso, estos principios luchan aún por ser objeto de una referencia concreta en numerosas posiciones en materia de políticas de los intermediarios, así como por su ejecución concreta en la práctica empresarial ordinaria. Una cuestión a este respecto es la medida en la que una entidad del sector privado tiene derecho a establecer condiciones de servicio que puedan resultar más restrictivas de la expresión que lo que un Estado está obligado a permitir con arreglo a normas internacionales como el PIDCP. Se trata de una cuestión análoga en ciertos aspectos a la libertad de prensa, en lo que se refiere al derecho de una entidad de los medios de comunicación a establecer una política editorial propia respecto a la información que publica. Esto es así a pesar de que, mientras que las redes sociales se basan de manera inequívoca en las manifestaciones de los usuarios, en los medios informativos las expresiones emanan de los empleados por la propia plataforma. Otra cuestión atañe al modo en que las empresas, en la medida en que cumplan las normas internacionales sobre derechos humanos, deciden respecto al equilibrio de derechos, como el de la libertad de expresión en relación con la protección de la privacidad, la igualdad o la dignidad, y qué medidas de compensación existen. Por último, hay cuestiones relacionadas con el modo en que las empresas adoptan decisiones cuando la legislación nacional no se atiene a las normas internacionales sobre derechos humanos, como en lo que se refiere a los límites legítimos a la libertad de expresión. La situación es dinámica y sigue evolucionando.

Al mismo tiempo, se observa una tendencia creciente a que los intermediarios de Internet desarrollen definiciones dispares de la incitación al odio y distintas directrices para regularla. Algunas empresas no emplean el término incitación al odio, pero manejan una lista descriptiva de términos relacionados con este fenómeno. En las condiciones de servicio de Yahoo! se prohíbe la publicación de "contenido que sea ilegal, peligroso, amenazante, abusivo, hostigador, tortuoso, difamatorio, vulgar, obsceno, calumnioso, invasivo de la privacidad de terceros, odioso, discriminatorio, o cuestionable desde el punto de vista racial, ético o de otro modo." De manera similar, Twitter no prohíbe explícitamente la incitación al odio, pero advierte a sus usuarios de que "en estos Servicios puede aparecer Contenido ofensivo, dañino, inexacto o de algún modo inapropiado, o en algunos casos, entradas mal identificadas o engañosas". No asume responsabilidad alguna respecto al contenido. Tales condiciones de servicio se complementan mediante las "Reglas de Twitter", un conjunto de condiciones para los usuarios, y la empresa ha respondido a las peticiones de eliminación de contenido relacionado con la incitación al odio formuladas por las administraciones públicas y la sociedad civil.

Otras compañías se refieren de manera explícita a la incitación al odio. En las condiciones de servicio de YouTube, por ejemplo, se procura el equilibrio de la libertad de expresión y la limitación a ciertas formas de contenido. Aunque se señala que "somos partidarios de la libertad de expresión", YouTube declara que "no permitimos los discursos de incitación al odio: los discursos que atacan o degradan a un grupo por motivos de origen racial

o étnico, religión, discapacidad, sexo, edad, condición de ex combatiente de guerra, identidad u orientación sexual". Así, esta definición es más amplia que la llamada del PIDCP a la limitación únicamente de los discursos que constituyan una apología intencionada del odio que incite a la discriminación, la hostilidad o la violencia. Es un ejemplo de cómo las empresas pueden actuar de manera más restrictiva que el derecho internacional, e incluso que algunas legislaciones regionales o nacionales en materia de incitación al odio.

Las condiciones de Facebook prohíben el contenido nocivo, amenazador o que puede incitar al odio o a la violencia. En sus normas comunitarias, Facebook refiere más ampliamente a este respecto que "elimina el lenguaje que incita al odio, es decir, todo contenido que ataca directamente a personas en función de los siguientes aspectos: raza, etnia, nacionalidad, religión, orientación sexual, sexo, género o identidad sexual, discapacidades o enfermedades graves". Microsoft cuenta con unas normas específicas respecto a la incitación al odio para varias de sus aplicaciones. Su política respecto a los teléfonos móviles prohíbe las aplicaciones que incluyan "tener contenido que podría ser ofensivo, abogue a favor de la discriminación, el odio o la violencia basándose en consideraciones de raza, etnia, origen nacional, idioma, sexo, edad, discapacidad, religión, orientación sexual, estado de veterano o pertenencia a cualquier otro grupo social". La empresa cuenta además con normas relativas a los juegos en línea, que prohíben toda comunicación indicativa de "incitación al odio, asuntos religiosos controvertidos y eventos delicados, actuales o históricos". Es un ejemplo más del modo en que las empresas pueden actuar de manera más restrictiva que el derecho regional internacional en materia de incitación al odio: "los asuntos religiosos controvertidos y los eventos delicados, actuales o históricos" no se prohíben necesariamente en el derecho internacional, ni se consideran automáticamente discriminatorios. En cualquier caso, y con el fin de promover lo que percibe como una comunidad en línea más segura, Microsoft ha optado por imponer una normativa restrictiva de la expresión en ciertos productos que forman parte de su oferta. Por otro lado, en algunas jurisdicciones, estas condiciones de servicio pueden resultar más liberales que los límites jurídicos locales.

Habitualmente, solo una pequeña minoría de usuarios leen las condiciones de servicio, y existen diversos niveles de "calidad" entre los distintos tipos de acuerdo. Un análisis de las tendencias pone de relieve que no se trata solo de cómo definen la incitación al odio los intermediarios de Internet, sino también del modo en que aplican sus definiciones. Cabe considerar aquí la responsabilidad de tales intermediarios. Muchos de ellos argumentan que no generan ni controlan el contenido en línea y que, por tanto, deberían asumir únicamente una responsabilidad limitada. Con arreglo a tal argumento se les eximiría de un examen o moderación previos de los contenidos, y se les exigiría responsabilidad únicamente tras la publicación en los casos en los que se llame su atención respecto al contenido que infrinja la legislación y/o sus condiciones de servicio. Existen diferentes regímenes jurídicos en materia de responsabilidad en todo el mundo, con efectos diversos, aunque, en última instancia, es probable que se aplique una única norma jurisdiccional que pueda hacer efectiva la intervención de la empresa de que se trate encaminada a limitar un determinado caso de expresión en línea, aunque deban

considerarse complejidades respecto al lugar de registro de la entidad, la ubicación de los datos y los destinos a los que pueden servirse tales datos.

En la noción de responsabilidad limitada se distingue entre los intermediarios de Internet y las empresas de medios de comunicación. En todo caso, existen debates sobre la medida en que los medios de comunicación han de asumir una responsabilidad limitada respecto a los comentarios generados por los usuarios en sus sitios *web*. Sus prácticas y condiciones de servicio para la moderación de contenidos, así como sus sistemas de autorregulación, como los comités de deontología periodística, pueden revestir importancia en cualquier caso para los intermediarios de Internet. Para los proveedores de servicios de Internet, la responsabilidad en una jurisdicción determinada constituye una cuestión relativamente sencilla. De manera similar a lo que sucede con otros intermediarios de Internet, pueden definir sus propios parámetros al ofrecer un servicio, pero, dado que están obligados a someterse al principio de territorialidad, tienden a actuar con arreglo a la legislación del país en el que ofrecen sus servicios. Esta circunstancia les hace responder con mayor flexibilidad que otros intermediarios a las peticiones externas de supresión de contenidos.

El asunto se complica en el caso de las plataformas de redes sociales con un ámbito de actuación internacional. Dado el enorme volumen de datos que manejan, dichas plataformas confían fundamentalmente en las notificaciones de los usuarios que denuncian los contenidos que consideran inapropiados, ofensivos o peligrosos. A continuación, las plataformas deciden, principalmente con arreglo a sus condiciones de servicio, si los contenidos en cuestión deben retirarse o no, o si han de emprenderse otras acciones para restringir el acceso a los mismos o la capacidad de sus autores para seguir utilizando los servicios de la plataforma. En ausencia de una autoridad jurisdiccional nacional múltiple con competencias sobre la empresa, y dada la limitada capacidad y alcance de las distintas jurisdicciones individuales, salvo de aquella en la que se encuentra domiciliada la actividad de la entidad, muchos intermediarios actúan conforme a sus propias condiciones de servicio globales de índole general.

Aparte de las antiguas directrices filtradas por empleados de las empresas a las que las plataformas de redes sociales subcontratan algunos aspectos de la regulación de contenidos, poco se sabe acerca del modo en que las condiciones de servicio se traducen en la práctica en cuanto a lo que se debe mantener, y lo que se debe filtrar o suprimir. Algunos han sugerido que Facebook ha venido desarrollando un conjunto de normas objetivas para actuar respecto a las expresiones a las que considere capaces probablemente de provocar violencia. Sin embargo, los directivos de Facebook han indicado que la empresa trata de evitar un enfoque excesivamente formal y prefiere considerar el contexto en cada caso en la medida de lo posible.

Es tendencia el que, últimamente, algunas empresas presten una mayor atención a las reclamaciones de los usuarios. En 2012, Facebook introdujo la posibilidad de que los usuarios marcaran el contenido que consideren inapropiado para llevar a cabo un seguimiento de sus denuncias hasta la resolución del caso. Ofrece asimismo herramientas para “socializar” las denuncias, que permiten a los usuarios notificar privadamente

la cuestión al autor de un determinado contenido antes de solicitar formalmente su supresión a Facebook. Estas nuevas oportunidades constituyen complementos interesantes a otras medidas de respuesta a los casos de incitación al odio percibidos, aún cuando escasean los datos que acrediten su efectividad a lo largo del tiempo, o si a los usuarios les satisfacen o no las opciones que se les ofrecen. Al mismo tiempo, se debate con profusión que agentes mercantiles actúen como tribunales al decidir qué discursos resultan admisibles, a pesar de que se trata de entidades privadas y de sus características en línea. Esta cuestión se examina con mayor detenimiento más adelante en el presente informe.

En resumen, en el análisis anterior se ha considerado el panorama de las normas y leyes internacionales y regionales, así como las tendencias emergentes en las empresas intermediarias de Internet transnacionales que se han constituido en los principales sitios y agentes en lo que atañe a la incitación al odio en línea y a su regulación. Las diferentes definiciones de la incitación al odio resultan evidentes en una compleja amalgama de políticas internacionales, que aplican de manera distinta los agentes de las administraciones públicas y las empresas. Aunque todos los agentes deberían procurar someterse a las normas contenidas en los tratados universales, la realidad práctica la complica la autonomía relativa de los intermediarios de Internet y el papel fundamental que desempeñan en las comunicaciones en línea. Al mismo tiempo, las respuestas reguladoras basadas en la actuación del Estado pueden resultar lentas de desarrollar, complejas de ejecutar, y vulnerables a la injerencia política. En este contexto, han surgido respuestas sociales a los casos percibidos de incitación al odio en línea.

4. ANÁLISIS DE LAS RESPUESTAS SOCIALES

El análisis persigue en este caso ofrecer una visión matizada de cómo se manifiestan las preocupaciones por la incitación al odio y la violencia en diversas respuestas sociales. En los apartados que siguen se abordan las cuestiones del seguimiento, la movilización, el ejercicio de presiones entre los intermediarios, la capacitación de los usuarios a través de las iniciativas de alfabetización mediática e informacional, y la moderación de los contenidos de los medios de comunicación.

4.1 SEGUIMIENTO Y ANÁLISIS DE LA INCITACIÓN AL ODIO

El clima de incitación al odio probablemente devenga en el más propicio para generar violencia en situaciones en las que están en juego importantes intereses políticos, como en unas elecciones. En el presente apartado se analizan cuestiones de ámbito general derivadas de las respuestas prácticas desarrolladas para abordar las posibilidades de incitación al odio en línea que surgen en tales situaciones. Una respuesta que proporciona un contexto para observaciones de mayor amplitud es la del proyecto de investigación UMATI, que comenzó en septiembre de 2012, previamente a las elecciones de marzo de 2013 en Kenya. En este proyecto se llevó a cabo un seguimiento de la expresión en línea, con el fin de estimar tanto la existencia, como la virulencia de los casos de incitación al odio. Las experiencias proporcionaron a las partes interesadas la oportunidad de analizar los asuntos y los destinatarios de la incitación al odio, y de reflexionar colectivamente sobre el potencial de determinados actos de expresión para dar lugar o no a situaciones de violencia.

En 2007, Kenya celebró las elecciones más controvertidas y violentas desde su regreso al multipartidismo en 1991, con el resultado de 1.000 personas fallecidas y 600.000 desplazados. Fue la primera elección en la que las nuevas TIC se convirtieron en un elemento integrante de la cita electoral. Las redes sociales, los mensajes de correo electrónico y los mensajes de texto SMS se utilizaron en una medida sin precedentes para convocar a partidarios y difundir información, pero también para propagar rumores, y determinados grupos políticos y étnicos sugirieron cómo sus oponentes planeaban acciones para atacar, expulsar y asesinar a personas y comunidades. Se falsificaron y difundieron documentos en línea para arrojar dudas sobre los candidatos presidenciales. A raíz de la violencia generada, Kenya estableció la Comisión Nacional de Cohesión e Integración, que colaboró con los medios y los agentes de la autoridad para atenuar las tensiones étnicas.

En este contexto, un grupo de investigadores y emprendedores se reunieron con anterioridad a las elecciones de 2013 en el país y pusieron en marcha UMATI (que

significa “multitud” en kiswahili), un proyecto encaminado al seguimiento de los casos de incitación al odio en línea. El objetivo general de UMATI era detectar señales de tensiones crecientes entre los ciudadanos Kenyanos, con el fin de ofrecer una visión de las diversas fases de los comicios, y hacer sonar la alarma antes del estallido de violencia. Las elecciones tuvieron lugar en marzo de 2013, y el proyecto duró nueve meses, de septiembre de 2012, a mayo de 2013. Se ocupó del seguimiento de blogs, foros, periódicos en línea y el contenido de Facebook y Twitter generado por kenyanos en inglés, así como en las principales lenguas habladas en Kenya. Adoptando la definición de “discurso peligroso” elaborada por Benesch como un subconjunto de la incitación al odio con el potencial más elevado para catalizar actos de violencia, el equipo de UMATI definió varios criterios prácticos para distinguir entre los diferentes actos de expresión y ponderar su capacidad de dar lugar a situaciones de violencia. Los encargados de la labor de seguimiento evaluaron las cuestiones con arreglo a la influencia ejercida por el autor en la comunidad en línea, el contenido de la declaración, y el contexto social e histórico del discurso. Como resultado, los actos de expresión pudieron clasificarse en tres categorías: discurso ofensivo, discurso moderadamente peligros, y discurso peligroso. El seguimiento diario, el posicionamiento de los actos de expresión a lo largo de una escala, y la ordenación de otras variables (incluidos los objetivos de la incitación al odio y si los actos de expresión aluden a determinados acontecimientos), permitieron a los investigadores determinar la evolución de la incitación al odio en el tiempo, y ofrecer una interpretación más matizada de los riesgos efectivos y percibidos.

Los resultados del proyecto UMATI, en los que se clasifican las situaciones de incitación al odio y los casos de violencia, o la ausencia de los mismos, durante las elecciones de Kenya de 2013, ofrecen una indicación más amplia de las complejidades de vincular el discurso en Internet con las acciones fuera de línea. En contraste con el contexto electoral anterior, los comicios de 2013 fueron en gran medida pacíficos. Esto no significa que el discurso de incitación al odio fuera menos abrasivo o generalizado. En 2013, a pesar de la ausencia de una base de referencia que pudiera permitir el establecimiento de comparaciones inequívocas, el proyecto UMATI siguió identificando casos graves, generalizados y en curso de incitación al odio y llamamientos a la violencia. Con todo, estos actos de expresión no se tradujeron directamente en violencia sobre el terreno. Como sugirió el equipo, otros factores al margen de la presencia de expresiones de odio han desempeñado probablemente un papel más significativo en cuanto a la incidencia de resultados violentos, y también pacíficos. Los numerosos llamamientos a la paz, procedentes de diversos ámbitos de la sociedad, incluidos los medios de comunicación, los grupos religiosos y los políticos de distintas posiciones en el espectro político, generaron un clima en el que los actos de violencia eran objeto de una firme condena.

El proyecto UMATI brindó además la oportunidad de comparar las percepciones públicas de la incitación al odio con las utilizadas por personas del ámbito académico y en los círculos de la formulación de políticas. Como resultado de una encuesta dirigida a los kenyanos, el proyecto ilustró que la mayoría de los que participaron en la investigación consideraban los insultos personales, la propaganda y los comentarios negativos sobre los políticos como formas de incitación al odio. Tales participantes mantenían asimismo

un concepto de la incitación al odio más amplio que el establecido en la Constitución de Kenya de 2010, que en su artículo 33 prohíbe "la propaganda a favor de la guerra, la incitación a la violencia y al odio, y la apología del odio que instigue a la discriminación por la pertenencia a una etnia, la denigración de los demás o la incitación a causar daño". Como explicó Nanjira Sambuli, Directora de Proyecto de UMATI, conocer cómo conceptualizan la incitación al odio los kenyanos brinda una oportunidad para debatir no solo lo que significa tal fenómeno, sino también para incorporarlo a un debate más amplio sobre la libertad de expresión.

Por último, el proyecto ofreció algunas indicaciones sobre el modo en que las diferentes plataformas de redes sociales pueden habilitar vías específicas para que los mensajes de odio se difundan y se contrarresten. Solo el 3% del total de comentarios que incitan al odio recabados por UMATI se originaron en Twitter, mientras que el 90% se encontraron en Facebook. En el informe final de UMATI figuran algunas indicaciones respecto a los motivos de tal situación, y se apunta a diferencias en las arquitecturas de los distintos sitios. La de Facebook permite que existan grupos y páginas sin actividad en los mismos, y que los usuarios sigan conductas distintas en espacios diferentes. Un usuario puede contar con una biografía "limpia" en su perfil personal, y publicar mensajes de incitación al odio en determinados grupos y páginas. En Twitter, por el contrario, todos los comentarios publicados por un usuario figuran en un único dominio de información, al que puede acceder cualquiera de sus seguidores en la aplicación.

Cuando se trata de abordar la incitación al odio, el proyecto puso de relieve asimismo que las diferentes plataformas permiten distintas respuestas, con una efectividad diversa. En muchos casos, los *tweets* que se consideraron inaceptables fueron objeto de rechazo, y a sus autores se les ridiculizó en público. En ocasiones, el "infractor" fue obligado incluso a retirar sus mensajes debido a la reacción del público en general, o a cerrar del todo su cuenta de Twitter. Como se concluye en el informe de iHub, "la arquitectura singular de hilo de conversación que se emplea en Twitter facilita [este tipo de respuesta], ya que todos los comentarios publicados figuran en un único hilo y los pueden ver todos." Se observó que es menos probable que se den respuestas similares en Facebook, ya que la arquitectura de la plataforma tiende a que las conversaciones se ajusten a un modelo de compartimentos estancos, y a resultar menos accesibles para el conjunto de los usuarios.

Tal seguimiento y análisis de las formas más graves de incitación al odio en línea constituyen una tendencia que puede que se acabe manifestando en muchos otros casos y situaciones.

4.2 MOVILIZACIÓN DE LA SOCIEDAD CIVIL

La experiencia en Myanmar constituye un ejemplo de respuestas positivas de la sociedad civil para promover la concienciación y contrarrestar las voces del odio. Tras aprobar una nueva constitución en 2008 y celebrar elecciones en 2010, Myanmar se ha emprendido

un camino hacia una mayor apertura e integración social. El Gobierno ha liderado diversas reformas en sectores clave, entre los que se cuenta el de los medios de comunicación, en el que han surgido nuevos espacios para el debate. En 2013, el 1,2% de la población disponía de acceso a Internet, y un 12% a un teléfono móvil, una proporción alcanzada partiendo de menos del 1% en 2009. Las dos empresas contratadas para desarrollar la infraestructura de TIC en el país se han comprometido a proporcionar una cobertura de la telefonía móvil superior al 90% en un plazo de cinco años. En este contexto, algunos han utilizado as redes sociales para difundir llamadas a la violencia. En 2014, la Relatora Especial de la ONU sobre cuestiones relativas a las minorías manifestó su preocupación respecto a Myanmar y a la propagación de desinformación, a la incitación al odio y a la violencia, y a la discriminación y la hostilidad en los medios de comunicación y en Internet. Se ha desarrollado una creciente tensión en línea, paralelamente a los casos de violencia real, con el resultado de cientos de fallecidos y miles de desplazados, aunque resultaría simplista buscar vínculos causales directos entre el discurso en Internet y los actos fuera de línea.

Con la rápida aparición de nuevos espacios en línea, aunque para una limitada proporción de la población, las tensiones fuertemente arraigadas se han presentado en una nueva forma. En un contexto en el que Facebook se ha convertido rápidamente en la plataforma preferida de los ciudadanos que dan sus primeros pasos en Internet, la tarea de abordar la intolerancia y la incitación al odio en línea constituye una cuestión cada vez más relevante. En este entorno, algunas personas y grupos han abogado por un uso más dinámico del medio, sobre todo en el caso de aquellos que se creen protegidos por una sensación de superioridad moral y reivindicaciones de actuar en defensa de los intereses nacionales. Ciertas personalidades políticas se han servido asimismo de los medios en línea para atender causas particulares. En las redes sociales, se han utilizado términos despectivos en referencia a minorías. En esta compleja situación, diversos agentes han comenzado a movilizarse, tratando de ofrecer respuestas que eviten ulteriores casos de violencia. Facebook ha procurado adoptar un papel más activo en la vigilancia de los usos de su plataforma de red social en Myanmar, desarrollando asociaciones con organizaciones locales y elaborando directrices sobre la denuncia de problemas accesibles en la lengua birmana. El Ministro de Información de Myanmar se ha comprometido a emprender nuevas acciones en la lucha contra la incitación al odio en línea, y ha manifestado su interés en desarrollar vínculos más sólidos con los Estados Unidos, con el fin de encontrar medidas efectivas para contrarrestar este fenómeno. A continuación se analizan las respuestas creativas formuladas por la sociedad civil local.

La sociedad civil local se ha constituido en una voz firme en la condena abierta de la difusión del discurso del odio en línea y, al mismo tiempo, aboga por la adopción de alternativas a la censura. Entre las respuestas más innovadoras figura la de *Panzagar*, que en birmano significa “discurso de las flores”, y que consistió en una campaña para oponerse abiertamente a la incitación al odio. El objetivo de la iniciativa es ofrecer un ejemplo festivo respecto al modo en que las personas pueden interactuar tanto en Internet, como fuera de línea. Las flores tienen un poderoso significado en Myanmar, y la campaña animó a los usuarios de Facebook a actualizar su perfil con una imagen de sí

mismos sostenido una flor en la boca. La campaña recibió una notable atención a escala tanto nacional, como internacional, pero, como han reconocido algunos activistas, las campañas han de arraigar entre los residentes en áreas rurales, y entre aquellos con un menor nivel educativo. Han de crearse coaliciones de éxito, y es necesario contar con la participación de los líderes religiosos de prestigio. Por otra parte, además de promover "el discurso de las flores", debe denunciarse la violencia. Los activistas apuntan a la toma de conciencia respecto a la necesidad de aclarar los límites de lo que puede decirse y lo que no, y el papel del Estado en el tratamiento del problema.

Aunque iniciativas como *Panzagar* han sido capaces de procurar la participación de diversos colectivos, los grupos de la sociedad civil no comparten necesariamente puntos de vista unánimes sobre las soluciones al problema de la incitación al odio. Algunos son contrarios a las leyes que sancionarían con mayor rigor el discurso del odio, mientras que otros se declaran a favor. A la luz de la transición en curso, los defensores de esta causa señalan la importancia de que la respuesta a la incitación al odio proceda de la sociedad civil. Los activistas locales se han centrado en las soluciones igualmente locales, en lugar de tratar de movilizar a la sociedad civil mundial respecto a estas cuestiones. Esta opción contrasta con otras campañas en línea que han sido capaces de atraer la atención del mundo sobre problemas relativamente desatendidos. Iniciativas como las promovidas por la *Coalición "Save Darfur"* para la guerra civil en Sudán, o la organización *Invisible Children* con la campaña Kony2012 que denunció las atrocidades cometidas por el Ejército de Resistencia del Señor, constituyen ejemplos populares. Como se ha subrayado en los comentarios sobre estas campañas, tales respuestas de ámbito mundial pueden tener repercusiones negativas en la capacidad para encontrar soluciones locales.

El caso de Myanmar es un ejemplo del modo en que las organizaciones de la sociedad civil pueden tomar la iniciativa para movilizar y crear coaliciones locales capaces de abordar las amenazas emergentes. Como han reconocido diversos activistas, el equilibrio entre el enfoque local, la elevación de la atención internacional, la obtención de resultados pertinentes a escala local, y la tarea de evitar la perturbación de una transición delicada, es frágil. Sin embargo, sus esfuerzos ponen de relieve que una movilización contra la incitación al odio en línea puede constituir una oportunidad para facilitar la labor de abordar los conflictos fuera de línea que se reflejan en Internet.

Esta experiencia, como en el caso de la esbozada en el apartado 4.2 anterior, puede ser emblemática de una tendencia potencial emergente que se replica en términos generales en otros países.

4.3 EJERCICIO DE PRESIONES SOBRE EMPRESAS DEL SECTOR PRIVADO

Varias organizaciones que han combatido la incitación al odio en otras formas, o han defendido los derechos de determinados grupos específicos en el pasado, se han encontrado desempeñando un papel cada vez más importante en línea. Esta tendencia

resulta especialmente evidente en los países desarrollados donde la penetración de Internet es elevada, y las empresas del sector privado constituyen intermediarios fundamentales. En este apartado se examinan las campañas e iniciativas emprendidas en los Estados Unidos de América, Australia y el Reino Unido de Gran Bretaña e Irlanda del Norte, donde han surgido cuestiones de incitación al odio relacionadas con la religión, la raza y el género. Organizaciones como la Liga contra la Difamación (ADL por sus siglas en inglés) y Women, Action and the Media (WAM!), con sede en Estados Unidos; Online Hate Prevention Institute, ubicada en Australia; The Sentinel Project, con sede en Canadá; y Tell MAMA (Measuring Anti-Muslim Attacks), radicada en el Reino Unido, dedican cada vez mayores esfuerzos a combatir la incitación al odio en línea mediante el ejercicio de presiones para que los intermediarios de Internet actúen con mayor firmeza contra la incitación al odio en la Red, y a través de la sensibilización de los usuarios.

En algunos casos, las organizaciones se han centrado en influir directamente en las empresas mediante la selección de casos específicos *ad hoc* y la puesta en marcha de negociaciones. Este proceso puede dar lugar a que las organizaciones promuevan sus casos mediante campañas en línea, la formulación masiva organizada de reclamaciones, cartas abiertas, peticiones en línea, y llamamientos activos a la movilización de los partidarios de la causa, tanto en Internet, como fuera de línea. Con todo, son las organizaciones las que impulsan en gran medida una causa específica. Un segundo tipo de iniciativa promovida por algunas organizaciones consiste en recabar quejas de los usuarios respecto a determinados tipos de contenido. Esta actividad resulta especialmente interesante cuando se considera respecto a los procesos que emplean los intermediarios de Internet para resolver los casos de incitación al odio. Aunque algunas empresas han comenzando a publicar informes de transparencia en los que refieren los requerimientos realizados por las administraciones públicas respecto a la revelación o la eliminación de datos, información y otros contenidos, no han divulgado la información relativa a las peticiones formuladas por usuarios individuales. Cuando una persona marca un contenido como inapropiado, puede que se le notifique el estado de tramitación de su reclamación, pero este proceso se mantiene oculto en gran medida respecto a otros usuarios y organizaciones. Como resultado, se limita la posibilidad de promover un mayor conocimiento de qué expresiones se consideran ofensivas, inapropiadas, insultantes o generadoras de odio. Entre los ejemplos de iniciativas de colaboración pública para recabar peticiones de actuación contra determinados tipos de mensajes figuran *HateBase*, promovida por The Sentinel Project y Mobiocracy; la plataforma de denuncia de incidentes de islamofobia de Tell MAMA; y la campaña de *Fight Against Hate* (lucha contra el odio) del Online Hate Prevention Institute. Estas iniciativas constituyen herramientas innovadoras para el seguimiento de la incitación al odio en todas las redes sociales, y del modo en que lo regulan las distintas empresas.

HateBase centra su labor en el análisis de la incitación al odio en mensajes disponibles pública en plataformas de redes sociales, con el fin proporcionar un mapa geográfico del contenido generador de odio difundido en Internet. De este modo, es posible obtener una visión de conjunto de escala global, y también aplicar un enfoque más localizado relativo al lenguaje específico utilizado y a las tendencias y objetivos populares en la incitación al

odio. La base de datos también comprende una función complementaria de denuncia individual utilizada para mejorar la precisión y el alcance del análisis, al procurar que los usuarios verifiquen los ejemplos de incitación al odio en línea, y confirmen la naturaleza generadora de odio de estos casos en una comunidad determinada. Del mismo modo, Fight Against Hate hace posible que se denuncien los casos de incitación al odio en línea en diversas redes sociales en una única plataforma, lo que ayuda a los usuarios a llevar un seguimiento del número de personas que denuncian los contenidos que incitan al odio, del lugar del que proceden, del plazo que le lleva a las empresas privadas responder a las denuncias, y de si el contenido en cuestión se ha moderado de manera efectiva. Por último, Tell MAMA ofrece una función similar de denuncia de múltiples sitios en una sola plataforma, aunque se centra únicamente en el contenido antimusulmán. Esta plataforma de denuncia también facilita la documentación de incidentes relacionados con la raza o la religión, para su análisis posterior. Las denuncias recibidas en la plataforma las tramita la organización que, a continuación, se pone en contacto con las víctimas y las ayuda a abordar el proceso de comunicación de los incidentes a las autoridades policiales pertinentes. La información registrada se utiliza asimismo para detectar las tendencias de la incitación al odio en Internet y fuera de línea contra los musulmanes en el Reino Unido.

En alusión a la importancia de generar datos empíricos, Andre Oboler, Primer Ejecutivo del Online Hate Prevention Institute, señaló que plataformas como estas brinda la posibilidad de realizar requerimientos visibles para otros usuarios registrados, lo que les permite efectuar un seguimiento de la fecha de la primera denuncia del contenido, del número de personas que lo denunciaron, y del plazo medio que lleva su supresión. A través de estos y otros medios, tales organizaciones pueden pasar a formar parte de coaliciones más amplias integradas por agentes participantes en el debate sobre la necesidad de encontrar un equilibrio entre la libertad de expresión y el respeto por la dignidad humana y la igualdad. Esta situación se ilustra adecuadamente en el ejemplo que sigue, en el que una página de Facebook con expresiones de odio contra los aborígenes australianos fue suprimida en última instancia por esta red social aún cuando la página no infringía abiertamente las condiciones de servicio de la empresa, porque diversos agentes, incluidos grupos de la sociedad civil y de presión, reguladores, y usuarios individuales determinaron que resultaba insultante.

Este caso ilustra cómo una controversia a gran escala en una determinada comunidad respecto a la incitación al odio en línea puede ser objeto de la atención de las organizaciones y las autoridades públicas interesadas que, a continuación, se implican activamente en el debate en línea, y ejercer presión sobre las empresas privadas para que estas resuelvan un asunto relacionado con tal práctica de incitación. En 2012, una página de Facebook en la que se hacía burla de los indígenas australianos denominándoles “memes aborígenes” provocó una airada protesta local en el ámbito de Internet en forma de un aluvión organizado de denuncias de abuso de contenido, una amplia cobertura de los medios de comunicación, una campaña social en la Red y una petición en línea exigiendo que Facebook suprimiera el contenido en cuestión. Meme se refiere en este caso a una forma visual de transmisión de mensajes breves a través de una combinación de imágenes con inscripciones incluidas en el cuerpo de la foto.

El amplio apoyo en línea a la lucha contra la página de Facebook de los "memes aborígenes" resultó notable en todas las plataformas de redes sociales y de información, y suscitó además el interés de diversos canales de noticias extranjeros. En respuesta a la conmoción en los medios de comunicación, Facebook publicó una declaración oficial, reconociendo que ciertos contenidos podrían ser "controvertidos, ofensivos, o incluso ilegales". A raíz de la declaración de Facebook, el Comisionado Australiano de Derechos Humanos refirió su desaprobación respecto a la polémica página, y al hecho de que Facebook actuase con arreglo a la Primera Enmienda de la Constitución de los Estados Unidos en un asunto que atañía a un infractor y a unas víctimas con residencia en Australia.

La petición en línea se estableció como reacción ulterior a la negativa de Facebook a retirar el contenido mediante la respuesta automática a varias denuncias de abuso de contenido con una declaración normalizada. En la carta abierta incluida en la petición se explicaba que el contenido se consideraba ofensivo debido a los ataques reiterados contra un grupo específico por motivos de raza, y se exigía que Facebook tomara medidas suprimiendo las páginas en cuestión y otras similares dirigidas contra los indígenas australianos. Facebook retiró temporalmente las páginas para la revisión de su contenido. Tras las conversaciones mantenidas con el Comisionado de Discriminación Racial y el Instituto, Facebook concluyó que el contenido no infringía sus condiciones de servicio, y permitió que las páginas se mantuvieran, bajo el requisito de incluir el término "controvertido" en su título para indicar claramente que en la página figuraba ese tipo de contenidos.

La segunda fase del caso tuvo lugar cuando un usuario de Facebook comenzó a dirigirse a activistas contrarios a la incitación al odio en línea con ataques personales de esta índole debidos al caso de los "memes aborígenes". Facebook respondió mediante el seguimiento y la supresión de los numerosos usuarios falsos creados por el infractor, pero le permitió mantener una cuenta operativa. Finalmente, en una tercera fase, Facebook impidió el acceso a la controvertida página en Australia, después de que el Comisionado de Discriminación Racial y la Autoridad Australiana de Comunicaciones y Medios de Información expresarán públicamente su preocupación al respecto. Con todo, la página prohibida de Facebook sigue siendo operativa y accesible desde fuera de Australia, y continúa difundiendo los contenidos generadores de odio publicados en otras páginas disponibles en dicho país. Los intentos de impedir a determinados usuarios que siguieran divulgando los polémicos "memes aborígenes" dieron lugar a que se les impusiera una prohibición de utilizar Facebook durante 24 horas.

En el siguiente caso, las organizaciones en cuestión abordaron una prolongada controversia en la Red y fueron más allá de la intervención como intermediarios de las quejas, presionando de manera activa e intensa a las empresas, y exigiendo una moderación más rigurosa de los contenidos y una acción autorreguladora permanente ulterior. En 2013, el grupo Women, Action and the Media (WAM!) y el Proyecto sobre el Sexismo Ordinario (*Everyday Sexism Project*) en el Reino Unido emprendieron una campaña común para mostrar anuncios de empresas destacadas en páginas de Facebook en los que se difundían contenidos gráficos abusivos para las mujeres. En respuesta

a la campaña, tanto Nissan, como la compañía de seguros Nationwide retiraron sus anuncios de Facebook. A la vista del éxito obtenido, los organizadores, con el respaldo de partidarios y activistas en línea, comenzaron a enviar reclamaciones por escrito y fotografías de los anuncios en páginas de incitación al odio a otras grandes empresas como Dove y American Express en sus plataformas de redes sociales, instándoles a actuar del mismo modo. Como resultado de la campaña, 15 grandes compañías optaron por retirar su publicidad de Facebook.

La campaña comprendió además una carta abierta redactada por los dos grupos antes referidos, en la que figuraban páginas que promovían la violación y otros actos de violencia contra las mujeres, y en la que se exigía que tales páginas fueran suprimidas y que Facebook revisara su política de regulación de contenidos. Junto con la carta abierta, una petición en línea en change.org recogió más de 225.000 firmas y contribuyó a la sensibilización respecto a estas cuestiones entre los usuarios de Internet. Los colaboradores de la campaña emprendieron otras acciones, como la puesta en marcha de una protesta a gran escala frente a la junta de accionistas de Facebook, la publicación del nombre de todas las empresas relevantes usuarias de la plataforma para la publicidad en línea, y el llamamiento para el envío a tales empresas de cartas de reclamación instando a estas a retirar sus anuncios de Facebook. Además, los activistas recabaron los servicios de expertos financieros en sus páginas de redes sociales, pidiéndoles que analizaran los posibles perjuicios fiscales que podría sufrir Facebook debido al creciente número de empresas que retiraban su publicidad. La campaña en línea con la etiqueta #FBrape dio lugar a que Facebook se pusiera en contacto con las organizaciones en cuestión, en el marco de una solicitud de cooperación. La campaña de #FBrape recibió una notable atención de los medios de comunicación únicamente después de que presionara con éxito a la empresa para que esta luchara activamente contra los contenidos de incitación al odio dirigidos a mujeres. La campaña había logrado un rápido éxito al establecer como objetivo a determinadas empresas y sus campañas de publicidad, en lugar de limitarse a Facebook directamente.

Sin embargo, la respuesta de Facebook no fue tan cooperativa inicialmente, ya que mantuvo que las páginas consignadas en la carta abierta no infringían las condiciones de servicio de la empresa. No obstante, poco después del inicio de la campaña y de que las empresas comenzaran a retirar sus anuncios, los contenidos ofensivos se suprimieron con celeridad. A continuación, Facebook publicó una declaración oficial en su sitio web, afirmando que deseaba aclarar sus condiciones de servicio y sus políticas de regulación de contenidos, así como promover la cooperación con las organizaciones que trabajan para promover la libertad de expresión, sin dejar de prevenir que se dirijan discursos de incitación al odio contra determinados grupos y personas. Reconociendo su omisión en la identificación y supresión de expresiones de odio, la empresa declaró su intención de revisar y actualizar sus directrices en cuanto a la moderación de ese tipo de expresiones, de impartir a sus moderadores de contenidos una formación de mejor calidad, de reforzar su colaboración con las organizaciones interesadas para contribuir a un esfuerzo compartido y flexible capaz de contrarrestar mejor los contenidos de incitación al odio

en línea, así como de actuar para exigir responsabilidades a los distribuidores de tales contenidos ofensivos por sus acciones.

En un caso al margen, aunque relacionado con el anterior, Twitter también adoptó una postura contraria al acoso en línea de las mujeres, en colaboración con WAM!, mediante la puesta en marcha de un proyecto piloto conjunto en forma de una plataforma de denuncia con la que se intentaría moderar los contenidos señalados en un plazo de 24 horas. Con las denuncias presentadas por las mujeres víctimas de abusos en línea se pretende atender una doble finalidad: por un lado, permitir que WAM! recabe datos sobre contenidos ofensivos centrados en el acoso en línea basado en el género, con el fin de analizar el fenómeno con detenimiento y, por el otro, ayudar a Twitter a mejorar sus mecanismos de regulación de contenidos en relación con los casos de discriminación y abuso en línea relacionados con el género. La herramienta de denuncia pide a las mujeres que nombren a los usuarios concretos que las acosan, o los tuits específicos que consideran ofensivos, que clasifiquen el tipo de acoso, y que respondan a preguntas generales sobre el número de veces en que han sido acosadas, en qué plataformas, y si el acoso lo cometieron uno o varios usuarios. Una vez presentada la denuncia, las reclamaciones se someten al examen de WAM!, y posteriormente se trasladan a Twitter para su investigación y moderación ulteriores. El programa piloto de la herramienta de denuncia se mantuvo activo durante tres semanas, en las que, según el propio programa, se recibieron 700 denuncias y se ayudó a más de 100 personas a obtener respuestas más rápidas de Twitter. WAM! prevé la elaboración de un informe sobre los datos recabados, encaminado a lograr una mejor interpretación de los casos de incitación al odio en línea contra las mujeres.

Parece que la lucha contra la incitación al odio en línea percibida comienza a alcanzar a varias partes interesadas, desde las administraciones públicas, a las empresas de tecnología y los proveedores de servicios de Internet, pasando por un número creciente de organizaciones activas y personas afectadas. Muchas comunidades y usuarios individuales en Internet luchan contra los contenidos generadores de odio en línea a diario, junto con otras organizaciones más formales. Sin embargo, esta lucha requiere una acción a gran escala con el fin de garantizar que la incitación al odio en línea pueda identificarse y corregirse en el largo plazo de manera efectiva y contextual. Exige además la capacitación de los usuarios para identificar y combatir los casos de incitación al odio sin bloquear el discurso legítimo, creando de este modo espacios más integradores para la expresión.

Los intermediarios de Internet, y las plataformas de redes sociales en particular, han mostrado una tendencia al avance en sus respuestas a los casos presuntos de incitación al odio en línea a través de una interacción prudente con las quejas de los usuarios, y de una creciente transparencia de sus procesos de regulación. Los directivos de Facebook han señalado que confían en múltiples equipos encargados de examinar diversos tipos de contenido en distintas lenguas, con el fin de actuar respecto a las denuncias con la máxima celeridad y eficacia posibles. Por otro lado, Facebook ha adoptado un cuadro de indicadores para realizar las denuncias que permite a los usuarios llevar un seguimiento del proceso de revisión, con el fin de mejorar sus comunicaciones individuales con cada

usuario. Adoptando mecanismos similares para abordar la incitación al odio, Twitter introdujo un botón de denuncia en 2013, tras una petición en línea formulada por un usuario individual.

En resumen, parece existir una tendencia a la colaboración cada vez más estrecha de los intermediarios de Internet con las organizaciones que realizan campañas, encaminada a proporcionar respuestas rápidas y efectivas a la incitación al odio en sus plataformas. Al mismo tiempo, dichos intermediarios también refieren que ponderan equitativamente las reclamaciones formuladas por usuarios individuales, y que tratan estas con tanta seriedad como en el caso de las peticiones y otras formas de acción colectiva. En cierta medida, estas empresas comienzan además a publicar informes para comunicar a los usuarios cualquier cambio en sus políticas y regímenes en materia de privacidad, aunque son pocas las que facilitan información acerca de las denuncias de los usuarios en comparación con los informes de transparencia sobre los requerimientos oficiales de administraciones públicas. Las acciones de los grupos autores de las campañas desempeñan un papel importante, en ocasiones conjuntamente con la actuación de funcionarios públicos y, en particular, en aquellos casos en los que, por diversos motivos, resulta poco práctico o problemático que las propias administraciones públicas aborden la cuestión.

4.4 CONTRARRESTAR LA INCITACIÓN AL ODIO EN INTERNET MEDIANTE LA ALFABETIZACIÓN MEDIÁTICA E INFORMACIONAL (MIL)

Mientras que en los apartados anteriores se han abordado mayoritariamente las respuestas reactivas a la proliferación de casos de incitación al odio en línea, en este apartado se analizan los intentos de ofrecer respuestas más estructurales a través de la educación. Se examinan diversas iniciativas dirigidas a los ciudadanos, y en especial a los jóvenes, para que tomen conciencia de las cuestiones que les rodean y de las posibles respuestas a la incitación al odio percibida en Internet.

La educación para la ciudadanía se centra en la preparación de los que la reciben para ser ciudadanos informados y responsables mediante el estudio de derechos, libertades y responsabilidades, y se ha empleado de diversas maneras tanto en sociedades pacíficas, como en otras que salen de un conflicto violento. Uno de sus objetivos principales consiste en promover la sensibilización respecto a los derechos políticos, sociales y culturales de personas y grupos, incluida la libertad de expresión y las responsabilidades e implicaciones sociales que se derivan de la misma. El interés de la educación para la ciudadanía en la incitación al odio es doble: atañe al conocimiento y las destrezas para identificar este fenómeno, y permite a sus destinatarios contrarrestar los mensajes de odio. Uno de sus retos actuales consiste en adaptar sus metas y estrategias al mundo digital, proporcionando un conocimiento y unas destrezas no solo para la argumentación, sino también de índole tecnológica, que un ciudadano puede necesitar

para contrarrestar la incitación al odio en la Red. Algunas organizaciones proponen un nuevo concepto de ciudadanía digital, en el que se incorporan los objetivos esenciales de la alfabetización mediática e informacional encaminada al desarrollo de las destrezas técnicas y primordiales para los consumidores y productores de medios en línea, y que les pone en contacto con asuntos éticos y cívicos de mayor alcance.

Es relevante a este respecto la educación para una ciudadanía mundial (GCED por sus siglas en inglés), una de las áreas de trabajo estratégicas del Programa de educación de la UNESCO para el período de 2014-2017, y una de las tres prioridades de la Iniciativa Mundial para la Prioridad de la Educación de la Secretaría General de la ONU. La GCED se propone dotar a los alumnos de todas las edades de los valores, conocimientos y destrezas que se basan en los derechos humanos, la justicia social, la diversidad, la igualdad de género y la sostenibilidad medioambiental, y que infunden respeto por todos estos conceptos. La GCED proporciona a los alumnos las competencias y la oportunidad para realizar sus derechos y obligaciones y promover así un mundo mejor y un futuro más halagüeño para todos.

Con esta perspectiva de mayor amplitud, la UNESCO y muchas otras entidades que trabajan bajo la égida de la Alianza Mundial para las Asociaciones sobre Alfabetización Mediática e Informacional promueven la capacitación de los usuarios. La MIL es un concepto global que comprende un paquete de competencias para su aplicación en Internet y fuera de línea. Incluye el desarrollo de las destrezas y capacidades técnicas requeridas para utilizar las tecnologías digitales, así como los conocimientos y facultades necesarias para encontrar, analizar, evaluar e interpretar textos de medios de comunicación específicos, crear mensajes en los medios de comunicación, y reconocer su influencia social y política. Múltiples competencias complementarias se consideran esenciales para el ejercicio de los derechos y las responsabilidades relacionados con las comunicaciones.

La aparición y auge de las nuevas tecnologías y las redes sociales han desempeñado un papel importante en esta transformación. Las personas han pasado de ser meras consumidoras de mensajes de los medios de comunicación, a productoras, creadoras y conservadoras de información, dando lugar a nuevos modelos de participación que interactúan con los tradicionales. Las estrategias docentes evolucionan en consecuencia, y pasan de fomentar la recepción crítica de los mensajes de los medios de comunicación, a incluir la habilitación para la creación de contenidos en dichos medios. Se observa una fuerte tendencia en la propia MIL a la continuidad en su evolución como concepto, reforzada por la dinámica de Internet. Comienza a englobar cuestiones de identidad, ética y derechos en el ciberespacio (véase la Declaración de París sobre la MIL en la era digital).

Ciertos conocimientos y destrezas pueden revestir especial importancia cuando se trata de identificar y responder a la incitación al odio en línea. En el presente apartado se analizan las iniciativas encaminadas a proporcionar información y herramientas prácticas a los usuarios de Internet para actuar como ciudadanos digitales activos. Entre los proyectos y las organizaciones consideradas figuran:

- "*No place for hate*" (sin lugar para el odio), de la Liga contra la Difamación (ADL), de Estados Unidos;
- el proyecto "*In other words*" (en otras palabras), a cargo de la Provincia de Mantua y la Comisión Europea;
- "*Facing online hate*" (afrontar el odio en la Red), a cargo de MediaSmarts, Canadá;
- "*No hate speech movement*" (movimiento contra el discurso del odio), a cargo del Departamento de Juventud del Consejo de Europa;
- "*Online hate*" (el odio en Internet), a cargo del Online Hate Prevention Institute, de Australia.

Aún cuando las iniciativas y organizaciones referidas presentan características singulares y persiguen fines específicos, todas hacen hincapié en la importancia de la MIL y de las estrategias educativas como medio efectivo para contrarrestar la incitación al odio. Subrayan la capacidad de un enfoque educativo para constituir una respuesta estructural y sostenida al discurso del odio, considerado en comparación con las complejidades que conllevan las decisiones de prohibir o censurar los contenidos en línea, o el tiempo y el coste que pueden requerir las acciones judiciales para producir resultados tangibles. Muchos argumentan que el paquete de competencias integrado en la MIL puede facultar a los usuarios y dotarles de las competencias que necesitan para responder a los casos de incitación al odio percibidos con celeridad, tan pronto se planteen. Este hecho puede resultar especialmente importante dada la prioridad que otorgan las plataformas de redes sociales a la denuncia individual de casos de abuso, incitación al odio o acoso.

Los participantes en estas iniciativas tienden a reconocer la importancia de los marcos normativo y jurídico como referencia para sus esfuerzos. La mayoría de las iniciativas incluyen la educación sobre los instrumentos jurídicos y los procedimientos utilizados para el enjuiciamiento de los autores de los actos de incitación al odio en línea, y muchos promueven una visión complementaria entre los aspectos jurídicos y educativos.

Un denominador común de las iniciativas analizadas es la prioridad otorgada al desarrollo de las capacidades para el pensamiento crítico y el uso éticamente reflexivo de las redes sociales (sobre la base de los principios de los derechos humanos), como puntos de partida para que las destrezas adquiridas mediante la MIL permitan combatir la incitación al odio en Internet. Se espera que estas competencias de la MIL puedan reforzar la capacidad de las personas para identificar y poner en cuestión los contenidos generadores de odio en línea, comprender algunos de sus supuestos, sesgos y prejuicios, y promover la elaboración de argumentos para hacerle frente. Las iniciativas que se examinan aquí desempeñan asimismo un importante papel al demostrar que la identificación de los casos de incitación al odio en Internet no es necesariamente tan sencilla como les puede parecer a algunos.

Las iniciativas analizadas tienden a dirigirse a diversas audiencias compuestas por usuarios a los que atañe y afecta el discurso del odio en línea. Las organizaciones

participantes estudiadas en el presente apartado centran sus esfuerzos en particular en los grupos vulnerables, y en aquellos propensos a ser víctimas del odio, o a ser reclutados por los grupos que lo practican. Los niños y los jóvenes constituyen uno de los principales colectivos objeto de estas iniciativas. Los padres, los profesores y la comunidad escolar también tienden a ser considerados destinatarios relevantes debido a su papel en la exposición de los menores a los contenidos generadores de odio, y en su protección frente a los mismos. Otros grupos también destinatarios de tales iniciativas son los compuestos por aquellos con la capacidad para conformar el panorama jurídico y político de la incitación al odio en Internet, incluidos los responsables de la formulación de políticas y las ONG, y por los que pueden ejercer un notable efecto en la comunidad en línea que expone el discurso del odio, entre los que destacan los periodistas, los blogueros y los activistas. En el cuadro 1 figura un resumen de las diferentes audiencias a las que se dirigen las iniciativas analizadas.

Cuadro 1. Audiencias consideradas por cada iniciativa educativa

	Menores	Jóvenes	Profesores	Padres	Responsables de la formulación de políticas	Blogueros	ONG	Público en general
Liga contra la Difamación	X	X	X	X	X			
In Other Words					X	X	X	X
No Hate Speech Movement		X				X		X
MediaSmarts	X	X	X	X				
Online Hate Prevention		X				X	X	X

Los objetivos de cada proyecto están estrechamente relacionados con los intereses y las necesidades de la audiencia pretendida de la iniciativa. Por ejemplo, MediaSmarts ha desarrollado un videojuego en línea para niños de 12 a 14 años de edad, diseñado para elevar su capacidad para reconocer sesgos, prejuicios y propaganda del odio. En el videojuego, cuando los menores se encuentran con diferentes grados de prejuicio y discriminación en forma de bromas, noticias o vídeos, se les pide que determinen el modo en que tales mensajes pueden promover el odio y, a continuación, que desarrollen estrategias para abordar dichos mensajes, ya sea pasándolos por alto, o afrontándolos.

La ADL ha centrado gran parte de su actuación y sus esfuerzos educativos en los profesores y los padres, facilitándoles información esencial sobre la manera de comentar los asuntos relacionados con el odio y la violencia con los menores, y sobre el modo de animar a los jóvenes a emprender las acciones pertinentes. El *No Hate Speech Movement* (movimiento contra el discurso del odio) organiza sesiones de formación dirigidas a blogueros y jóvenes activistas, en las que estos pueden comentar sus experiencias de casos de incitación al odio en Internet y compartir las buenas prácticas

aplicadas para combatirlos. Con tales sesiones se pretende promover una interpretación de base del discurso del odio y promover la toma de conciencia respecto al impacto que pueden ejercer blogueros y activistas en el tratamiento de los contenidos generadores de odio. El proyecto "*In Other Words*" ha procurado influir en los responsables de la formulación de políticas y en la sociedad civil para que aborden la vigilancia de diversos tipos de medio. Aboga por el uso de una información precisa sobre las minorías y los grupos vulnerables en las manifestaciones de los medios de comunicación, y anima a la vigilancia encaminada a evitar la difusión de estereotipos, prejuicios y otros discursos discriminatorios.

A pesar de las particularidades de los contenidos y las audiencias de cada iniciativa, todas comparten tres fines educativos generales: informar sobre el discurso del odio, analizarlo, y hacerle frente. Estos tres fines pueden percibirse en una escala que comprende metas progresivas y objetivos específicos, cada uno de ellos centrado en diferentes aspectos del problema y la provisión de alternativas concretas para responder al odio en línea. Un resumen figura en el cuadro 2.

Cuadro 2. Metas y objetivos educativos

Información	Análisis	Acción
– Fomentar la sensibilización respecto a la incitación al odio y sus consecuencias. – Transmitir y difundir información. – Comunicar el marco jurídico pertinente.	– Identificar y evaluar los casos de incitación al odio. – Analizar causas comunes y supuestos y prejuicios subyacentes. – Reconocer conductas sesgadas. – Denunciar y exponer los casos de incitación al odio.	– Responder a la incitación al odio. – Escribir contra la incitación al odio. – Modificar el discurso de la incitación al odio. – Seguimiento de los medios de comunicación.

La primera meta educativa consiste en transmitir información sobre la incitación al odio, e incluye la sensibilización respecto a la incitación al odio en Internet, sus diversas formas, y sus posibles consecuencias. Comprende además la provisión de información sobre los marcos jurídicos nacionales, regionales e internacionales pertinentes. Pueden encontrarse ejemplos de estas iniciativas en múltiples formatos, como el vídeo titulado "*No Hate Ninja Project - A Story About Cats, Unicorns and Hate Speech*" (Proyecto ninja de lucha contra el odio - Una historia sobre gatos, unicornios y el discurso del odio), a cargo del *No Hate Speech Movement*; el tutorial electrónico interactivo denominado "*Facing online hate*" (Afrontar el odio en Internet), de MediaSmarts, o el conjunto de herramientas desarrollado por el proyecto "*In Other Words*" (en otras palabras).

La segunda meta educativa es más compleja y se centra en la comprensión a través del análisis de la incitación al odio en Internet. Este análisis comprende valoraciones y evaluaciones de los distintos tipos de discurso del odio en línea, incluidos el racismo, el sexismo y la homofobia, y de las múltiples formas en las que se presenta. Un aspecto importante del análisis es el examen crítico de la incitación al odio con el fin de determinar sus causas comunes y comprender sus supuestos y prejuicios subyacentes. Este proceso analítico hace posible que los usuarios denuncien y expongan los contenidos generadores

de odio en la Red. Son ejemplo de proyectos con esta meta educativa el foro de debate "*No Hate*" (sin odio) y la plataforma "*Reporting hate speech*" (denuncia del discurso del odio). El foro de debate gestionado por el *No Hate Speech Movement* permite que los jóvenes analicen lo que constituye un contenido generador de odio, y refieran los ejemplos de incitación al odio en línea que se hayan encontrado con anterioridad. La plataforma de denuncia diseñada por el *Online Hate Prevention Institute* permite a los usuarios que comuniquen y vigilen los casos de incitación al odio en Internet mediante la indicación de lo que perciben como contenidos de esta índole; el seguimiento de sitios web, foros y grupos; y la revisión de los materiales generadores de odio descubiertos por terceros.

La tercera meta educativa identificada en estas iniciativas hace hincapié en el fomento de las acciones dirigidas a combatir y contrarrestar los actos de incitación al odio. Con los recursos empleados en el marco de esta meta educativa se pretende promover acciones y respuestas concretas al discurso del odio en la Red. Las acciones propuestas varían, dependiendo del enfoque del proyecto y la organización, y de su naturaleza más o menos combativa y beligerante. En cualquier caso, la prioridad fundamental sigue siendo la capacitación de los usuarios para responder a los contenidos generadores de odio y para combatirlos de manera asertiva. Son ejemplos de estas iniciativas las sesiones de formación dirigidas a blogueros, periodistas y actividades, y gestionadas por el *No Hate Speech Movement*; los materiales docentes y los planes de estudio elaborados por MediaSmarts; y las políticas de vigilancia de los medios de comunicación propuestas por el proyecto "*In Other Words*".

Mientras que algunas organizaciones e iniciativas se centran en el contenido del discurso del odio en Internet, otras hacen hincapié en su aspecto personal, llamando la atención respecto a las víctimas o al impacto general en la comunidad. Con independencia de su enfoque, la mayoría de proyectos consideran que el desarrollo de destrezas digitales constituye un aspecto esencial para prevenir, exponer y combatir la incitación al odio en la Red. Las herramientas y estrategias analizadas ponen de relieve diversos enfoques respecto al desarrollo de tales destrezas, desde las guías básicas de actuación, a una formación más compleja y especializada. La gran variedad de formatos examinados y analizados en las distintas iniciativas hace posible llegar y atraer a audiencias muy dispares.

En todo caso, siguen faltando evaluaciones exhaustivas de estas iniciativas, y resulta difícil determinar si tienen éxito, y en qué medida, en la lucha contra el discurso del odio, o en la tarea de influir en los grupos que más probablemente participen en la incitación al odio en línea. Por ejemplo, aunque las iniciativas y los recursos de MediaSmarts han recibido múltiples galardones y reconocimientos, no se ha establecido claramente quiénes son los que más se aprovechan de sus recursos, y resulta difícil evaluar los resultados de sus programas. En el caso del proyecto "*In Other Words*", entre los resultados previstos figuraba el desarrollo de materiales para su divulgación, pero no se dispone de información sobre el modo en que se han utilizado tales materiales desde su publicación, ni sobre a qué audiencias han llegado. Tampoco en el caso del "*No Hate Speech Movement*", que ha desarrollado diversos materiales y recursos (entre los que se cuentan vídeos, manuales de formación, herramientas docentes y la plataforma en línea para la denuncia de contenidos generadores de odio), existen directrices inequívocas y públicas sobre

la manera de evaluar o comunicar los efectos obtenidos. Aunque la mayoría de estas iniciativas son encomiables y capaces de ofrecer instrumentos potentes para combatir el discurso del odio a escala estructural, se necesita más información para comprender el modo en que las personas integran las destrezas recién adquiridas en su vida diaria, y qué impacto tiene tal integración en su actividad en Internet. Tal necesidad puede abordarse como una posible tendencia emergente a medida que evolucionan las respuestas a la incitación al odio en línea.

4.5 MODERACIÓN DE CONTENIDOS EN LOS MEDIOS DE COMUNICACIÓN

Al margen de los casos de abusos cometidos por tabloides, los artículos sobre discursos del odio no equivalen generalmente a una apología de la incitación a la discriminación, la hostilidad o la violencia, y forman parte más bien de un servicio informativo de interés público sobre las realidades que se deben conocer. Sin embargo, es habitual que las instituciones de los medios de comunicación se encuentren a menudo con la necesidad de identificar y responder a tal tipo de discurso publicado por los usuarios en las plataformas en línea de dichas instituciones. Diversos sistemas y prácticas se han analizado en dos estudios: una revisión de las excepciones jurídicas e institucionales en el sudeste de Europa a cargo del Instituto de Medios de Comunicación de Albania, y otro titulado *Online comment moderation: emerging best practices* (Moderación de comentarios en línea: buenas prácticas emergentes), producido por la Asociación Mundial de Periódicos y Editores de Noticias, en el que se analizan las prácticas de 104 medios de comunicación de 63 países. Gestionar los flujos dinámicos de mensajes de los usuarios, sin restringir la expresión legítima, constituye todo un reto para los medios informativos, y pone de relieve la necesidad de políticas relativas al modo en que cada institución define la incitación al odio, como fundamento para determinar qué respuestas calibradas pueden reclamarse. Esto requiere un sistema de vigilancia a cargo de cada medio de comunicación, aunque se trate únicamente de un mecanismo mínimo para que los lectores puedan indicar y denunciar los incidentes para su ulterior investigación por los editores de las plataformas. Las prácticas de vigilancia y análisis de la incitación al odio en línea en los medios informativos podrían compartirse de manera rentable con las empresas de intermediarios de Internet, a pesar de la diferente posición de estos dos tipos de entidades. La Red de Periodismo Ético (Ethical Journalism Network) ha promovido un plan de cinco puntos concebido para que las salas de redacción identifiquen los casos de incitación al odio y respondan en consecuencia, tanto en la cobertura de noticias, como en la moderación de los comentarios de los usuarios. Puede surgir una tendencia (tanto en Internet, como fuera de línea) del afán por instrumentalizar el periodismo al servicio de la lucha contra el discurso del odio. En cualquier caso, es ampliamente reconocido que uno de los antídotos a este tipo de discurso consiste en las normas de información profesional, y en comunicar de manera creíble al público destinatario los hechos que atañen a la presencia, la naturaleza y el impacto de tales expresiones en una sociedad determinada.

5. CONCLUSIÓN Y RECOMENDACIONES

La aparición y la propagación de la incitación al odio en Internet constituyen un fenómeno en evolución. Las tendencias ponen de relieve el surgimiento de una combinación de medidas para abordar la complejidad de un fenómeno que aún no se entiende bien, y que las sociedades desarrollan las respuestas personalizadas y coordinadas planteadas por diversos agentes. A medida que evolucionan tales tendencias, se requerirán soluciones efectivas fundamentadas en una mejor comprensión del modo en que las diversas formas de expresión surgen, interactúan y, posiblemente, desaparecen en línea. La aparición de cada una de las respuestas examinadas en el presente capítulo se vincula a determinadas circunstancias singulares, pero su análisis y difusión proporcionan una gama general de métodos que los distintos interlocutores pueden adaptar en lo que atañe al desarrollo de dichas tendencias y la obtención de un efecto ulterior. Es posible señalar varios aspectos generales relativos a las tendencias de la incitación al odio en línea y la evolución de las respuestas a este fenómeno:

5.1 DEFINICIÓN E INTERPRETACIÓN

- Es probable que las instituciones internacionales sigan evitando el establecimiento de definiciones rigurosas de la incitación al odio. Tal precaución parecen compartirla importantes agentes privados que conforman la comunicación en Internet. Las plataformas de redes sociales han evitado la propuesta de normas y procedimientos estrictos para identificar qué tipo de contenidos deben eliminarse. Algunos han tratado de "socializar" la moderación de contenidos, permitiendo que los usuarios resuelvan las controversias mediante las interacciones facilitadas por la plataforma. De este modo se posibilita la consideración de diversos matices y se evita un enfoque mecánico.

- Se han promovido definiciones más restringidas, y su uso puede ser adoptado de manera más general por diversos agentes, precisamente con el fin de priorizar las formas más graves de incitación al odio en una época de flujos de información masivos. Tales definiciones comprenden los conceptos de "discurso peligroso" y "discurso del miedo". Son nociones que ofrecen herramientas para identificar y describir determinadas formas de incitación al odio, posiblemente señalando los casos críticos o zonas de peligro en las que las respuestas colectivas pueden resultar necesarias para evitar la propagación de la violencia. Se trata de un aspecto importante en la respuesta al reto de establecer conexiones entre las expresiones de odio en línea y los daños reales, como la hostilidad, la discriminación o la violencia. Los elementos que caracterizan la comunicación en Internet, como el anonimato percibido por los usuarios y la inmediatez con la que un determinado mensaje puede

llegar a audiencias amplias, hacen que el problema resulte especialmente complejo. Siguen faltando estudios sistemáticos sobre las conexiones entre la incitación al odio en línea y la violencia fuera de línea, y es posible que tal necesidad de lugar a una tendencia de la investigación en los próximos años.

- Al mismo tiempo, adoptar un enfoque restringido puede tener una parte negativa si se aplica en exclusiva. Se corre el riesgo de que la prioridad otorgada al potencial de un acto de incitación al odio para dar lugar a situaciones de violenta pueda propiciar que se adopte un planteamiento estrecho limitado a las respuestas de la ley y el orden. Concentrarse únicamente en la violencia puede llevar a respuestas que privilegien al Estado (como agente que cuenta con el control legítimo del uso de la violencia), y a que se pasen por alto posiblemente otros agentes que podrían promover soluciones diferentes o complementarias. Sin embargo, existen interpretaciones alternativas de la incitación al odio que se centran en el respeto de la dignidad humana desde una perspectiva más amplia, así como en la habilitación de los destinatarios de los actos de incitación para exigir respeto y que se les defienda, colocándoles de este modo en el centro de las iniciativas de respuesta efectivas, en lugar del Estado o cualquier otro agente. Tal enfoque no está exento de problemas y contradicciones, ya que un énfasis excesivo en la dignidad puede dar lugar a una cacofonía de relativismo o de apoyo a ideas particularistas disconformes con los derechos humanos. Sin embargo, propone que, al abordar la incitación al odio en Internet, se tengan en cuenta diferentes perspectivas, y que se comparen, en lo que respecta a su capacidad tanto para explicar este fenómeno y su complejo vínculo con la violencia real, como para ofrecer respuestas que reflejen un planteamiento más global.

- Paradójicamente, la complejidad de la definición del discurso del odio también ofrece oportunidades para desarrollar interpretaciones locales compartidas de los distintos estándares internacionales en esta materia. La incitación al odio actúa como una especie de “significante vacío”. Es un término que puede parecer que se explica por sí mismo para la mayoría, pero para el que se tiende a ofrecer descripciones muy dispares cuando se pregunta por él. Este hecho puede suponer un problema, por ejemplo, cuando las acusaciones de emitir mensajes generadores de odio se utilizan instrumentalmente para desacreditar un discurso legítimo o justificar casos de censura. Son casos en los que la crítica o la ridiculización de personas, o de opiniones o creencias, se etiqueta como incitación al odio, superando con mucho los parámetros establecidos por el PIDCP. Sin embargo, la característica del término como un significante vacío puede brindar asimismo oportunidades para que diversos agentes se reúnan y debatan sobre cuestiones que pueden resultar difíciles de abordar de otro modo. Puede que la tendencia al debate de los asuntos planteados por la incitación al odio en Internet se generalice dada la creciente relevancia del fenómeno.

5.2 JURISDICCIÓN

- Gran parte de la atención dirigida a la identificación y la respuesta a la incitación al odio en línea se ha concentrado en las administraciones públicas. Sin embargo, existe en la actualidad una clara tendencia a que los intermediarios de Internet, los servicios que median en la comunicación en línea, desempeñen un papel cada vez más importante en las tareas tanto de autorización, como de restricción de la expresión. Muchos de ellos, y en especial los motores de búsqueda y las plataformas de redes sociales, actúan en varios países y regulan las interacciones de los usuarios con arreglo a sus propias definiciones de incitación al odio, con una relación poco clara con la legislación internacional en materia de derechos humanos. Se sirven en gran medida de las notificaciones de los usuarios respecto a los contenidos considerados inapropiados, y cuando un caso se somete a su atención, la respuesta por defecto consiste en decidir al respecto con arreglo a sus propias condiciones de servicio. En cualquier caso, las condiciones en las que actúan los intermediarios de Internet, en lo que se refiere al modo en que se relacionan con las normas y reglamentos nacionales e internacionales, los grupos de presiones y los usuarios individuales, cambian de manera constante.

- Las propias empresas y muchos agentes de la sociedad civil parecen sentirse especialmente incómodos cuando se obliga a instituciones privadas a actuar como tribunales y decidir lo que debe o no se debe ofrecer en Internet. Actualmente se debate la medida en que tales tribunales pueden diferir de la autorregulación voluntaria, con arreglo a la cual, las empresas ofrecen sus propios canales para los usuarios individuales que formulan las reclamaciones, aún cuando estos mantienen el derecho a resolver un determinado asunto ante los juzgados nacionales si su demanda no se atiende en primera instancia. No obstante, esta nueva territorialización jurídica de los espacios en línea puede dar lugar a una progresiva fragmentación de Internet, en la que determinados estados o grupos de estados impongan sus propias normas, socavando el potencial de la Red para compartir la expresión más allá de las fronteras y acercar a los pueblos. Tal proceso crea un escenario en el que Internet se experimenta de manera muy diferente en distintas ubicaciones, y en el que la norma del libre flujo queda eclipsada por las excepciones nacionales o regionales. El equilibrio de la prioridad entre las normas comunes y las diferencias nacionales cambiaría.

- La mayoría de los intermediarios de Internet aplican cada vez más un enfoque basado en el uso. Facebook, por ejemplo, ha activado una función de “denuncia social” que brinda a los usuarios una vía para enviar un mensaje a las personas que publican información que al usuario no le gusta, pero que no infringe las condiciones de servicio de la empresa. Otra opción, aunque dista de convertirse en tendencia (si bien es una función que ofrece Facebook) consiste en un servicio de notificación sucesiva (“*notice and notice*”) en virtud del cual, un usuario, a través del intermediario, puede instar a otra parte a retirar una determinada expresión. En ocasiones, las plataformas de redes sociales han modificado o mejorado los mecanismos de seguimiento y moderación

de contenidos. Este enfoque ha comprendido cierto grado de cooperación con las administraciones públicas, pero, en estos casos, la informalidad podría servir para reducir la asunción de responsabilidades y la transparencia, tanto para los estados, como para las empresas privadas. Aunque la informalidad en algunas situaciones responde bien a la naturaleza fluida de la incitación al odio en línea, adolece de la desventaja de constituir una solución ad hoc y poco sistemática. En algunos casos, puede ser la capacidad particular de un grupo de presión para "dar con la tecla" y marcar la diferencia, no la importancia ni la validez de un caso específico per se, o si el asunto en cuestión de incitación al odio percibida excede en realidad de lo legítimo en cuanto a expresión.

- La tendencia a que la acción de los intermediarios repercuta en los casos de incitación al odio continuará, aunque bajo la influencia creciente de los grupos de la sociedad civil (nacionales y transnacionales) de determinadas administraciones públicas.

5.3 COMPRENSIÓN

- La naturaleza ofensiva de los mensajes generadores de odio ofrece aparentemente una sólida justificación para su limitación y el acallamiento de sus autores, a través, por ejemplo de su expulsión de una plataforma o, incluso, de prohibirles el uso de Internet. Tales justificaciones, aún cuando puedan resultar desproporcionadas y no superen la prueba de "necesidad" para que la limitación sea legítima, tienden a crecer con fuerza tras el acaecimiento de incidentes dramáticos. En estas ocasiones, las autoridades puede abogar por la adopción de medidas severas para contener el potencial de Internet para propagar el odio y la violencia, aunque los vínculos entre la expresión en línea y la violencia en el mundo real pueda ser tenue. En este contexto, los esfuerzos por identificar y comprender el discurso del odio, no solo con el fin instrumental de contrarrestarlo o eliminarlo, sino también de determinar de qué es expresión, resultan especialmente difíciles. Sin embargo, tales esfuerzos revisten claramente una gran importancia, a pesar de las tendencias a formular respuestas excesivamente apresuradas o reactivas. Se requieren estudios para establecer quiénes actúan en los espacios extremistas en Internet, por qué dicen lo que dicen, y cómo lo interpretan, ya que tal investigación puede proporcionar a menudo resultados contrarios a lo esperable de acuerdo con el sentido común. Tales estudios siguen siendo escasos, pero una mejor comprensión de las dinámicas que pueden dar lugar a ciertos tipos de discurso fundamentaría la formulación de unas respuestas innovadoras no basadas únicamente en la represión. Por ejemplo, ¿existen vínculos entre las desigualdades económicas y el discurso del odio? ¿Cómo aprovechan con éxito algunos la incitación al odio con fines partidistas, y por qué muchas de las víctimas suelen proceder de entornos vulnerables o desfavorecidos? ¿Existen conexiones entre el acceso a la educación y el discurso del odio? Las respuestas a preguntas como estas pueden apuntar a la necesidad de políticas proactivas y prácticas para el fomento de la integración social, y no únicamente a respuestas reactivas para abordar la incitación

al odio entendida como un síntoma de reivindicaciones más profundas. Esta sigue siendo una tendencia ostensiblemente poco desarrollada.

- Una tendencia parcial emergente es la del reconocimiento de que la incitación al odio en Internet engloba un amplio conjunto de fenómenos condicionados parcialmente por sus diferentes plataformas. Las arquitecturas de estas plataformas varían de manera significativa, y repercuten notablemente en el modo en que el discurso del odio se propaga y puede contrarrestarse. Así, una comprensión más precisa de la manera en que cada plataforma puede propiciar o restringir la elaboración y difusión de distintos tipos de mensajes puede constituir un factor importante en la formulación de las respuestas pertinentes.

- Las grandes plataformas de redes sociales han adoptado fundamentalmente un enfoque reactivo respecto al tratamiento de los mensajes de odio denunciados por sus usuarios, y al análisis de si tales mensajes infringen o no sus condiciones de servicio. Sin embargo, dichas plataformas podrían adoptar un enfoque más proactivo. Disponen de acceso a un enorme volumen de datos que puede analizarse y combinarse con los sucesos de la vida real, lo que permitiría obtener una interpretación más matizada de las dinámicas que caracterizan la incitación al odio en Internet. Ya se recaban y analizan grandes cantidades de datos con fines relacionados con el marketing. Podrían dedicarse esfuerzos similares como parte del mandato de responsabilidad social de las empresas propietarias de estas plataformas, contribuyendo así a la generación de conocimiento que puede ser compartido con muy diversos interlocutores. La presión ejercida por distintas partes interesadas externas podría estimular una tendencia a una mayor transparencia y puesta en común de los datos.

- Diversas iniciativas de fomento de la alfabetización mediática e informacional en distintas áreas han comenzado a aparecer como respuesta de índole más estructural a la incitación al odio en Internet. Dada la creciente exposición de los jóvenes a las redes sociales, la información sobre el modo de identificar el discurso del odio y de reaccionar a este reviste cada vez más importancia. Aunque algunos centros docentes han expresado su interés en incorporar progresivamente la alfabetización mediática e informacional a sus planes de estudios, estas iniciativas siguen siendo poco uniformes y, a menudo, no alcanzan a los más vulnerables, que son los que más necesitan ser advertidos del riesgo de la incitación al odio en Internet (y fuera de línea), y del modo de contrarrestarlo. Reviste especial importancia que se incorporen módulos sobre la lucha contra la incitación al odio en aquellos países donde se dan los niveles más altos de riesgo real de violencia generalizada. También es necesario incluir en tales programas unos módulos para la reflexión sobre la identidad, de manera que los jóvenes puedan reconocer los intentos de manipular sus emociones a favor del odio, y se les capacite para defender su derecho individual a ser los dueños de su propia identidad y destino. Iniciativas preferenciales y preventivas como estas han de acompañarse además de medidas para evaluar su repercusión en la conducta efectiva de los estudiantes en Internet y fuera de línea, y en la capacidad de estos para identificar y responder a los mensajes de incitación al odio. Es primordial en la tarea de contrarrestar el discurso del odio en Internet que la adopción de la MIL, sobre todo

por parte de las autoridades nacionales de educación, se convierta en una tendencia generalizada en los próximos años.

5.4 RECAPITULACIÓN

- Es probable que la definición detallada de la incitación al odio en Internet a escala internacional seguirá sin ser objeto de un consenso observado universalmente durante algún tiempo. No obstante, no cabe duda de la aparición de diversos compromisos al respecto.

- El problema de la incitación al odio en línea requiere soluciones colectivas. Como se ha indicado en el presente estudio, existen elementos específicos del asunto del discurso del odio en Internet que probablemente conviertan a las respuestas en las que solo se cuenta con un agente, o con un número limitado de agentes, en opciones altamente ineficaces. Ningún agente o respuesta por sí solo puede resolver el problema de la incitación al odio en la Red.

- Internet se extiende más allá de fronteras, y problemas complejos como el discurso del odio en línea no pueden abordarse de manera sencilla limitándose a confiar en el poder del Estado. Por ejemplo, identificar y procesar a todos los que publican mensajes de odio resultaría irrealizable para la mayoría de los Estados.

- Como propone la Relatora Especial de la ONU sobre cuestiones relativas a las minorías, los Estados podrían colaborar con las organizaciones y los proyectos que conducen campañas de lucha contra la incitación al odio, también en la Red, incluida la provisión de ayuda financiera.

- Los intermediarios de Internet, por su parte, están interesados en mantener una independencia relativa y una imagen “limpia”. Han procurado la consecución de este objetivo demostrando su capacidad de respuesta a las presiones ejercidas por grupos de la sociedad civil, particulares y administraciones públicas. Estas negociaciones han sido *ad hoc* hasta la fecha y, sin embargo, no han dado lugar al desarrollo de principios generales colectivos conformes con la legislación internacional sobre derechos humanos.

- Como han sugerido algunos de los entrevistados para el presente estudio, muchos usuarios parecen haberse insensibilizado ante la incidencia y la presencia del discurso del odio en Internet. Se requieren más iniciativas estructurales para explicar no solo cómo pueden denunciarse ciertos casos, sino también por qué este factor es importante en la creación de espacios compartidos en los que pueda entablarse un diálogo sobre la incitación al odio. Podría consolidarse un espacio intermedio silencioso o pasivo para apartarse de los extremos generadores de odio, procurando que los activistas aborden la expresión del odio en Internet mediante otros discursos que la contrarresten.

IV. PROTECCIÓN DE LAS FUENTES PERIODÍSTICAS EN LA ERA DIGITAL[5]

5 Este capítulo se basa en Posetti, J. (de próxima publicación) *Protecting Journalism Sources in the Digital Age* (Protección de las fuentes periodísticas en la era digital) París: UNESCO

1. INTRODUCCIÓN

A escala internacional, las leyes sobre protección de las fuentes corren cada vez más un riesgo de erosión, restricción y puesta en peligro en la era digital. Esta tendencia supone un reto directo para los derechos humanos universales consolidados de libertad de expresión y respeto de la privacidad, así como para su pertinencia respecto a la libertad de prensa y el papel del periodismo independiente. Al evaluar dicha tendencia, es importante comenzar por desentrañar los principios y los argumentos asociados a la protección de las fuentes periodísticas.

Los periodistas se acogen a la protección de las fuentes, consagrada desde el punto de vista ético y legal, para recabar y revelar información sirviendo el interés público. En estos casos, las fuentes pueden exigir confidencialidad para protegerse de represalias físicas, económicas o profesionales en respuesta a sus revelaciones. El uso de fuentes confidenciales no está reñido con la práctica periodística profesional que conlleva el recurso a múltiples fuentes, la verificación y la corroboración, todas ellas de suma importancia para la credibilidad cuando se emplean tales fuentes. No obstante, sin dichas fuentes, es posible que muchos reportajes de investigación nunca hubieran salido a la luz. A menudo, incluso los artículos que conllevan la recogida de opiniones en la calle, o una sesión informativa, se basan en la confianza de que el periodista respetará la confidencialidad cuando esta se requiera.

Todos estos factores explican por qué existe una sólida tradición jurídica de protección de las fuentes en el ámbito internacional, en reconocimiento de la función vital que desempeñan las fuentes confidenciales en la tarea de facilitar el periodismo “vigilante” o de “exigencia de responsabilidades”. También explican por qué se aplica a los periodistas una obligación ética establecida a escala mundial de evitar revelar la identidad de sus fuentes confidenciales. Aunque el profesionalismo periodístico excluye la incitación o el consentimiento de la infracción de la ley, que puede adoptar la forma de una filtración no sancionada, los periodistas tienen el deber de considerar la importancia para el interés general de publicar la información resultante. En este proceso, mantener la confidencialidad es una manera de no poner en peligro el flujo de tal información capaz de contribuir de forma relevante a la lucha contra la corrupción y las infracciones de los derechos humanos.

No obstante, en muchos casos, la situación jurídica no contempla el reconocimiento de tal confidencialidad, y los periodistas pueden ser obligados aún legalmente a identificar sus fuentes, o se enfrentan si no a sanciones, enjuiciamiento y penas de prisión. Las excepciones a la protección jurídica podrían incluir circunstancias que conlleven serias amenazas a la vida humana, cuando un periodista es acusado de cometer un delito, o si es testigo de un delito grave. Dónde se traza el límite legal, y cómo se interpreta este, son factores que varían en todo el mundo, pero el principio que establece la confidencialidad como norma, y la revelación como excepción, es el estándar aceptado comúnmente.

El valor de proteger la confidencialidad de las fuentes para la sociedad es ampliamente reconocido, al compensar con mucho los casos poco habituales de periodistas que abusan de la confidencialidad, como, por ejemplo, al inventar fuentes o al abstenerse de verificar la información antes de su publicación. Tales abusos salen a la luz invariablemente, y son objeto de una firme condena por parte de las organizaciones profesionales de periodistas, que subrayan el requisito de servirse de fuentes anónimas únicamente cuando resulte necesario para proteger la fuente de la exposición, en el curso de la actividad periodística ejercida para atender el interés público. En este sentido, en los estándares en materia de libertad de expresión se apoya a escala internacional el principio de confidencialidad, que protege directamente al periodista al reconocer su obligación profesional de no revelar la identidad de las fuentes, e indirectamente a la fuente a través del compromiso del periodista. Con todo, este principio funciona en la práctica únicamente si la identidad de la fuente confidencial no puede descubrirse con facilidad por otros medios, y cuando existen límites jurídicos al uso de esta información si el anonimato se pone en peligro. La necesidad de proteger la confidencialidad de las fuentes se justifica en distintos instrumentos internacionales y nacionales (véanse los apartados 4 y 5 más adelante) en gran medida en cuanto que garantiza un flujo libre de información, sobre todo en lo que se refiere a la proporcionada por informantes. Sin tal protección, es probable que se dé un “efecto de inhibición”, y que los poseedores de información sensible se muestren reacios a facilitarla. Otro efecto en cadena es el que se produce cuando determinados medios de comunicación o personas particulares que ejercen el periodismo saben o sospechan que se les pondrá bajo presión para que revelen las fuentes, y puede que se reduzca su disposición a buscar o utilizar ulteriormente la información suministrada bajo condiciones de confidencialidad, con la consiguiente contracción de los contenidos de interés público como resultado.

La expansión de los medios digitales de comunicación y seguimiento, que coincide con un aumento de la sensibilidad respecto a los asuntos de seguridad en numerosos países, plantea dificultades concretas a los mecanismos tradicionales de protección jurídica de las fuentes de los periodistas. El compromiso de un informador para rechazar los intentos de obligarle a identificar sus fuentes en el pasado analógico proporcionó seguramente una protección significativa a las fuentes anónimas, pero en la era de la información digital, la vigilancia masiva, la conservación obligatoria de los datos, y la revelación por parte de intermediarios terceros, este régimen tradicional de protección de la identidad puede burlarse.

Los avances tecnológicos y un cambio en los métodos operativos de los servicios policiales y de inteligencia redefinen actualmente el carácter de la privacidad, y de la clasificación jurídica de la protección de las fuentes periodísticas. Ayudados por el progreso tecnológico, los cuerpos policiales y de seguridad nacionales han modificado su práctica, y han pasado de un proceso de detección de los delitos ya cometidos, a otro de prevención de las amenazas. En la era digital, no es el acto de cometer (o la sospecha de que se ha cometido) un delito lo que puede llevar a un periodista o a una fuente a ser objeto de vigilancia, sino el simple acto de utilizar la tecnología de los móviles, el correo electrónico, las redes sociales e Internet. Como resultado, las comunicaciones

periodísticas se ven cada vez más atrapadas en las redes de los cuerpos policiales y de seguridad nacionales. A esto hay que añadir los casos en los que las comunicaciones de determinados periodistas y fuentes pueden seleccionarse expresamente para someterse a una vigilancia orientada a ciertos objetivos. En un informe de 2014 a cargo de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos se señala: "La falta de una legislación nacional adecuada, así como de una apropiada ejecución de la misma, unas salvaguardas procesales débiles, y una supervisión inefectiva". Tales deficiencias revisten especial importancia para la privacidad profesional de la labor periodística, incluidas las comunicaciones digitales de los periodistas con sus fuentes.

Paralelamente a estos acontecimientos, en la pasada década se ha asistido de manera creciente a la adopción de leyes restrictivas en materia de lucha contra el terrorismo y seguridad nacional, restringiendo posiblemente las protecciones jurídicas existentes, incluidas las "leyes de secreto profesional". Estas conllevan medidas de ampliación del alcance de la información "clasificada", y de reducción de las excepciones que permitirían la cobertura para servir el interés público, así como de penalización de toda revelación (en algunos casos, incluida también la publicación por periodistas) de la información clasificada como secreta, sin que existan disposiciones relativas a las excepciones asociadas al interés público. Estas tendencias en cuanto a seguridad, junto con el seguimiento digital, pueden afectar tanto a los periodistas, como a sus fuentes, y restringir, o "inhibir" el periodismo de interés público, y en especial el de investigación que se sirve de fuentes confidenciales. En esta compleja situación, se evoluciona en lo que atañe al derecho a la privacidad en la era digital.

En este contexto digital y de preocupación por la seguridad, se debate sobre qué agentes periodísticos cumplen las condiciones para obtener la protección de sus fuentes, lo que eleva la necesidad de definir de manera inclusiva términos como "periodismo" y "periodistas" en referencia a cuestiones como "¿quién puede reclamar el derecho a unas leyes sobre protección de las fuentes?" Otro asunto es el de la extensión de las leyes de secreto profesional a todos los actos de periodismo, incluidos los procesos de información digital y las comunicaciones periodísticas con las fuentes, y no solo a los que se producen justo después de la publicación de los contenidos basados en tales comunicaciones.

2. METODOLOGÍA

En este capítulo se presenta un análisis cuantitativo y cualitativo de los datos en todo el mundo en relación con la protección de las fuentes periodísticas en la era digital. El estudio lo llevó a cabo WAN-IFRA, la asociación mundial de editores de noticias que alberga al Foro Mundial de Editores de Noticias (WEF por sus siglas en inglés), y una versión más completa se ha publicado paralelamente al presente informe.

2.1 ESTRUCTURACIÓN DEL ESTUDIO

Los investigadores aplicaron un proceso de "datificación" a un informe de 2007 de David Banisar encargado por Privacy International y titulado *Silencing Sources: An International Survey of Protections and Threats to Journalists' Sources*. (Silenciamiento de las fuentes: Un estudio internacional de las protecciones y las amenazas que atañen a las fuentes periodísticas). Tal proceso exigió la extracción manual de datos y la búsqueda de términos clave en el documento, con el fin de a) identificar a todos los países mencionados en el informe, y b) establecer qué países requirieron una investigación adicional para reforzar los datos disponibles, posibilitando así la realización de un cotejo sólido del estudio de 2007. El resultado consistió en el desarrollo de una base de datos en la que se refería cada uno de los países identificados en el informe de 2007, junto con los distintos tipos de protecciones jurídicas aplicables en todo el mundo.

Se identificaron 124 territorios mediante la "datificación" del informe de *Privacy International*, pero la limitación del estudio a los Estados Miembros de la UNESCO redujo la cifra de países seleccionados para su examen a 121. Este subconjunto de países (véase el anexo 3) constituye el objeto de la investigación que se presenta aquí.

2.2 EXAMEN DEL ENTORNO

Una vez se estableció el conjunto de datos inicial, a cada país se le asignó un investigador, o un auxiliar de investigación, con arreglo a la capacidad lingüística, para llevar a cabo un ejercicio de ordenación cualitativa, conocido como examen del entorno. El proceso de puesta en marcha de dicho examen exigió:

a) la preparación de una revisión bibliográfica (centrada en obras especializadas, boletines e informes relevantes),
b) búsquedas en Internet de bases de datos jurídicas, legislativas y de ONG pertinentes en cada país,
c) búsquedas en Internet de sitios web de noticias,

d) la puesta en contacto con las organizaciones miembro y asociadas de WAN-IFRA para recabar su aportación,

e) la puesta en contacto con diversas fuentes en los países.

La recogida de datos comenzó el 1 de agosto de 2014 y finalizó el 20 de julio de 2015.

2.3 ANÁLISIS DE LOS DATOS DE LOS PAÍSES

Una vez estudiado cada país, se determina un subconjunto de países cuyos cambios se hayan identificado desde 2008 hasta mediados de 2015. Por último, en 84 de los 121 países (69%) estudiados se registraron cambios relativos a las protecciones jurídicas de las fuentes periodísticas.

2.4 ENCUESTAS

Se diseñó un conjunto de preguntas para encuestas en línea, con el fin de contar con la participación de miembros de las comunidades periodística, académica, jurídica, de Internet, y de interlocutores interesados en la libertad de expresión de todo el mundo. En concreto se les pidió que: señalaran los cambios del entorno jurídico y regulador relativos a la protección de las fuentes desde 2007; que identificaran a expertos/agentes destacados para futuras entrevistas cualitativas; y que sugirieran posibles estudios de caso. Esta encuesta se puso en marcha en octubre de 2014, y continuó hasta enero de 2015.

Los resultados pertinentes de una encuesta en línea anterior, iniciada con ocasión del Foro Mundial de Editores de Noticias celebrado en Turín, Italia, en junio de 2014, se sintetizaron con los datos de la encuesta distribuida en relación con este estudio encargado por la UNESCO. Se recabaron datos que acreditaran la repercusión de las revelaciones sobre vigilancia realizadas por Edward Snowden en las salas de redacción de todo el mundo, en cuanto a los cambios en la formación y en la práctica en referencia a la protección de las fuentes, junto con información sobre otros asuntos de seguridad digital más generales. Por otro lado, se examinaron los datos pertinentes de la encuesta del Estudio general sobre Internet de la UNESCO en respuesta a la pregunta: “¿en qué medida protegen las leyes al periodismo de interfaz digital y a las fuentes periodísticas?”

Un total de 134 personas de 35 países, representando a todas las regiones de la UNESCO, respondieron a las encuestas combinadas. Los datos de la encuesta se examinaron para obtener pruebas de los cambios de los marcos jurídicos de protección de las fuentes, así como de diversas dimensiones digitales. Este ejercicio se utilizó para reforzar los resúmenes regionales que se presentan más adelante, y facilitar la identificación de los agentes expertos, y el desarrollo de los estudios temáticos.

2.5 ENTREVISTAS CUALITATIVAS

Se identificó a docenas de agentes clave con conocimientos técnicos especializados en materia jurídica, periodística y de libertad de expresión, a través de los procesos del examen del entorno y de encuesta. En última instancia, se seleccionó a 49 entrevistados de 22 países según su capacitación especializada pertinente, y con el fin de lograr un equilibrio regional y entre los dos géneros.

2.6 DEBATES DE EXPERTOS

Se celebraron dos debates de expertos relacionados con la investigación durante la fase final del estudio. El primero de ellos tuvo lugar en Washington, DC durante el Foro Mundial de Editores de Noticias en junio de 2015. La Asociación de la Prensa Extranjera de Londres y el Frontline Club de dicha ciudad albergaron conjuntamente el segundo debate, convocado en julio de 2015. Las aportaciones de los expertos en las dos sesiones se aprovecharon para actualizar y reforzar el análisis del estudio.

2.7 ESTUDIO TEMÁTICO

Se identificaron numerosos estudios de caso posibles en los procesos de examen de entorno y de encuesta. Se seleccionaron tres estudios temáticos para un análisis exhaustivo capaz de garantizar la inclusión de las cuestiones más destacadas y la reflexión sobre la diversidad regional y lingüística. El tercero, relativo a ***una herramienta modelo de evaluación para los marcos jurídicos internacionales de protección de las fuentes***, se presenta aquí. En este estudio temático se refiere el desarrollo de una herramienta de evaluación de 11 puntos para calibrar la eficacia de los marcos jurídicos de protección de las fuentes en la era digital, llevado a cabo sobre la base de unas extensas entrevistas cualitativas con expertos internacionales.

3. PRINCIPALES RESULTADOS Y RECOMENDACIONES

1. En 84 Estados Miembros de la UNESCO de los 121 estudiados (69%) para este informe se observaron cambios reseñables, fundamentalmente con un efecto negativo, respecto a la protección de las fuentes periodísticas entre 2007 y mediados de 2015.

2. La cuestión de la protección de las fuentes se cruza con otras como las de la vigilancia masiva y dirigida a objetivos concretos, la conservación de datos, los efectos indirectos de la legislación sobre la lucha contra el terrorismo y la seguridad nacional, y el papel de las empresas de Internet terceras conocidas como "intermediarios".

3. La protección jurídica y normativa de las fuentes periodísticas corre un riesgo creciente de erosión, restricción y puesta en peligro.

4. Sin un refuerzo sustancial de las protecciones jurídicas y las limitaciones a la vigilancia y la conservación de datos, el periodismo de investigación que se sirve de fuentes confidenciales será difícil de sostener en la era digital, y la actividad periodística en muchos otros casos se encontrará con la inhibición de posibles fuentes.

5. La transparencia y la asunción de responsabilidades respecto a la vigilancia masiva y selectiva, y la conservación de datos, son factores de una enorme importancia si se pretende que las fuentes confidenciales puedan seguir entrando en contacto con los periodistas en condiciones de seguridad.

6. Los distintos Estados afrontan una necesidad de adoptar o actualizar leyes de protección de las fuentes.

7. Se recomienda definir "actos de periodismo" de manera diferenciada a la función del "periodista", a la hora de determinar quién puede beneficiarse de dichas leyes.

8. Para optimizar los beneficios, la legislación sobre protección de las fuentes debe reforzarse conjuntamente con la protección jurídica extendida a los informantes, que constituyen un conjunto significativo de las fuentes periodísticas confidenciales.

9. Las leyes referidas han de cubrir los procesos periodísticos y las comunicaciones con las fuentes confidenciales (incluidas las llamadas telefónicas, las redes sociales, y los mensajes de correo electrónico), así como el periodismo publicado que depende de fuentes de esa misma índole.

10. Los periodistas adaptan cada vez más su práctica en un esfuerzo por proteger parcialmente a sus fuentes de la exposición, pero las amenazas al anonimato y al cifrado menoscaban tales adaptaciones.

11. El coste financiero de la amenaza que pesa sobre la protección de las fuentes en la era digital es muy significativo (por lo que se refiere a las herramientas de seguridad digital, la formación, y el asesoramiento jurídico), al igual que su repercusión en la producción y el alcance del periodismo de investigación basado en fuentes confidenciales.

12. Es necesario formar a los periodistas y a diversos agentes de la sociedad civil en seguridad digital.

13. Es posible que los periodistas y otros agentes que se sirven de fuentes confidenciales para informar atendiendo el interés público tengan que impartir formación a sus fuentes sobre métodos seguros de contacto y puesta en común de información.

4. IDENTIFICACIÓN DE TEMAS ESENCIALES

Los datos recabados para este estudio confirmaron la existencia de cuatro tendencias clave interrelacionadas, que se solapan y afectan a la protección jurídica de las fuentes periodísticas en la era digital.

Los temas esenciales de dicha era que se deducen de la investigación emprendida para este capítulo ponen de relieve pautas que se reflejan a escala mundial: 1. las leyes de protección de las fuentes corren el riesgo de verse sobrepasadas por la legislación sobre seguridad nacional y lucha contra el terrorismo que, cada vez más, amplía las definiciones de "información clasificada" y limita las excepciones respecto a los actos periodísticos; 2. el uso generalizado de la vigilancia masiva y selectiva de periodistas y de sus fuentes socava los marcos jurídicos de protección de las fuentes al interceptar las comunicaciones periodísticas antes de la publicación; 3. la ampliación de los requisitos aplicados a los intermediarios terceros para que conserven obligatoriamente los datos de los ciudadanos durante plazos cada vez más prolongados eleva el grado de exposición de las comunicaciones periodísticas con las fuentes confidenciales; 4. los debates sobre el derecho de los agentes de los medios digitales al acceso a las leyes de protección de las fuentes allí donde existen estas se intensifica en todo el mundo. En estos temas se basa el catálogo regional de cambios que afectan a los marcos jurídicos de protección de las fuentes (incluidos cambios legislativos, precedentes judiciales, incidentes y revelaciones) que siguen.

5. ENTORNOS REGLAMENTARIOS Y NORMATIVOS INTERNACIONALES

La protección de las fuentes en los instrumentos internacionales esbozados más adelante se percibe como necesaria para garantizar el libre flujo de información, un elemento esencial de varios convenios internacionales sobre derechos humanos. Se adopta el supuesto de que se requieren "circunstancias excepcionales" para justificar la revelación de las fuentes confidenciales de los periodistas. En este sentido, la necesidad de la información sobre la fuente debe considerarse esencial, y únicamente en casos en los que exista un "interés vital" puede justificarse tal revelación.

5.1 AGENTES DE LAS NACIONES UNIDAS

5.1.1 Resoluciones

2012: Resolución del Consejo de Derechos Humanos (A/HRC/RES/21/12) sobre la seguridad de los periodistas, aprobada en septiembre de 2012.

2012: Resolución adoptada por el Consejo de Derechos Humanos de la ONU (UN Doc. A/HRC/RES/20/8) sobre la promoción, protección y disfrute de los derechos humanos en Internet, que reconoce la necesidad de defender los derechos de las personas del mismo modo, con independencia del entorno.

En la primera resolución se señala "la necesidad de asegurar mayor protección para todos los profesionales de los medios de información y para las fuentes periodísticas". En la segunda se afirma que "los derechos de las personas también deben estar protegidos en Internet". Además, se apoya de manera relevante la opción de extender las disposiciones jurídicas sobre protección de las fuentes para procesos periodísticos "analógicos" al ámbito digital.

2013: Resolución adoptada por la Asamblea General de la ONU (A/RES/68/163) sobre la seguridad de los periodistas y la cuestión de la impunidad (2013)

En esta resolución se reconoce que "... que el periodismo está en constante evolución y ha llegado a incluir las aportaciones de instituciones del sector de los medios de comunicación, particulares y una serie de organizaciones que buscan, reciben y difunden todo tipo de información e ideas, tanto en línea como en los demás medios de comunicación, en el ejercicio de la libertad de opinión y de expresión, de conformidad con el artículo 19 del Pacto Internacional de Derechos Civiles y Políticos, contribuyendo así a dar forma al debate público". Se reconocen además los cambios en las definiciones de

"periodismo" que atañen a los debates sobre quién tiene derecho a invocar la protección de las fuentes, y se alude al valor del periodismo para el interés público. Se toma nota con aprecio del Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad, en el que se establece que los esfuerzos para acabar con los delitos contra estos profesionales han de cubrir no solo a los periodistas reconocidos formalmente, sino también a los defensores de los derechos humanos, los trabajadores de medios de comunicación locales y a los periodistas ciudadanos.

En noviembre de 2013, la 37ª sesión de la Conferencia General de la UNESCO aprobó una resolución sobre "Cuestiones relacionadas con Internet, con inclusión del acceso a la información y el conocimiento, la libertad de expresión, la privacidad y las dimensiones éticas de la sociedad de la información".

En dicha resolución se reconoce formalmente el valor del periodismo de investigación para la sociedad, y el papel de la privacidad en la tarea de garantizar tal función: "...la privacidad es esencial para proteger las fuentes periodísticas, que permiten a una sociedad disfrutar del periodismo de investigación y fortalecer el buen gobierno y el estado de derecho, y esa privacidad no debe ser objeto de injerencias arbitrarias o ilegales".

En las respuestas a una encuesta adjunta al estudio de la UNESCO sobre cuestiones relacionadas con Internet se señala la importancia de las posiciones de las Naciones Unidas respecto al asunto de la protección de las fuentes periodísticas. En el estudio finalizado, que se fundamentó en la investigación preliminar derivada de este estudio, se propuso (dentro de un paquete de opciones) a los 195 Estados Miembros de la UNESCO que "reconozcan la necesidad de un refuerzo de la protección de la confidencialidad de las fuentes del periodismo en la era digital". El estudio sobre Internet figura en el orden del día de la Conferencia General de la UNESCO de 2015.

En diciembre de 2013, la Asamblea General de las Naciones Unidas (AGNU) aprobó una resolución sobre el derecho a la privacidad en la era digital. (A/C.3/68/167)

Esta resolución fue copatrocinada por 57 Estados Miembros, y en ellas se exhorta a todos los Estados a que "...respeten y protejan el derecho a la privacidad, incluso en el contexto de las comunicaciones digitales. ... Adopten medidas para poner fin a las violaciones de esos derechos y creen las condiciones necesarias para impedirlas, como cerciorarse de que la legislación nacional pertinente se ajuste a sus obligaciones en virtud del derecho internacional de los derechos humanos". En la resolución se expresa "una profunda preocupación... por los efectos negativos que pueden tener para el ejercicio y el goce de los derechos humanos la vigilancia y la interceptación de las comunicaciones, incluidas la vigilancia y la interceptación extraterritoriales de las comunicaciones y la recopilación de datos personales, en particular cuando se llevan a cabo a gran escala".

Exhorta asimismo a todos los Estados a que: "examinen sus procedimientos, prácticas y legislación relativos a la vigilancia y la interceptación de las comunicaciones y la recopilación de datos personales, incluidas la vigilancia, interceptación y recopilación a gran escala, con miras a afianzar el derecho a la privacidad, velando por que se dé cumplimiento pleno y efectivo de todas sus obligaciones en virtud del derecho internacional de los derechos humanos"; y a que "establezcan o mantengan mecanismos nacionales de supervisión independientes y efectivos capaces de asegurar la transparencia, cuando proceda, y la rendición de cuentas por las actividades de vigilancia de las comunicaciones y la interceptación y recopilación de datos personales que realice el Estado"; haciendo hincapié en la necesidad de que los Estados garanticen la ejecución plena y efectiva de sus obligaciones con arreglo al derecho internacional de los derechos humanos.

La Asamblea General solicitó además a la Alta Comisionada de las Naciones Unidas para los Derechos Humanos que presente un informe sobre "la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala". La Asamblea, con arreglo a la resolución del Consejo de Derechos Humanos de 2012 (UN Doc. A/HRC/20/L.13), afirmó asimismo que "los derechos de las personas también deben estar protegidos en Internet, incluido el derecho a la privacidad". Debido a sus llamamientos a proteger el derecho a la privacidad, también en el contexto de las comunicaciones digitales, esta resolución de la AGNU atañe a la protección de las fuentes. El derecho a la privacidad en Internet se aplica asimismo a los periodistas, y puede relacionarse con el trato de estos con fuentes confidenciales. Los informantes (un subconjunto destacado de fuentes periodísticas confidenciales) se comunicarán con mayor probabilidad con los periodistas directamente en línea si estos pueden contar con que su derecho a la privacidad les ayude a proteger sus comunicaciones profesionales.

2014: Resolución adoptada por el Consejo de Derechos Humanos de las Naciones Unidas (A/HRC/RES/27/5) sobre la seguridad de los periodistas

En la resolución se reconoce "la particular vulnerabilidad de los periodistas que se convierten en blanco de la vigilancia o intercepción de comunicaciones cometidas en forma ilegal o arbitraria en violación de sus derechos a la privacidad y la libertad de expresión". Esta observación se aplica directamente a las cuestiones de la protección de las fuentes y de la seguridad de los periodistas y sus fuentes.

Diciembre de 2014: Resolución de la AGNU sobre la seguridad de los periodistas y la cuestión de la impunidad (A/RES/69/185)

En esta resolución de la AGNU se formulan dos observaciones relacionadas con el papel del periodismo en la conformación del debate público y "la particular vulnerabilidad de los periodistas que se convierten en blanco de la vigilancia o intercepción de comunicaciones cometidas en forma ilegal o arbitraria en violación de sus derechos a la privacidad y la libertad de expresión".

5.1.2 Informes, recomendaciones, declaraciones y comentarios

Julio de 2011: Oficina del Pacto Internacional de Derechos Civiles y Políticos, Comité de Derechos Humanos de las Naciones Unidas, Observación General Nº. 34

En esta Observación se reconoce la condición de la libertad de opinión y de expresión como "la piedra angular de todas las sociedades libres y democráticas" que "constituyen la base para el pleno goce de una amplia gama de otros derechos humanos". "La existencia de medios de prensa y otros medios de comunicación libres y exentos de censura y de trabas" se describe como esencial para el ejercicio de la libertad de opinión y expresión. En la Observación se insta a la protección de todas las formas de expresión y los medios para su difusión, incluidos los modos de expresión electrónicos y basados en Internet.

2012: Declaración de Cartago - participantes en la conferencia del Día Mundial de la Libertad de Prensa de la UNESCO:

En esta declaración se hace hincapié en los retos que plantean las comunicaciones en Internet al mantenimiento de la libertad de expresión y los derechos a la privacidad esenciales para el ejercicio del periodismo de investigación.

Junio de 2013: "Informe del Relator Especial (Frank La Rue) para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión" al Consejo de Derechos Humanos

La Rue concluyó que: "Los Estados no pueden garantizar que las personas estén en condiciones de buscar y recibir información ni de expresarse a menos que respeten, protejan y promuevan su derecho a la intimidad". Esta declaración subraya la relación entre los derechos a la libertad de expresión y el acceso a la información y la privacidad que fundamentan la protección de las fuentes.

En julio de 2013, Navi Pillay, Alta Comisionada para los Derechos Humanos en esa fecha, incidió en el derecho a la privacidad en la protección de aquellos que revelan información con implicaciones en materia de derechos humanos.

Haciendo hincapié en el caso de Edward Snowden, Pillay afirmó que los sistemas jurídicos nacionales han de garantizar la disposición de vías para que aquellos que revelen violaciones de los derechos humanos puedan expresar su preocupación sin miedo a las represalias. Esta afirmación atañe a las fuentes confidenciales porque, aunque la protección de la confidencialidad periodística no comprende necesariamente la protección del acto de revelación por parte de la fuente, el miedo a la represalia es un factor que afecta a la confianza de la fuente en el compromiso del periodista de mantener

la confidencialidad. De esta manera, un mayor temor a la represalia puede reforzar el "efecto de inhibición".

Pillay declaró que el derecho a la privacidad, el derecho de acceso a la información y la libertad de expresión se encuentran estrechamente vinculados. También apuntó explícitamente a la necesidad de que las personas "confíen en que sus comunicaciones privadas no se someten al control indebido del Estado". El resultado de la ausencia de tal confianza es un "efecto de inhibición" en las fuentes que podría dar lugar, a su vez, al bloqueo de los "conductos de información". Esta perspectiva también influye en la confidencialidad de las fuentes periodísticas.

Informe (A/HRC/23/40) de 2013 del Relator Especial para la Libertad de Opinión y de Expresión, Frank La Rue:

En el informe se refiere que: "los periodistas deben estar en condiciones de contar con comunicaciones privadas, seguras y anónimas. Un entorno en que la vigilancia está generalizada y no está restringida por las debidas garantías procesales ni la supervisión judicial es incompatible con la protección de las fuentes". La afirmación de La Rue pone de relieve el modo en que la vigilancia puede repercutir en la actividad periodística, y en especial, en la que depende de fuentes confidenciales.

En febrero de 2014, la ONU albergó un seminario sobre el Derecho a la privacidad en la era digital (Ginebra)

En este acto, el Relator La Rue realizó un llamamiento a favor de un mandato especial de las Naciones Unidas para la protección del derecho a la privacidad, y añadió: "la privacidad y la libertad de expresión no solo están vinculadas, sino que también actúan como facilitadores de la participación ciudadana, el derecho a la libertad de prensa, el ejercicio de la libre expresión, y la posibilidad de que determinadas personas se reúnan, ejerzan el derecho a la libre asociación, y puedan criticar las políticas públicas".

Julio de 2014 - Resumen del debate de expertos del Consejo de Derechos Humanos sobre la seguridad de los periodistas: Informe de la OACDH

En el resumen se señala que: "Un problema recurrente que se planteó durante el debate fue si el marco jurídico vigente era suficiente para velar por la seguridad y la protección de los periodistas y los trabajadores de los medios de comunicación. La cuestión se examinó tanto en lo que respecta a la protección física contra las amenazas y la violencia, como a la protección contra la injerencia indebida, también de carácter jurídico o administrativo." Por otra parte, en el resumen se refiere que la aparición de nuevas formas de periodismo (incluidas las redes sociales y los blogs) ha dado lugar a "a una mayor vulnerabilidad de los medios de comunicación, incluida la injerencia ilegal en la vida privada y las actividades de los periodistas. Había que condenar esa injerencia y apoyar la independencia de los medios tradicionales y digitales."

De acuerdo con el resumen, La Rue señaló que la privacidad y el anonimato de los periodistas también constituyen elementos esenciales para garantizar la libertad de prensa. Los ponentes destacaron además que: los autores de blogs, los periodistas en línea y los ciudadanos periodistas desempeñaban un papel importante en la promoción de los derechos humanos... [y] la protección de los periodistas debía abarcar a todos los proveedores de información, tanto profesionales como no profesionales." Esto atañe a la cuestión de la aplicación de la protección jurídica de las fuentes periodísticas. Por último, en la reunión se declaró que las leyes nacionales de seguridad y lucha contra el terrorismo no deben utilizarse para silenciar a los periodistas.

Estas cuestiones tienen que ver con el derecho de los periodistas a recibir y transmitir la información recabada de fuentes confidenciales para servir al interés público, sin injerencias.

Informe de la UNESCO de 2014 sobre las Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios

La amenaza de la vigilancia para el periodismo se subraya en este informe global en el que se hace hincapié en el papel de las leyes nacionales de seguridad y lucha contra el terrorismo y el extremismo como instrumentos utilizados en algunos casos "... para limitar el debate legítimo y acallar las voces disidentes en los medios de comunicación, y avalan una intensificación de la vigilancia, lo cual puede considerarse una violación del derecho a la privacidad y un riesgo para la libertad de expresión". En el informe se añade que "las agencias de seguridad de diversos países han accedido a los documentos, correo electrónico y registros telefónicos de los periodistas, así como a una inmensa colección de datos que podrían permitirles rastrear los movimientos de periodistas, fuentes y soplones".

Julio de 2014: "El derecho a la privacidad en la era digital: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos"

La AGNU encargó este informe sobre la protección y la promoción del derecho a la privacidad en el contexto de la vigilancia y la interceptación de las comunicaciones digitales y la recopilación de datos personales en los planos nacional y extraterritorial, incluso a gran escala. En el informe se determinó que, en la era digital, las tecnologías de las comunicaciones han reforzado la capacidad de "los gobiernos, las empresas y los particulares para realizar actividades de vigilancia, interceptación y recopilación de datos".

También se destacaron en el informe los riesgos de los grandes conjuntos de datos para la reidentificación de los datos "anónimos". La cuestión de la recogida de metadatos (p. ej., los datos que indican patrones de conducta, como el número de llamadas entre dos personas, y los horarios de las mismas, en lugar de su contenido) también influye en gran medida en la protección de las fuentes. En este sentido, el efecto inhibidor en

las fuentes confidenciales, dado el riesgo de caracterización y exposición planteado por la combinación de la conservación de los datos y las consecuencias del análisis de los grandes conjunto de datos, se exacerba.

En el informe también se asegura que "incumbe al gobierno demostrar que la injerencia es necesaria y proporcional al riesgo concreto de que se trate. Así pues, los programas de vigilancia en masa o "a granel" pueden considerarse arbitrarios, aunque persigan un objetivo legítimo y hayan sido aprobados sobre la base de un régimen jurídico accesible". Se concluye que las administraciones públicas se sirven cada vez más de agentes del sector privado para conservar los datos (a menudo, en el contexto de la legislación sobre la conservación de datos obligatoria que constituye un rasgo común de los programas de vigilancia), "por si acaso". Se refiere además que tales medidas no son ni "necesarias" ni "proporcionales".

Citando una sentencia del Tribunal Europeo de Derechos Humanos, en el informe se declara que incumbe al Estado garantizar que toda injerencia en el derecho a la privacidad, la familia, el hogar o la correspondencia sea autorizada por leyes que "sean suficientemente precisas". Se observa además la práctica de los Estados que comparten su información de inteligencia y sobrepasan los límites a la vigilancia de sus propios ciudadanos. Estas actuaciones traen consecuencias evidentes para los periodistas, sobre todo para los corresponsales extranjeros y aquéllos que llevan a cabo investigaciones internacionales.

También se alude al papel de los intermediarios terceros en este informe. Se trata de una nueva dimensión relevante que atañe a la protección de las fuentes de los periodistas, ya que se ejercen presiones crecientes sobre los intermediarios terceros que puedan disponer de acceso a las comunicaciones digitales "privadas" de los periodistas con las fuentes confidenciales (como motores de búsqueda, PSI, empresas de telecomunicaciones y redes sociales) para que entreguen determinados datos a gobiernos y corporaciones, en el contexto de procedimientos judiciales o con arreglo a planteamientos extrajudiciales. Este proceso es objeto de una creciente formalización: a medida que la prestación de servicios de telecomunicaciones pasa del sector público al sector privado, se ha producido, según se refiere en el informe, una "delegación de las responsabilidades policiales y cuasijudiciales a los intermediarios de Internet... La promulgación de leyes que obligan a las empresas a preparar sus redes para la interceptación es motivo de especial preocupación, en particular porque crea un ambiente que facilita las medidas de vigilancia exhaustiva". En el informe se añade que "Gobiernos de todos los continentes han utilizado tanto mecanismos legales formales como métodos encubiertos para tener acceso a los contenidos, así como a los metadatos".

Noviembre de 2014: resolución del Consejo del Programa Internacional para el Desarrollo de la Comunicación (PIDC) de la UNESCO

En 2014, el consejo de 39 Estados miembros del PIDCE acogió favorablemente el Informe sobre la seguridad de los periodistas y el peligro de la impunidad, en el que se utiliza el término "periodistas" para designar el conjunto de "periodistas, trabajadores de los medios de comunicación y productores de las redes sociales que generan un

significativo volumen de actividad periodística de interés público". El Consejo reafirmó además la importancia de las condenas de "el asesinato de periodistas, productores y trabajadores en medios y redes sociales que desarrollaban actividades periodísticas y fueron asesinados o fijados como objetivo en el ejercicio de su labor profesional".

> ***Mayo de 2015: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos sobre el cifrado, el anonimato y el marco de derechos humanos, a cargo del Relator Especial de la ONU para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión, David Kaye***

En este informe del nuevo Relator Especial se hace hincapié en las funciones esenciales desempeñadas por el cifrado y el anonimato. Según Kaye, tales defensas, actuando juntas o por separado, generan una zona de privacidad para proteger la opinión del control externo. Señala además la especial importancia del cifrado y el anonimato en entornos hostiles.

Kaye subraya asimismo el valor del anonimato y el cifrado para los periodistas, investigadores, juristas y miembros de la sociedad civil que tratan de proteger sus fuentes confidenciales y sus comunicaciones con estas. Observó que las personas que intentan "buscar, recibir e impartir" información e ideas pueden verse obligadas a servirse del anonimato y del cifrado, sobre todo en los entornos donde la censura se encuentra generalizada. Un asunto afín abordado por Kaye es el de una tendencia a que los Estados traten de combatir las herramientas del anonimato, como Tor, los proxies o las VPN, mediante la denegación del acceso a las mismas. Es evidente que tales medidas pueden socavar de manera indirecta los intentos de proteger legalmente las fuentes periodísticas confidenciales en el contexto de las comunicaciones digitales.

Kaye reconoció además que muchos Estados admiten la legalidad de mantener el anonimato de las fuentes periodísticas. Sin embargo, señaló que: "los Estados infringen a menudo el anonimato de las fuentes en la práctica, incluso cuando se dispone en la legislación", incidiendo en las presiones sobre los periodistas que minan tales disposiciones legales, ya sea de manera directa, o progresiva. Otro asunto destacado por el Relator Especial es la creciente generalización y la repercusión del registro obligatorio de las tarjetas SIM en las comunicaciones confidenciales, incluidas las que mantienen los periodistas y sus fuentes. Señaló que más de 50 países de África exigen, o han iniciado el proceso para exigir, el registro de las tarjetas SIM, que conlleva la provisión de datos identificables, y que "tales políticas minan directamente el anonimato... y pueden proporcionar a los Gobiernos la capacidad para el seguimiento de periodistas y otros particulares yendo mucho más allá del interés público legítimo". Kaye concluyó que los Estados deben apoyar y promover unos procesos de cifrado y anonimato consolidados, y recomendó específicamente que se refuercen las disposiciones jurídicas y legislativas con el fin de posibilitar unas comunicaciones seguras para los defensores de los derechos humanos y los periodistas.

6. INSTRUMENTOS REGIONALES DE LAS LEYES Y LOS MARCOS NORMATIVOS EN MATERIA DE DERECHOS HUMANOS

6.1 INSTITUCIONES EUROPEAS

Las organizaciones y órganos legislativos europeos han emprendido iniciativas significativas a escala regional encaminadas a identificar y atenuar los riesgos que plantea la protección de las fuentes en el entorno digital.

6.1.1 Resoluciones, declaraciones, observaciones, recomendaciones, informes y directrices del Consejo de Europa

Septiembre de 2007: adopción de las Directrices del Comité de Ministros del Consejo de Europa sobre la protección de la libertad de expresión e información en épocas de crisis

En estas directrices se recomienda que los Estados miembros del Consejo de Europa (CdE) adopten la Recomendación nº. R (2000)7 sobre el "derecho de los periodistas a no revelar sus fuentes de información" en la legislación y en la práctica.

Los principios que siguen figuran en un anexo a la Recomendación nº. R (2000)7:

- ***Principio 1 (Derecho de los periodistas a la no revelación)***

La ley y la práctica nacionales en los Estados miembros deberán disponer una protección explícita e inequívoca del derecho de los periodistas a no revelar información que identifique a una fuente...

- ***Principio 2 (Derecho de otras personas a la no revelación)***

Otras personas que, por sus relaciones profesionales con periodistas, tengan noticia de una información que identifique a una fuente a través de la recogida, el tratamiento editorial o la difusión de dicha información, deberán ser protegidos igualmente con arreglo a los principios establecidos en la presente Recomendación.

- ***Principio 3 (Límites al derecho a la no revelación)***

a) El derecho de los periodistas a no revelar la información que identifique a una fuente no deberá someterse a otras restricciones ajenas a las previstas en el artículo 10, apartado 2 del Convenio...

b) *La revelación de información que identifique a una fuente no se considerará necesaria salvo pueda establecerse de manera convincente que:*

   i. *las medidas alternativas razonables a la revelación no existen o han sido agotadas por las personas o autoridades públicas que procuren la revelación; y*

   ii. *el interés legítimo en la revelación supere claramente el interés público en la no revelación, siempre que:*

      - *se demuestre la imperiosa necesidad de la revelación,*
      - *las circunstancias sean de una índole suficientemente fundamental y grave,*
      - *se determine que la necesidad de la revelación responde a una necesidad social acuciante, y*
      - *los Estados miembros dispongan de un cierto margen de valoración en la evaluación de tal necesidad, si bien tal margen se someterá a la supervisión del Tribunal Europeo de Derechos Humanos.*

c) *Los requisitos anteriores deberán aplicarse en todas las etapas de los procedimientos en los que pueda invocarse el derecho a la no revelación.*

- ***Principio 4 (Pruebas alternativas a las fuentes de los periodistas)***

En los procedimientos judiciales contra un periodista incoados a causa de una presunta violación del honor o la reputación de una persona, las autoridades deberán considerar, a efectos del establecimiento de la verdad o, en cualquier caso, de la acusación, todas las pruebas a su disposición de conformidad con el derecho procesal nacional, y no podrán exigir a tal efecto la revelación de información que identifique una fuente por parte del periodista.

- ***Principio 5 (Condiciones relativas a la revelación)***

a) *La propuesta o petición formulada por las autoridades competentes para el inicio de actuaciones encaminadas a la revelación de información que identifique a una fuente solo deberán ser emprendidas por personas o autoridades públicas que tengan un interés legítimo directo en tal revelación.*

b) *Los periodistas deberán ser advertidos por las autoridades competentes de su derecho a no revelar información que identifique a una fuente, así como de los límites de tal derecho antes de que se requiera la revelación.*

c) *Las sanciones a periodistas por no revelar la información que identifique a una fuente solo deberán imponerlas las autoridades judiciales en procedimientos judiciales que prevean una audiencia de los periodistas interesados con arreglo a lo dispuesto en el artículo 6 del Convenio.*

d) A los periodistas deberá asistirles el derecho a que la imposición de una sanción por no revelar información que identifique a una fuente sea revisada por otra autoridad judicial.

e) Cuando los periodistas respondan a una petición u orden de revelación de información que identifique a una fuente, las autoridades competentes deberán considerar la aplicación de medidas para limitar el alcance de tal revelación, por ejemplo, excluyendo al público en general de la misma, sin perjuicio de lo dispuesto en el artículo 6 del Convenio, en su caso, y respetando ellas mismas la confidencialidad de tal revelación.

- ***Principio 6 (Intercepción de comunicaciones, vigilancia y registro e incautación judiciales)***

a) Las siguientes medidas no deberán aplicarse si su propósito es eludir el derecho de los periodistas, conforme a los términos de los presentes principios, a no revelar la información que identifique a una fuente:

i. órdenes o acciones de intercepción que atañan a la comunicación o la correspondencia de los periodistas o sus empleadores,

ii. órdenes o acciones de vigilancia que atañan a periodistas, sus contactos o sus empleadores, o

iii. órdenes o acciones de registro o incautación que atañan a instalaciones privadas o empresariales, las pertenencias o la correspondencia de periodistas o sus empleadores, o los datos personales relacionados con su labor profesional.

b) Cuando la información que identifique a una fuente haya sido obtenida por la policía o las autoridades judiciales con arreglo a cualquiera de las acciones anteriores, aunque tal obtención no haya sido el objeto de las mismas, deberán adoptarse medidas para evitar el uso ulterior de dicha información como prueba ante los tribunales, salvo que la revelación esté justificada conforme al principio 3.

- ***Principio 7 (Protección contra la autoinculpación)***

Los principios establecidos en la presente Recomendación no limitarán en modo alguno las leyes nacionales sobre la protección contra la autoinculpación en procedimientos penales, y los periodistas, en la medida en que tales leyes sean aplicables, disfrutarán de tal protección respecto a la revelación de la información que identifique una fuente.

En lo que atañe a la definición de periodista, en la Recomendación se dispone que las leyes deben proteger "a toda persona física o jurídica que se dedique de manera habitual o profesional a la recogida y la difusión de información al público a través de vías de comunicación de masas". En las directrices de 2007 del CdE en las que se hace referencia a la Recomendación R(2000)7 se recomienda asimismo que "los profesionales de los medios de comunicación no sean obligados por las fuerzas del orden público a

entregar la información o los materiales... recabados en el contexto de la cobertura de situaciones de crisis".

2010: Informe sobre la protección de las fuentes periodísticas de la Asamblea Parlamentaria del Consejo de Europa

En el informe se declara que "la protección de las fuentes de información de los periodistas constituye una condición básica para el ejercicio pleno de la profesión periodística, y del derecho de la población a ser informada de los asuntos de interés público". Observando que la protección de las fuentes se infringe a menudo, se hace hincapié en la necesidad de limitar las excepciones a las disposiciones jurídicas al respecto. Se alude además a la aparición de amenazas a la protección de las fuentes periodísticas en la era digital. Por otro lado, se recomienda que "los Estados miembros que no hayan adoptado la legislación que especifique el derecho de los periodistas a no revelar sus fuentes de información procedan a su adopción" de conformidad con la jurisprudencia del Tribunal Europeo de Derechos Humanos y las recomendaciones del Comité de Ministros".

2011: la Comisión de Derechos Humanos del Consejo de Europa publica un documento de consulta sobre la protección de los periodistas frente a la violencia

Este informe a cargo del Comisario para los Derechos Humanos del CdE vincula directamente la protección de las fuentes periodísticas con la seguridad de los periodistas. Hace referencia además a una sentencia del Tribunal Europeo de Derechos Humanos [*Goodwin v. el Reino Unido* (27 de marzo de 1996)] en la que se señala que la "protección de las fuentes periodísticas es una de las condiciones básicas para la libertad de prensa". El Tribunal concluyó en dicho asunto que, en ausencia de "una exigencia imperativa de interés público", una orden de revelación de fuentes "infringiría la garantía de libertad de expresión consagrada en el artículo 10 del Convenio Europeo de Derechos Humanos (CEDH)". Este asunto dio lugar a que el Comité de Ministros del Consejo de Europea adoptara la Recomendación nº. R (2000)7 sobre el derecho de los periodistas a no revelar sus fuentes de información. El CdE reafirmó la necesidad de protección para garantizar que las salvaguardas básicas de las fuentes no se vean menoscabadas por los esfuerzos en materia de seguridad, recordando una declaración (2005) en la que se señalaba que los Estados miembros no deben socavar la protección de las fuentes en nombre de la lucha contra el terrorismo, teniendo en cuenta que "la lucha contra el terrorismo no permite a las autoridades la elusión de este derecho yendo más allá de lo permitido [artículo 10 del CEDH y Recomendación R (2000) 7]".

2011: la Asamblea Parlamentaria del Consejo de Europa adopta la Recomendación 1950 sobre la protección de las fuentes periodísticas.

En esta Recomendación se reafirma el papel esencial de la protección de las fuentes para la función democrática del periodismo. Se reconoce asimismo el "gran número de casos" de violación de la protección de las fuentes en Europa y la importancia de tal protección

para el periodismo de investigación. La Recomendación exige que las excepciones a las leyes de protección de las fuentes se formulen de manera restringida y se atengan a los requisitos del artículo 10 del CEDH para evitar las peticiones generalizadas de las autoridades respecto a la revelación de fuentes. Se apunta asimismo a la importancia de las fuentes confidenciales en el ámbito policial y judicial, y al derecho de los periodistas a no revelarlas. Al problema de la conservación de datos en relación con la protección de las fuentes también se hace referencia en la Recomendación. Se alude además en la Recomendación a la importancia de aplicar los principios de la provisión de información confidencial a intermediarios terceros, que atañen a la amenaza emergente derivada del ejercicio de presiones sobre tales intermediarios para que entreguen determinados datos a autoridades o litigantes, eludiendo así las leyes sobre protección de las fuentes.

Se propuso además que el Comité de Ministros dirigiera un llamamiento a los Estados miembros para que:

- legislen en materia de protección de las fuentes;
- revisen su legislación nacional en materia de vigilancia, lucha contra el terrorismo, conservación de datos, y acceso a registros de telecomunicaciones;
- cooperen con organizaciones de periodistas y para la libertad de los medios de comunicación en la elaboración de directrices dirigidas a los fiscales y funcionarios de policía, y de materiales docentes para los jueces sobre el derecho de los periodistas a no revelar sus fuentes;
- formulen directrices para las autoridades públicas y los proveedores privados de servicios relativas a la protección de la confidencialidad de las fuentes periodísticas en el contexto de la intercepción o la revelación de datos informáticos y de tráfico de redes informáticas.

En la Recomendación se indica asimismo la necesidad de extender la protección de las fuentes a las plataformas de medios no tradicionales, con arreglo a los cambios en la práctica profesional, los modos de publicación y distribución, el papel de las redes sociales, y las audiencias participativas y las fuentes. En cualquier caso, en la Recomendación también se adopta la postura de que los blogueros y los agentes de las redes sociales no son periodistas y, por tanto, no deben contar con la posibilidad de reclamar el acceso a las leyes sobre protección de las fuentes. No obstante, que no se diferencie entre “periodismo” y “periodistas” puede excluir en la práctica a un número significativo de blogueros que ejercen como agentes periodísticos, como es el caso de los blogueros del ámbito académico o jurídico, así como a activistas en organizaciones de defensa de los derechos humanos que utilizan las redes sociales, y al personal dedicado a la docencia del periodismo y sus alumnos.

Las sinergias entre la protección de los informantes y los marcos jurídicos diseñados para proteger a los periodistas de ser obligados a revelar sus fuentes también se reconocen en la Recomendación.

Declaración de 2014 del Comité de Ministros sobre la protección del periodismo y la seguridad de los periodistas y otros agentes de los medios de comunicación, aprobada:

En esta Declaración se señala que la aplicación arbitraria y desproporcionada de las leyes en materia de difamación, seguridad nacional o terrorismo "genera un efecto inhibidor sobre el ejercicio del derecho a impartir información e ideas, y da lugar a la autocensura". Por otra parte, se declara que "el acceso inmediato y libre a la información como norma general y la firme protección de las fuentes periodísticas son esenciales para el ejercicio cabal del periodismo, sobre todo en lo que respecta al de investigación". El Comité afirma asimismo que la vigilancia de periodistas y otros agentes de los medios de comunicación "puede poner en peligro el ejercicio legítimo de la libertad de expresión si se lleva a cabo sin las salvaguardas necesarias, y puede amenazar incluso la seguridad de las personas en cuestión. También puede socavar la protección de las fuentes de los periodistas". El Comité convino además en considerar ulteriores medidas respecto a la armonización de leyes y prácticas en lo que se refiere a la difamación, la lucha contra el terrorismo y la protección de las fuentes de los periodistas con el CEDH

Enero de 2015: Comisión de Asuntos Jurídicos y Derechos Humanos del Consejo de Europa - Informe sobre vigilancia masiva / Resolución y recomendación

En este informe, preparado por el Relator Pieter Omtzigt, sobre el impacto de la vigilancia masiva en los derechos humanos, se abordaron las implicaciones de la protección de fuentes periodísticas en el contexto de la libertad de expresión y el acceso a la información. Omtzigt se refirió a la repercusión del "efecto inhibidor" en las comunicaciones periodísticas con fuentes confidenciales, y las limitaciones consiguientes de la revelación de información para atender el interés público.

Enero de 2015: Resolución y recomendación del Consejo de Europa sobre la vigilancia masiva

El 26 de enero de 2015, la Comisión de Asuntos Jurídicos y Derechos Humanos del Consejo de Europa aprobó por unanimidad una resolución y una recomendación sobre la base del informe referido anteriormente. En la Resolución se señala que la Asamblea Parlamentaria "considera con honda preocupación las prácticas de vigilancia masiva" reveladas por Edward Snowden, que "ponen en peligro derechos humanos fundamentales, incluidos los derechos a la privacidad... y la libertad de información y de expresión". La Asamblea también manifestó su inquietud respecto a la "recogida de enormes cantidades de datos personales por parte de empresas privadas, y el riesgo de que tales datos puedan ser objeto de acceso y utilización con fines ilícitos por agentes estatales y no estatales", así como por "el uso generalizado de leyes secretas, tribunales secretos e interpretaciones secretas de tales leyes, sometido a un escaso control". La Comisión invitó al Consejo de Ministros del CdE a considerar la posibilidad de "dirigir una recomendación a los Estados miembros sobre la tarea de garantizar la protección

de la privacidad en la era digital y la seguridad de Internet, a la luz de las amenazas que plantean las técnicas de vigilancia masiva recién reveladas".

6.1.2 Resoluciones, declaraciones, informes y directrices del Consejo de la Unión Europea

Mayo de 2014: Consejo de la Unión Europea - "Directrices de la UE sobre derechos humanos relativas a la libertad de expresión en Internet y fuera de Internet"

En estas directrices se aconseja lo que sigue: "Los Estados deben proteger por ley el derecho de los periodistas a no revelar sus fuentes con objeto de garantizar que los periodistas puedan informar sobre asuntos de interés público sin que sus fuentes teman represalias", Se añade que la UE "apoyará la adopción de legislación que proporcione protección adecuada para denunciantes y apoyará las reformas para proteger el derecho de los periodistas a no revelar sus fuentes".

6.2 AMÉRICA

En 1997, la Conferencia Hemisférica sobre Libertad de Expresión celebrada en la ciudad de México adoptó la Declaración de Chapultepec. El principio 3 establece que "no podrá obligarse a ningún periodista a revelar sus fuentes de información". En 2000, y sobre la base de la Declaración de Chapultepec, la Comisión Interamericana de Derechos Humanos (CIDH) aprobó la Declaración de Principios sobre Libertad de Expresión, como documento orientativo para interpretar el artículo 13 de la Convención Americana sobre Derechos Humanos. En el artículo 8 de la Declaración se establece que "Todo comunicador social tiene derecho a la reserva de sus fuentes de información, apuntes y archivos personales y profesionales". La utilización del término "comunicador social" guarda relación con el debate sobre "¿quién es periodista?" en referencia a las leyes de secreto profesional.

En 2013, en el informe de la CIDH sobre *Violencia contra periodistas y trabajadores de medios: Estándares interamericanos y prácticas nacionales sobre prevención, protección y procuración de la justicia*, a cargo de la Relatoría Especial para la Libertad de Expresión se define a los periodistas como "aquellos individuos que observan, describen, documentan y analizan acontecimientos, declaraciones, políticas y cualquier propuesta que pueda afectar a la sociedad, con el propósito de sistematizar esa información y reunir hechos, análisis y opiniones para informar a sectores de la sociedad o a esta en su conjunto". En el informe se aclara que esta definición incluye a "a quienes trabajan en medios de información y al personal de apoyo, así como a quienes trabajan en medios de comunicación comunitarios, a los y las "periodistas ciudadanos/as".

6.3 ÁFRICA

El artículo 9 de la Carta Africana de Derechos Humanos se otorga a todas las personas el derecho a recibir información y a expresar y difundir opiniones. La Declaración de principios sobre la libertad de expresión en África, publicada por la Comisión Africana de Derechos Humanos y de los Pueblos en 2002, proporciona directrices detalladas a los Estados miembros de la Unión Africana sobre la protección de las fuentes. Estipula que "los profesionales de los medios de comunicación no serán obligados a revelar las fuentes de información confidenciales, ni otros materiales de los que disponga con fines periodísticos, salvo de conformidad con los siguientes principios":

- *la identidad de la fuente es necesaria para la investigación o el enjuiciamiento de un delito grave, o la defensa de un acusado de un delito penal;*
- *la información u otros datos similares que den lugar al mismo resultado no puede obtenerse de otras fuentes;*
- *el interés público en la revelación supera el daño a la libertad de expresión;*
- *y la revelación ha sido ordenada por un tribunal, tras una vista oral completa.*

6.4 INSTITUCIONES INTERREGIONALES

6.4.1 Organización para la Seguridad y la Cooperación en Europa

El Representante de la OSCE para la Libertad de los Medios de Comunicación publica periódicamente declaraciones y observaciones relativas a las infracciones de los marcos jurídicos de protección de las fuentes, y a las amenazas a estos. La Recomendación de Vilnius de junio de 2011 sobre seguridad de los periodistas incluye la recomendación de "animar a los legisladores a reforzar la seguridad de las condiciones de trabajo de los periodistas, creando una legislación que promueva las libertades de los medios de comunicación, incluidas las garantías del libre acceso a la información, la protección de las fuentes confidenciales, y la despenalización de las actividades periodísticas".

6.4.2 La Organización de Cooperación y Desarrollo Económicos

Informe de marzo de 2014: 'The CleanGovBiz Toolkit for Integrity' (Las herramientas CleanGovBiz para la integridad)

En este informe se plantean las siguientes preguntas: "¿se les garantiza a los periodistas que se mantendrá la confidencialidad de sus fuentes de información? En caso afirmativo, ¿cómo se les garantiza?". Se reconoce además la importancia del anonimato de las

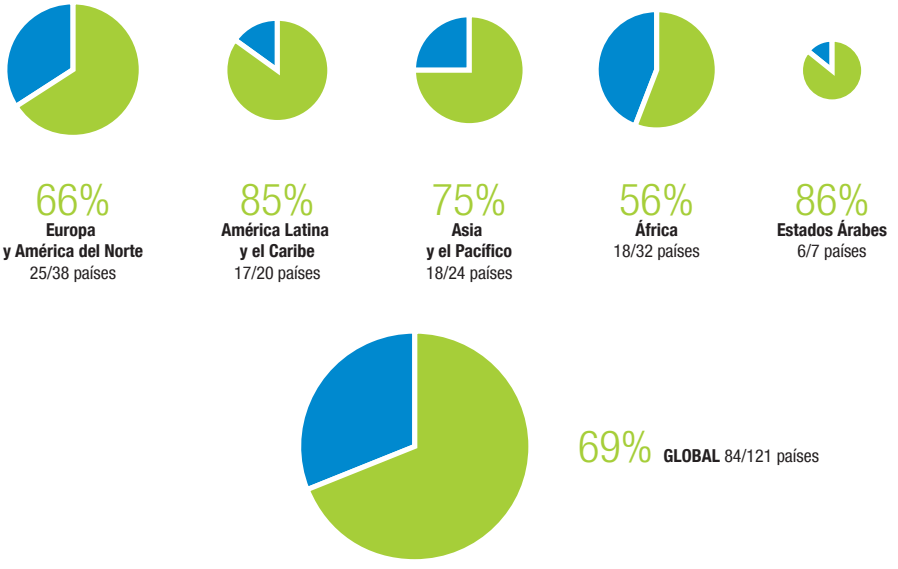
fuentes ya que “puede resultar peligroso para los ciudadanos facilitar información a los periodistas, sobre todo si esa información denuncia conductas indebidas graves o tiene que ver con la corrupción”. En el informe se señala que obligar a un periodista a revelar una fuente en casos de corrupción implicaría cortedad de miras. El informe, en el que también se cita la Recomendación R(2000)7 del Comité de Ministros del CdE, destaca los riesgos de mayor calado que conlleva desenmascarar las fuentes confidenciales de los periodistas para la capacidad de las personas de proporcionar información, y para la capacidad del público de recibirla. Por otra parte, se estipula que tal protección “no debe incluir únicamente a las personas de contacto de los periodistas, sino también a sus propios lugares de trabajo y su investigación”. Se argumenta además que: “las excepciones solo las otorgará un juez, y únicamente en el caso de testigos esenciales y delitos graves”, subrayando la importancia de especificar claramente las restricciones, “de manera que los periodistas puedan informar con fiabilidad a sus posibles fuentes de los riesgos que conlleva la situación”.

7. PANORAMA POR REGIÓN DE LA UNESCO

Como se señaló anteriormente, los cambios en los entornos jurídicos y reguladores en materia de protección de las fuentes periodísticas se registraron en 84 de los 121 países (69%) examinados para el presente informe durante el período de 2007 a 2015. El espacio disponible no permite un análisis detallado, pero los resultados, consignados en el estudio completo, ilustran unos efectos fundamental o potencialmente negativos en lo que atañe a la protección de las fuentes. Tales cambios se identificaron y analizaron en cada una de las cinco regiones de la UNESCO, prestando especial atención a los temas clave de:

1. el "efecto de eclipsado" de otras leyes ejercido por la legislación sobre la seguridad nacional y la lucha contra el terrorismo;
2. el papel de la vigilancia (masiva y selectiva) en el menoscabo de las protecciones;
3. el papel de los intermediarios terceros y la conservación de datos;
4. los cambios en el derecho a la protección: ¿quién es periodista?; ¿qué es periodismo?;
5. otras dimensiones digitales (p. ej., el anonimato);
6. dimensiones no digitales.

Porcentaje de países con cambios en los entornos jurídicos y reguladores en cuanto a la protección de las fuentes periodísticas, 2007-2015



7.1 ÁFRICA

En 18 de los 32 países (56%) examinados en la región africana se observaron cambios relevantes en la protección de las fuentes entre 2007 y mediados de 2015. Sin embargo, en 2015, las leyes de protección de las fuentes en África siguieron siendo limitadas. Los cambios jurídicos que han afectado a la confidencialidad de las fuentes y su protección en África en los ocho últimos años fueron en gran medida "no digitales". En varios Estados, los marcos jurídicos de protección de las fuentes se han visto amenazados por las medidas de establecimiento de exclusiones amplias respecto al derecho de los periodistas a proteger sus fuentes de la revelación por motivos de "seguridad nacional" y a la penalización de las infracciones. Entretanto, las acusaciones de vigilancia masiva surgieron como un tema destacado en algunos países. Los cambios ponen de relieve con menor obviedad el contexto digital y los riesgos asociados. Esto puede deberse a que el grado de penetración de Internet en esta región sigue siendo bajo. Como resultado, muchos de los asuntos relacionados con la recogida de información digital o la publicación de noticias en la Red no han entrado aún en el debate nacional en numerosos países africanos. Abundan los gobiernos que actualmente no perciben una necesidad de regular los medios digitales (ya sea para proteger o restringir el periodismo), en parte debido al número relativamente escaso de personas con un acceso significativo a tales medios. Esta tendencia puede cambiar en el futuro, a medida que aumente la cifra de usuarios que puedan acceder regularmente a contenidos de noticias en línea.

7.2 REGIÓN ÁRABE

Se produjeron cambios en seis de los siete países (86%) estudiados en la región entre 2007 y mediados de 2015. Los más destacados atañen a la vigilancia masiva y los ámbitos no digitales. Solo se observó un cambio digno de mención en los distintos países en relación con los intermediarios terceros. Puede que este hecho tenga que ver con una penetración limitada de Internet, o con los estrictos controles aplicados a la Red en ciertas partes de la región. Aunque la extensión en el uso de Internet en los estados árabes sigue siendo escasa en comparación con otras regiones, el número creciente de usuarios ha dado lugar a que tres países hayan adoptado leyes que regulan el uso de la Red desde 2007, con posibles implicaciones para la protección de las fuentes. En dos de los países estudiados se apreciaron cambios respecto a la cuestión de quién tiene derecho a reivindicar la protección de las fuentes. Cuatro de los seis países en los que hubo cambios mostraron evoluciones no digitales en relación con la protección de las fuentes.

Cabe señalar que la metodología aplicada al estudio excluyó a varios Estados árabes objeto de una drástica transición desde 2007. En este sentido, se recomienda la puesta en marcha de nuevos estudios exhaustivos en todos los Estados árabes de la UNESCO, con el fin de determinar los efectos de la radical transformación de los entornos de las comunicaciones en la protección de las fuentes en la región.

7.3 ASIA Y EL PACÍFICO

De los 24 países analizados en la región de Asia y el Pacífico, 18 (75%) han puesto de relieve la existencia de cambios en lo que respecta a la protección de las fuentes periodísticas desde 2007. La repercusión en las libertades civiles de las medidas adoptadas para reforzar la seguridad nacional, la vigilancia masiva y la conservación de datos; la implicación de intermediarios terceros; las definiciones ambiguas de periodistas y blogueros; y otras cuestión de índole digital y no digital, han debilitado la protección de las fuentes. Los cambios más destacados se reflejan en los ocho países en los que se documentaron problemas en materia de seguridad nacional. Siete países aplicaron medidas relacionadas con la vigilancia masiva y la conservación de datos en el período examinado, y cinco países se ocuparon de las definiciones de periodistas y blogueros en referencia al acceso a la protección de las fuentes.

7.4 EUROPA Y AMÉRICA DEL NORTE

Veinticinco de los 38 (66%) países examinados en Europa y América del Norte experimentaron cambios significativos relativos a las leyes de protección de las fuentes en el período de 2007 a 2015. Tales cambios reflejaron los temas clave identificados, asociados a los efectos digitales emergentes en los marcos jurídicos de protección de las fuentes: a) efectos en materia de seguridad nacional y lucha contra el terrorismo; b) vigilancia; c) conservación y entrega de datos y el papel de los intermediarios terceros; d) cuestiones relativas al derecho a reivindicar la protección de las fuentes; e) el aumento del riesgo de exposición de las fuentes debido a las comunicaciones periodísticas almacenadas digitalmente e incautadas durante las investigaciones.

7.5 AMÉRICA LATINA Y EL CARIBE

En 17 de los 20 países (85%) examinados en América Latina y el Caribe se identificaron cambios significativos con repercusión en la cobertura de la protección de las fuentes entre 2007 y 2015. Esos 17 países se encuentran en América Latina. La vigilancia fue uno de los temas considerados claramente en 10 de los países estudiados, y 5 de ellos adoptaron nuevas leyes que permiten la conservación y/o la intercepción de datos. Cuatro países han propuesta modificaciones de las leyes de secretos de Estado o de clasificación de la información, que en algunos casos disponen penas de cárcel por la revelación de tal información. Aunque muchos países cuentan con leyes para proteger las fuentes periodísticas, cada vez resulta más evidente que estas pueden ser identificadas por otros medios, como las interceptaciones, amenazas, redadas, accesos a datos almacenados y la biometría. En muchos de los países examinados en América Latina, estos factores, junto con la clasificación y la restricción de la información en nombre de

la seguridad nacionales, han convertido a gran parte de los mecanismos de protección de las fuentes periodísticas en elementos simbólicos, más que efectivos en la práctica, debido a los efectos de la corrupción y la delincuencia organizada.

En cualquier caso, tres países de América Latina han promulgado nuevas leyes de protección de las fuentes.

8. ESTUDIO TEMÁTICO: HACIA UN MARCO INTERNACIONAL PARA EVALUAR LAS EXCEPCIONES A LA PROTECCIÓN DE LAS FUENTES

En este apartado se examina el desarrollo de un marco de once puntos para evaluar la eficacia de los sistemas jurídicos de protección de las fuentes en la era digital. Se basa en entrevistas cualitativas extensas con 31 expertos internacionales de las cinco regiones de la UNESCO en las áreas del derecho, los derechos humanos, otros ámbitos académicos, y el periodismo profesional, además de especialistas en las TIC. Las entrevistas se llevaron a cabo en persona, a través de Skype, por teléfono y por correo electrónico entre noviembre de 2014 y febrero de 2015. Sobre la base de un estudio inicial de las cuestiones consideradas, y en consulta con la UNESCO, los investigadores presentaron un proyecto de estándar de ocho puntos para su consideración por los expertos. A continuación, se procedió a su desarrollo y ampliación a una herramienta de evaluación de once puntos, basada en las aportaciones de los expertos.

La nueva herramienta se ha diseñado para ser aplicable a todos los entornos internacionales, y para evaluar la eficacia de los marcos jurídicos de protección de las fuentes en cada Estado, en el contexto de las leyes y principios internacionales consolidados en materia de derechos humanos.

Principios para la evaluación de los marcos jurídicos de protección de las fuentes a escala internacional

En condiciones ideales, un marco de protección de las fuentes sólido y exhaustivo contemplaría la necesidad de:

1. reconocer el valor del interés público de la protección de las fuentes, con su fundamento jurídico en el derecho a la libertad de expresión (incluida la libertad de prensa) y a la privacidad. Tal protección debe incorporarse asimismo a la constitución del país y/o a la legislación nacional,

2. reconocer que la protección de las fuentes debe extenderse a todos los actos de periodismo y a todas las plataformas, servicios y medios (de almacenamiento y publicación de datos), y que ha de incluir los datos digitales y los metadatos,

3. reconocer que la protección de las fuentes no conlleva ni el registro de los profesionales del periodismo, ni la concesión de licencias a los mismos,

4. reconocer el posible efecto pernicioso en el periodismo de interés público, y en la sociedad, de que la información relacionada con las fuentes se capture en el registro, el seguimiento, el almacenamiento y la recogida de datos en grandes cantidades,

5. afirmar que los agentes estatales y empresariales (incluidos los intermediarios terceros) que capturan datos digitales periodísticos deben tratar estos de manera confidencial (reconociendo asimismo la idoneidad de un almacenamiento y un uso de tales datos conforme con el derecho general a la privacidad),

6. proteger los actos de periodismo de la vigilancia selectiva, la conservación de datos y la entrega de material relacionado con fuentes confidenciales,

7. definir excepciones a todas las premisas anteriores de un modo muy restrictivo, de manera que se preserve el principio de la protección de las fuentes como la norma y el estándar efectivos,

8. definir excepciones cuando se requiera con arreglo a disposiciones de "necesidad" y "proporcionalidad" (en otras palabras, cuando no sea posible una alternativa a la revelación, cuando exista más interés público en la revelación que en la protección, y cuando las condiciones y el alcance de la revelación sigan preservando la confidencialidad en la medida de lo posible),

9. definir un proceso judicial transparente e independiente con opción al recurso respecto a las excepciones autorizadas, y garantizar que los agentes de las fuerzas de orden público y los agentes judiciales reciban formación sobre los principios considerados,

10. tipificar como delito las infracciones arbitrarias, no autorizadas y deliberadas de la confidencialidad de las fuentes cometidas por terceros,

11. reconocer que las leyes sobre protección de las fuentes pueden reforzarse mediante una legislación complementaria sobre informantes.

Nuevos estudios podrían dar lugar al desarrollo de un repositorio de ejemplos de leyes modelo y sentencias ilustrativas que aborden las cuestiones de las "excepciones" y las disposiciones sobre "necesidad". Un resumen de tal repositorio podría adjuntarse a este marco de evaluación modelo.

9. DIMENSIONES DE GÉNERO

Las periodistas afrontan riesgos adicionales en el desempeño de su trabajo, tanto en línea, como fuera de Internet. En el mundo físico, entre tales riesgos figuran el acoso sexual, el asalto físico y la violación. En el ámbito digital, los actos de acoso y las amenazas de violencia aumentan de manera desenfrenada. Del mismo modo, las fuentes mujeres se enfrentan a diversos riesgos cuando actúan como denunciantes o informantes confidenciales. Estas cuestiones se manifiestan de diversos modos en lo que atañe a la protección de las fuentes en la era digital. Se desarrollan con mayor detalle más adelante, y pueden resumirse como sigue:

1. En comparación con sus colegas varones, las periodistas afrontan riesgos adicionales en el trato con las fuentes confidenciales.

2. Las fuentes mujeres se enfrentan a riesgos físicos mayores en sus encuentros con periodistas y al revelar información confidencial.

3. Los riesgos físicos que encaran las mujeres, tanto las periodistas, como las que actúan como fuente, en el curso de las comunicaciones confidenciales pueden exigir que las mujeres confíen cada vez más en las comunicaciones digitales, lo que da lugar a vulnerabilidades específicas.

4. Cabría señalar que las salvaguardas en las comunicaciones digitales seguras, incluido el cifrado, son aún más necesarias para las periodistas y las fuentes mujeres que para los varones.

Factores específicos para su consideración

1. *Las mujeres periodistas y fuentes han de ser capaces de comunicarse por medios digitales.*

Las periodistas que informan de conflictos y de la delincuencia organizada son especialmente vulnerables a las agresiones físicas, incluidos los asaltos y el acoso sexuales. En ciertos contextos, su movilidad física puede verse restringida debido a las amenazas manifiestas para su seguridad, o como resultado de prohibiciones culturales respecto a la conducta de las mujeres en público, incluidos los encuentros en privado con varones que ejercen como fuentes. En este sentido, a menudo, las periodistas necesitan estar en disposición de servirse de medios no físicos seguros de comunicación con sus fuentes.

Las mujeres que ejercen como fuente pueden enfrentarse a los mismos riesgos físicos esbozados anteriormente, sobre todo si su contacto periodístico es varón, y/o son objeto de restricciones culturales, o trabajan en zonas de conflicto. Por otro lado, las fuentes confidenciales que son mujeres y han sido víctimas de la violencia doméstica pueden verse físicamente incapacitadas para abandonar su domicilio y, por tanto, es posible que dependan de las comunicaciones digitales. Estos factores plantean retos

adicionales para las mujeres periodistas y que ejercen como fuentes, en lo que respecta al mantenimiento de la confidencialidad en la era digital.

2. *La seguridad digital es fundamental para las mujeres que ejercen como fuentes y las periodistas*

Las periodistas han de poder confiar en la seguridad de las comunicaciones digitales para garantizar que no corren un mayor riesgo en zonas de conflicto o cuando tratan materias peligrosas, como la corrupción o la delincuencia. La capacidad para interceptar y analizar de manera encubierta las comunicaciones periodísticas con las fuentes eleva el riesgo físico tanto para las periodistas, como para sus fuentes en tales contextos. En este sentido, las comunicaciones cifradas y otras medidas preventivas revisten una enorme importancia para garantizar que sus movimientos no sean objeto de seguimiento, y para que la identidad de las fuentes siga siendo confidencial.

Los riesgos de exposición para las fuentes confidenciales se magnifica en el caso de las informantes mujeres. Por tanto, es necesario que puedan disponer de acceso a métodos de comunicación digital seguros para garantizar que se corre un riesgo mínimo de detección y desenmascaramiento. También es necesario que confíen en la capacidad para establecer un contacto seguro con los periodistas, de manera que las historias que afecten a las mujeres se cuenten, y se propicie la participación de este colectivo en el periodismo de interés público. Las informantes pueden ayudar asimismo a evitar que se multiplique la "inhibición" del periodismo de investigación que depende de fuentes confidenciales femeninas. Se requieren además sólidas medidas de protección jurídica en materia de confidencialidad, aplicadas de un modo en que se tenga en cuenta el género, sobre todo en lo que atañe a las órdenes judiciales que obligan a la revelación de las fuentes.

3. *Acoso y amenazas en línea*

Los periodistas y las fuentes que se comunican a través de Internet, incluidas las aplicaciones para teléfonos móviles, pueden exponerse a un mayor riesgo de acoso y amenazas de violencia relacionados con el género. Tales riesgos han de comprenderse y atenuarse para evitar una inhibición ulterior de la participación de las mujeres en el periodismo, ya sea como periodistas, o como fuentes.

10. CONCLUSIÓN

Se han producido cambios significativos en el ámbito de la protección jurídica de las fuentes periodísticas entre 2007 y mediados de 2015. Se ha observado una tendencia parcial al reconocimiento preliminar de las dificultades existentes en lo que se refiere a los agentes internacionales, pero el reconocimiento de la cuestión es menor a escala estatal nacional. Los cambios registrados en los ocho últimos años en el 69% (84 países de 121) de los Estados se mueven en general en direcciones que van en contra de una sólida protección de las fuentes en la era digital. Los marcos jurídicos que sostienen la protección de las fuentes periodísticas se encuentran sometidos a una tensión significativa en dicha era, y esta forma de protección es objeto innecesariamente de daños colaterales en un contexto marcado por otras tendencias de la seguridad de mayor alcance que pueden dar lugar para ciertas sociedades a una pérdida de los beneficios derivados de esta particular excepción.

El derecho a la privacidad, del que dependen en parte los periodistas y los informantes para garantizar la confidencialidad, se pone directamente en duda, lo que repercute en la protección de las fuentes y la libertad de expresión en términos más generales. En muchos de los países estudiados, los marcos jurídicos referidos anteriormente sufren el menoscabo de la legislación en materia de seguridad nacional, lucha contra el terrorismo y conservación de datos, que eclipsa a las leyes de protección de las fuentes, o corren el riesgo de verse debilitados por el ejercicio de la vigilancia masiva y selectiva. Otras amenazas surgen debido a la presión que se ejerce sobre los intermediarios terceros para que faciliten los datos que pueden exponer a las fuentes, en respuesta a requerimientos jurídicos o autorizados por el Estado. También aumentan las dificultades en el caso de las medidas técnicas que facilitan el mantenimiento de la confidencialidad, como los límites al anonimato o las medidas para ilegalizar el cifrado.

Por otra parte, está la cuestión del derecho a la protección: en una era en la que los ciudadanos y otros comunicadores sociales cuentan con la capacidad para publicar directamente para sus propias audiencias, y los que comparten información de interés público son reconocidos como agentes periodísticos legítimos por las Naciones Unidas, ¿a quién deben aplicarse las leyes de protección de las fuentes? Por un lado, conviene ampliar la definición jurídica de “periodista” para garantizar una protección adecuada de los “periodistas ciudadanos” (que trabajan en línea y fuera de Internet), y la jurisprudencia avanza gradualmente en el tratamiento de esta cuestión de redefinición. Por otro lado, sin embargo, tal ampliación abre el debate sobre la concesión de licencias y el registro de aquellos que ejercen el periodismo y desean que se les reconozca para obtener la protección de sus fuentes. Por este motivo, las pruebas esenciales en la sociedad contemporánea para el acceso a las leyes de protección de las fuentes evolucionan hacia la definición y la identificación de los “actos de periodismo”, dejando a un lado los factores de descripción ocupacional o profesional.

Los periodistas y los medios de comunicación se encuentran en un proceso de adaptación de sus prácticas, reforzando la seguridad digital y retomando métodos de comunicación de la era predigital con las fuentes confidenciales. En cualquier caso, si los Estados y los organismos regionales no revisan y consolidan sus marcos jurídicos de protección de las fuentes, que los periodistas adapten sus métodos de comunicación y retomen elementos básicos analógicos (una opción no siempre viable, sobre todo, y como se ha referido anteriormente, en el caso de las periodistas) no bastará para preservar dicha protección en la era digital. En una época de dispositivos tecnológicamente avanzados para el espionaje, también es necesario que los Estados revisen sus prácticas de vigilancia y su supervisión con arreglo a las resoluciones sobre privacidad de la Asamblea General de la ONU. Por otra parte, los Estados han de limitar las leyes de conservación y facilitación de datos, potenciar las medidas de rendición de cuentas y transparencia (aplicadas tanto a los Estados como a las empresas respecto a los datos periodísticos), y crear excepciones para los actos periodísticos en el marco de la legislación nacional general en materia de seguridad.

V. FOMENTO DE LA LIBERTAD EN LA RED: EL PAPEL DE LOS INTERMEDIARIOS DE INTERNET[6]

6 Este capítulo se basa en MacKinnon, R. y cols. 2014. *Fostering Freedom Online: The Role of Internet Intermediaries* (Fomento de la libertad en la Red: el papel de los intermediarios de Internet). UNESCO Series on Internet Freedom (Serie de la UNESCO sobre la libertad en Internet). París: UNESCO / Internet Society. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

1. INTRODUCCIÓN

A medida que evoluciona Internet, una tendencia cada vez más evidente es la del papel que desempeñan las empresas del sector privado. Entre estas, el motor de búsqueda de Google, la red social de Twitter y los servicios de telecomunicación e Internet de Vodafone constituyen ejemplos de *intermediarios de Internet* porque *median* en las comunicaciones en *línea* y habilitan diversas formas de expresión en la Red. Los intermediarios también pueden actuar como puntos de control, árbitros, defensores, o "guardianes" selectivos de la expresión. Sin embargo, el poder de los intermediarios solo puede entenderse plenamente en el contexto del poder estatal. La posición de los intermediarios de Internet en relación con los Estados y con las normas internacionales de derechos humanos es complicada: suelen actuar en varias jurisdicciones, y los Estados esperan de ellos que cumplan la legislación nacional que, a su vez, se atiene en diversos grados a las normas referidas. Algunos consideran estas empresas como una fuente de "tecnología de la liberación" que contribuirá a "romper las cadenas" de los oprimidos. Otros las han criticado por no hacer lo suficiente para proteger los derechos a la privacidad de los usuarios y facilitar el ejercicio de una vigilancia sin asumir responsabilidades por parte del sector de privado y las administraciones públicas. Los intermediarios se muestran cada vez más concienciados de que tienen un papel importante y positivo que desempeñar en el fomento de los derechos. Sin embargo, para proteger la libertad de expresión y la privacidad y abstenerse de infringir derechos, han de atenerse con mayor rigor a las normas internacionales de transparencia, necesidad, proporcionalidad, fin legítimo y respeto de las garantías procesales.

En el presente capítulo se examinan las tendencias recientes de las políticas y las prácticas de los intermediarios respecto a la libertad de expresión y la privacidad de los usuarios, sobre la base del estudio de la UNESCO de 2014 titulado *Fostering Freedom Online: The Role of Internet Intermediaries* (Fomento de la libertad en la Red: el papel de los intermediarios de Internet). Esta publicación sirvió para fundamentar el estudio exhaustivo de la UNESCO sobre asuntos relacionados con Internet, encargado por los Estados Miembros en la Resolución 61 de la 37ª Conferencia General de la UNESCO en 2013, publicado en 2015 bajo el título de *Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet* (Claves para promover unas sociedades del conocimiento integradoras: acceso a la información y el conocimiento, libertad de expresión, privacidad y ética en una Internet global).

1.1 EMPRESA Y DERECHOS HUMANOS

El derecho internacional en materia de derechos humanos se ha centrado tradicionalmente en la conducta de los Estados, sobre la base de las declaraciones y los convenios establecidos por estos. Sin embargo, en las últimas décadas, existe un

creciente reconocimiento de que las empresas también han de asumir responsabilidades relacionadas con los derechos humanos, por las que han de rendir cuentas. Puesto que la mayoría de los intermediarios de Internet los gestionan empresas del sector privado, este capítulo se basa en las normas consolidadas relativas a la actividad empresarial y los derechos humanos establecidas en el marco de "proteger, respetar y remediar" de las Naciones Unidas. Se evalúa que, mientras los gobiernos tienen la obligación primordial de proteger los derechos humanos, las empresas son responsables por su parte de respetarlos, y ambas entidades deben garantizar el acceso a remedios efectivos.

Esta perspectiva se ha desarrollado con mayor amplitud en diversas tendencias a lo largo de los últimos cinco años. En 2011, el Consejo de Derechos Humanos de la ONU (CDHNU) aprobó los Principios Rectores sobre las empresas y los derechos humanos de las Naciones Unidas, el resultado de seis años de investigación y consulta con empresas, administraciones públicas y la sociedad civil por parte del Representante Especial del Secretario General para la cuestión de los derechos humanos y las empresas transnacionales y otras empresas. Los Principios Rectores comienzan con la consideración del deber de los Estados de proteger contra los abusos de los derechos humanos cometidos por empresas que actúen en su territorio, y de "enunciar claramente que se espera de todas las empresas domiciliadas en su territorio y/o jurisdicción que respeten los derechos humanos en todas sus actividades". Estos principios se aplican a todas las empresas, y no solo a los intermediarios de Internet. Son asimismo de aplicación universal. Navi Pillay, Alta Comisionada para los Derechos Humanos, señaló en su informe de junio de 2014 a la Asamblea General que "la responsabilidad de respetar los derechos humanos se aplica a todas las actividades globales de una empresa, con independencia del lugar en que se ubiquen sus usuarios, y de que el Estado de que se trate atienda sus propias obligaciones en materia de derechos humanos".

En el presente capítulo se identifican las tendencias relativas a lo que los intermediarios de Internet han hecho y pueden seguir haciendo para maximizar la libertad de expresión en el marco de diversas jurisdicciones, contextos, tecnologías y modelos empresariales. No obstante, para el seguimiento y la comprensión de estas actividades, es necesario antes examinar con mayor detenimiento la naturaleza de los intermediarios y su relación con la libertad de expresión.

1.2 INTERMEDIARIOS

Un intermediario, según la definición del experto jurista Thomas F. Cotter, es "toda entidad que hace posible la comunicación de información de una parte a otra". En un informe de 2010, la OCDE explica que los intermediarios de Internet "reúnen o facilitan las transacciones entre terceros en Internet. Otorgan acceso, albergan, transmiten e indizan contenidos, productos y servicios generados por terceros en la Red, o prestan servicios basados en Internet a terceros". En la mayoría de las definiciones de intermediario se excluyen explícitamente a los productores de contenidos, al igual que en el presente

capítulo. De manera más concreta, la OCDE excluye de la función del intermediario "las actividades en las que los proveedores de servicios otorgan acceso, albergan, transmiten o indizan contenidos o servicios generados por ellos mismos". En este sentido, los editores y otros medios que crean y difunden contenidos originales *no* son intermediarios. Son ejemplo de tales entidades los sitios web de noticias que publican artículos escritos y editados por su personal o colaboradores invitados, o los servicios de suscripción de vídeo digital que contratan o invitan a personas para producir vídeos y difundirlos a sus suscriptores.

Al mismo tiempo, muchas entidades ofrecen servicios híbridos y son intermediarios en una u otra medida. La medida en que los servicios de redes sociales, por ejemplo, ejercen fundamentalmente como intermediarios, o desempeñan una función de medio de comunicación, es importante en términos de expectativas. En 2011, el Consejo de Europa adoptó una definición amplia de los medios de comunicación, aplicando seis criterios para evaluar cuándo un nuevo agente puede ser considerado como un medio. Tales criterios comprenden la intención de actuar como medio, el ejercicio de control editorial, y la aplicación de estándares profesionales. No obstante, algunas partes interesadas han objetado que los esfuerzos dedicados por ciertos Estados a definir a los intermediarios como "medios de comunicación" han dado lugar a una restricción más acentuada de la libertad de expresión. Aunque existen ciertas similitudes potenciales entre tales medios y los intermediarios en algunos casos, también se dan diferencias significativas en su evolución. Mientras que los medios son responsables en general de sus contenidos desde el punto de vista jurídico, debido a su control editorial, los intermediarios suelen asumir una responsabilidad jurídica limitada, en cuanto que los contenidos transmitidos parten de agentes independientes a su control (véase 2.2 más adelante).

Todos los intermediarios de Internet de gestión mercantil estudiados en el presente capítulo exigen a sus usuarios que convengan con las "condiciones de servicio" antes de permitirles la utilización de este. En ocasiones, tales condiciones pueden restringir la expresión de los usuarios, cuando esta se encuentra protegida en realidad por la legislación en ciertas jurisdicciones. Aunque la ejecución de dichas condiciones puede asemejarse a veces a una función editorial, el fundamente jurídico de tal ejecución en Estados Unidos y Europa, donde surgieron los intermediarios de Internet por vez primera, no se deriva de la legislación que atañe a los medios de comunicación, sino del Derecho contractual y mercantil.

1.2.1 Tipos de intermediarios

El presente capítulo se ocupa de los servicios y plataformas que se dedican fundamentalmente a albergar, otorgar acceso, indizar o facilitar la transmisión y la puesta en común de contenidos creados por terceros. Dado que la importancia de los intermediarios ha aumentado para la economía global del conocimiento, varias organizaciones se han propuesto describir o clasificar los tipos de intermediarios con arreglo a sus actividades y su función técnica. Entre tales organizaciones figuran la

OCDE, el Relator Especial de la ONU para la Libertad de Opinión y de Expresión, y diversas instituciones de la sociedad civil. En el cuadro que se muestra a continuación se ofrece una comparación de los principales tipos de intermediario que han caracterizado o seleccionado estas organizaciones para su examen.

Cuadro 1: Categorías y ejemplos clave de intermediarios de Internet

<table>
<tr><th>OCDE</th><th>Relator Especial La Rue</th><th>ARTÍCULO 19</th><th>Centro para la Democracia y la Tecnología.</th><th>Socios Globales</th></tr>
<tr><td rowspan="2">Proveedores de acceso y servicios de Internet</td><td rowspan="2">Proveedores de servicios de Internet (PSI)</td><td rowspan="2">Proveedores de servicios de Internet (PSI)</td><td rowspan="2">Proveedores de acceso/PSI
Operadores de red y proveedores de telecomunicaciones móviles</td><td>Capa física: hace posible las comunicaciones</td></tr>
<tr><td>Conectividad y código: lenguaje o protocolos de la comunicación</td></tr>
<tr><td>Proveedores de servicios de proceso de datos y de alojamiento web</td><td></td><td>Proveedores de alojamiento web</td><td>Registradores de dominios y registros
Empresas de alojamiento de sitios web</td><td rowspan="5">Aplicaciones: herramientas para navegar por contenidos</td></tr>
<tr><td>Motores de búsqueda y portales de Internet</td><td>Motores de búsqueda</td><td>Motores de búsqueda</td><td>Motores de búsqueda y portales de Internet</td></tr>
<tr><td>Intermediarios de comercio electrónico</td><td rowspan="2"></td><td rowspan="2"></td><td rowspan="2">Plataformas de comercio electrónico y mercados en línea</td></tr>
<tr><td>Sistemas de pago por Internet</td></tr>
<tr><td>Plataformas de redes participativas</td><td>Servicios para blogs
Comunidades en línea
Plataformas de redes sociales</td><td>Plataformas de redes sociales</td><td>Proveedores de servicios en línea
En general, todo sitio web que aloje contenidos generados por los usuarios o permita las comunicaciones entre estos</td></tr>
</table>

De esta clasificación se deduce claramente que distintos tipos de intermediarios desempeñan funciones diferentes y cuentan con arquitecturas técnicas dispares. Por ejemplo, los proveedores de servicios de Internet (PSI) conectan el dispositivo de un usuario a la Red y, a continuación, los proveedores de alojamiento web y los registradores y registros de dominio hacen posible que se publiquen los sitios web y que se pueda acceder a ellos. Los motores de búsqueda hacen accesible una parte de la *World Wide Web* al permitir que los usuarios realicen búsquedas en sus bases de datos y, a menudo, constituyen un intermediario esencial entre los sitios web y los internautas. Las redes sociales posibilitan que los usuarios de Internet intercambien texto, fotos y vídeos, y les permiten publicar contenidos dirigidos a su red de contactos o al público en general.

Asimismo, resulta evidente que la existencia de diversos tipos de intermediario conlleva distintas clases de modelos de negocio. Para proporcionar acceso a Internet y/o servicios de telecomunicaciones, las empresas se sirven de equipos y servicios en las jurisdicciones geográficas en las que residen físicamente los clientes. Este tipo de servicio requiere una considerable inversión de recursos, equipos y personal en jurisdicciones físicas, la solicitud de permisos de la administración pública, y el cumplimiento de la legislación local. De esta manera, los Estados mantienen un alto grado de influencia en los PSI.

Los mismos agentes no proporcionan necesariamente servicios de telecomunicaciones y acceso a Internet. Gran parte de la prestación de servicios de Internet se lleva a cabo sobre la infraestructura de transmisión técnica de telecomunicación, que puede constituir una capa subyacente para la exclusión o la limitación del acceso a ciertos PSI o a los usuarios de sus clientes. A su vez, los PSI pueden limitar el acceso a un segundo nivel con independencia de su relación con los operadores de infraestructuras de telecomunicaciones. La dependencia de los PSI de las telecomunicaciones convierte el nivel de los intermediarios vinculado a las redes en un elemento particularmente susceptible a la regulación de los Estados.

Por el contrario, otros tipos de intermediario como los proveedores de alojamiento web, los registradores y registros de nombres de dominio, los motores de búsqueda y las redes sociales no han de localizar necesariamente al personal, los equipos u otros recursos físicos en el área geográfica de los usuarios a los que se proponen prestar servicio. La arquitectura abierta e interoperable de Internet hace posible que un usuario en un país dado pueda efectuar una búsqueda en Google, crear un sitio web con un servicio de alojamiento web, o comunicarse con sus amigos en Facebook sin que tales empresas dispongan de personal, oficinas o equipos en dicho país. Este hecho puede distanciar a los intermediarios de Internet, y a sus usuarios, del control ejercido por los Estados en los que no han establecido su sede principal ni mantienen otro tipo de presencia física.

Esta independencia relativa constituye precisamente el motivo por el que ciertos representantes del ámbito académico han documentado que los nuevos medios de comunicación, y en particular, las redes sociales, fomentan la libertad de expresión en contextos en los que la expresión fuera de Internet se encuentra sometida a una fuerte restricción por parte del Estado. No obstante, en la práctica, un número creciente de Estados imponen su jurisdicción sobre los intermediarios ejerciendo control sobre el nivel subyacente de los proveedores de telecomunicaciones y los PSI, que actúan como puntos de paso forzoso para el acceso a la Red. Los Estados pueden amenazar con denegar el acceso a todos los usuarios bajo su jurisdicción a un determinado servicio si los intermediarios situados en una ubicación remota dejan de cumplir su legislación, y cada vez llevan a efecto tal amenaza. Dirigiendo su actuación a los intermediarios a diferentes niveles, los Estados pueden ejercer su control sobre la expresión de los usuarios en Internet, o sobre el acceso a la información, aún cuanto la expresión o el acceso se lleven a cabo fuera de la jurisdicción nacional. Los Estados también pueden delegar los controles en los intermediarios, sin ocuparse de vigilar directamente a los usuarios por sí mismos.

1.2.2 Modos de restricción

Dependiendo del tipo de intermediario y del servicio ofrecido, los intermediarios controlan cómo y con quién pueden comunicarse sus usuarios. Disponen de acceso a la información creada por los usuarios, así como a diversos datos relacionados directamente con los usuarios. Por este motivo, los intermediarios son clave en la tarea de facilitar y proteger los derechos a la libertad de expresión y la privacidad. Ejercen asimismo como vías a través de las cuáles, los gobiernos pueden vigilar, regular y controlar las actividades y el acceso a la información de los usuarios en Internet. Las dos vías fundamentales para restringir la libertad de expresión a través de los PSI, los motores de búsqueda y las redes sociales pueden describirse en términos generales como sigue:

1. **al nivel de las redes**, los proveedores de acceso a las telecomunicaciones y los PSI pueden utilizarse para coartar la libertad de expresión de tres maneras principales:

    a) ***Filtrado***: se bloquea el acceso a sitios web en su totalidad, a páginas específicas, o a términos clave concretos. El filtrado lo efectúa el PSI o los operadores de red que controlan los flujos de Internet en una jurisdicción, o algún tipo de combinación de las dos entidades. El contenido sigue existiendo en otro lugar en Internet, pero no pueden acceder al mismo los usuarios de la red en la que se aplica el filtro. Tal bloqueo impide que los usuarios reciban información, pero también puede evitar que la publiquen en una ubicación específica como una red social.

    b) ***Interrupción del servicio***: Uno o varios servicios ofrecidos por un proveedor, o por todos los proveedores, pueden interrumpirse en una determinada jurisdicción o área geográfica, impidiendo que los usuarios de dicha área accedan a Internet a través de la línea fija o el móvil, envíen mensajes SMS, etc.

    c) ***Servicio no neutral***: El acceso a ciertos contenidos o aplicaciones se “atenúa” o ralentiza, dificultando el acceso a los usuarios. Como alternativa, puede cobrarse a los usuarios tarifas diferentes por el acceso a distintos tipos de contenidos o servicios, o se les puede otorgar un acceso gratuito a determinados servicios.

Los otros dos tipos de intermediarios considerados en el presente capítulo, a saber, los motores de búsqueda y las redes sociales, resultan afectados directamente si tales restricciones se llevan a cabo al nivel de la red. Al mismo tiempo, el filtrado o la amenaza de filtrado a dicho nivel constituye un medio encaminado a presionar a los motores de búsqueda, las redes sociales u otros intermediarios para que establezcan restricciones al nivel de plataforma.

2. Los intermediarios que operan **a nivel de plataforma**, como los motores de búsqueda y las redes sociales, pueden actuar para suprimir contenidos por completo, bloquear el acceso a los mismos para determinadas categorías de usuarios, o desactivar sus cuentas. Estas acciones las lleva a cabo la propia empresa, o las autoridades públicas a las que se haya concedido un acceso técnico directo a las funciones esenciales de la plataforma. La supresión, el bloqueo o la desactivación pueden efectuarse

a petición de un gobierno, de los usuarios, o de terceros, o con arreglo a las normas privadas propias del intermediario.

Las restricciones descritas anteriormente constituyen una herramienta de ejecución para diversos tipos de gobernanza pública y privada. Se utilizan para ejecutar la reglamentación o la legislación estatal, o para contribuir a identificar las infracciones de la reglamentación estatal, y ejecutar las condiciones de servicio y otras normas privadas de las empresas. También se emplean en algunos países para aplicar las normas emitidas por órganos privados o semipúblicos.

A la libertad de expresión pueden afectarle asimismo las acciones de los intermediarios relacionadas con la privacidad (a nivel de red y de plataforma). Los usuarios de Internet que creen que sus comunicaciones y su conducta en línea son vigiladas o expuestas de un modo que infringe sus derechos a la privacidad se expresarán libremente con menor probabilidad al utilizar los servicios de intermediarios. La privacidad puede verse afectada negativamente por todas las escalas de intermediarios, como sigue:

a) las tareas de **recogida y seguimiento de datos** se llevan a cabo en todas las escalas de Internet, y pueden restringir la expresión al fomentar la autocensura.

b) La **falta de seguridad en el modo en que se almacenan los datos de los usuarios o en la manera en que se transmiten los contenidos** puede dar lugar a infracciones de la privacidad, y a interceptaciones no autorizadas o efectuadas por autoridades públicas, sin la intervención activa de la empresa.

c) Los diferentes servicios y plataformas proporcionan a los usuarios de Internet distintos niveles de control sobre su información personal, y sobre el modo en que se conserva o se accede a la misma públicamente, en su caso.

En el cuadro que sigue figura un resumen de los modos de restricción descritos anteriormente.

Cuadro 2: Modos en que puede restringirse la expresión y la privacidad a través de los intermediarios de Internet, previa petición, o a iniciativa propia de la empresa

	PSI	Motores de búsqueda	Redes sociales
Restricciones a nivel de red	• Filtrado • Interrupción del servicio • Servicio no neutral		
Restricciones a nivel de plataforma		• Manipulación del posicionamiento de búsqueda • Supresión o retirada de los vínculos a determinadas páginas web o categorías de páginas web	• Supresión de contenidos de la plataforma • Bloqueo de contenidos, y oportunidades de libre expresión, mediante la restricción del acceso de determinadas categorías de usuarios (incluida la ubicación geográfica) • Limitación o desactivación de cuentas
Efectos inhibidores relacionados con la privacidad	• Recogida y retención de datos de los usuarios con fines mercantiles o por mandato de la administración pública • Requisitos respecto al registro de cuentas con el "nombre real" • Peticiones de datos de usuarios por parte de la administración pública • Vigilancia en tiempo real llevada a cabo por la administración pública	• Recogida y retención de datos de los usuarios con fines mercantiles • Peticiones de datos de usuarios por parte de la administración pública • Catálogo de datos personales de los usuarios mediante las búsquedas con su nombre	• Recogida y retención de datos de los usuarios con fines mercantiles • Requisitos de identificación con el "nombre real" • Peticiones de datos de usuarios por parte de la administración pública

El papel que han venido desempeñando los intermediarios en la protección o la restricción de la libertad de expresión lo complica más aún la escala mundial de numerosas empresas. Las compañías multinacionales, así como los servicios de Internet con usuarios en múltiples jurisdicciones, pueden estar sometidas a una amalgama global de regímenes jurídicos y normativos. Algunas empresas de Internet han procurado abordar este dilema mediante la creación de filtros específicos nacionales y la formulación de políticas de empresa sobre el tratamiento de las peticiones de la administración pública respecto a la restricción de los contenidos, y las solicitudes de datos de los usuarios. Cuando una empresa carece de oficinas físicas o personal en una determinada jurisdicción, resulta difícil para la administración pública obligar a dicha empresa a someterse a su legislación o a responder a sus peticiones de restricción de contenidos. Como respuesta, algunos gobiernos han recurrido al filtrado, o la amenaza de filtrado, de contenidos o de servicios en su conjunto. A menudo, ante toda esta complejidad, las normas en materia de libertad de expresión no se entienden, protegen, respetan ni remedian adecuadamente.

1.2.3 Compromisos con la libertad de expresión

A la vista de este panorama mundial cada vez más complejo, han surgido diversas iniciativas como una tendencia emergente en los últimos años en los ámbitos empresarial y gubernamental, con el fin de ayudar a los intermediarios de Internet a promover el respeto por la privacidad y la libertad de expresión de los usuarios. Por ejemplo, en 2013, la Comisión Europea publicó una "guía sectorial" sobre el modo en que las empresas de las TIC pueden adoptar y aplicar los Principios Rectores sobre las empresas y los derechos humanos de las Naciones Unidas, que se formularon en consulta con las empresas del sector, el ámbito académico, la sociedad civil y los gobiernos. Algunos intermediarios han comenzado a asumir compromisos públicos con el respeto por los derechos de los usuarios. Desde su puesta en marcha en 2008, varias empresas de Internet se han sumado a la *Global Network Initiative* (GNI, Iniciativa de Redes Mundiales), un órgano integrado por diversas partes interesadas, en el que destacados intermediarios colaboran con distintos representantes de la sociedad civil, la inversión responsable y el ámbito académico en la ejecución de un conjunto de principios fundamentales de la libertad de expresión y la privacidad. Entre los intermediarios examinados en este informe, Google es un miembro fundador de la GNI. En enero de 2014, Google supero un proceso de evaluación que permitió verificar que la empresa había ejecutado de manera satisfactoria los principios de la GNI en cuanto a la gestión de los requerimientos de la administración pública respecto a la restricción de contenidos y los datos de los usuarios. Facebook se incorporó a la GNI en mayo de 2013, pero en septiembre de 2015 no se había sometido a una evaluación para comprobar si ha ejecutado o no los principios de la Iniciativa. En 2012, un grupo de empresas de telecomunicación entre las que se cuenta Vodafone establecieron el Diálogo sectorial sobre libertad de expresión y privacidad, en un esfuerzo por desarrollar los principios y las buenas prácticas pertinentes.

En este contexto, se observa una tendencia emergente en cuanto al número creciente de empresas de Internet y telecomunicaciones que han comenzado a publicar "informes de transparencia" periódicos, así denominados por la luz que arrojan sobre el volumen y la naturaleza de las peticiones de supresión de contenidos (ya procedan de la administración pública o de entidades privadas), o de revelación de datos de los usuarios. Tal transparencia ayuda a los usuarios y a la población en general a comprender qué clases de restricción se vienen adoptando, y en nombre de quién se llevan a cabo. Entre las empresas estudiadas en el presente capítulo, Facebook, Google, Twitter y Vodafone han publicado informes de transparencia. No obstante, es importante señalar que diversas variaciones sustanciales en cuanto a alcance, detalle y metodología de elaboración de informes dificultan la tarea de extraer conclusiones significativas acerca del respeto por la libertad de expresión y la privacidad de una empresas en comparación con otra. Varios expertos han dirigido un llamamiento a las empresas para que colaboren con representantes del ámbito académico y activistas para establecer enfoques más normalizados respecto a los informes de transparencia. Han propuesto que la transparencia plena conlleva algo más que referir las cifras de peticiones de la administración pública recibidas y atendidas, y que es necesario también actuar con transparencia respecto a las políticas y las prácticas de la empresa para gestionar tales peticiones, así como a los mecanismos de aplicación privados.

1.3 METODOLOGÍA

En el presente capítulo se revisan los estudios de caso elaborados en *Fostering Freedom Online: Role of Internet Intermediaries* (Fomento de la libertad en la Red: el papel de los intermediarios de Internet), y se examinan tres tipos de intermediarios y 11 empresas:

1. **PSI y servicios de telecomunicaciones Vodafone, Vivo/Telefônica Brasil, Bharti Airtel, Safaricom**
2. **Motores de búsqueda**: Google, Baidu, Yandex
3. **Redes sociales**: Facebook, Twitter, Weibo, iWiW

Los estudios de caso comprenden la descripción y el análisis de los contextos jurídicos y normativas en evolución en los que actúan los intermediarios de Internet, así como las tendencias en las políticas y las prácticas empresariales. África y la igualdad de género, por su condición de prioridades globales de la UNESCO, son objeto de apartados especiales. El capítulo concluye con las recomendaciones generales dirigidas a todas las partes interesadas.

La selección de los tres tipos de intermediarios diferentes se basó en la clasificación en cinco partes de intermediarios de Internet elaborada por la OCDE, más los tres tipos de intermediario elegidos como ejemplo en el informe de 2011 de Frank La Rue, antiguo Relator Especial de las Naciones Unidas, sobre el derecho a la libertad de opinión y de expresión en Internet. Se seleccionaron empresas y países de interés para cada caso porque representan colectivamente un conjunto de entornos culturales, regionales, políticos y jurídicos en los que han surgido intermediarios de Internet relevantes.

Para cada uno de los países objeto del estudio, se encargó a un equipo de investigación interno que cumplimentara un cuestionario pormenorizado elaborado a principios de 2014. En los cuestionarios figuraba un promedio de 61 preguntas acerca del contexto jurídico y político que atañe a la regulación de Internet, las políticas y prácticas de las empresas seleccionadas en los países elegidos, y el modo en que la combinación de determinadas políticas empresariales y contextos jurídicos afecta a los usuarios de la Red, así como varias preguntas específicas relativas a las cuestiones de género. La investigación para los cuestionarios se llevó a cabo en marzo y abril de 2014, meses en los que los investigadores celebraron entrevistas con representantes de las empresas, la administración pública, la sociedad civil, y los ámbitos académico y del derecho. Para responder a las preguntas sobre las perspectivas de los usuarios en cada uno de los países objeto de los estudios de caso, los investigadores examinaron los estudios académicos disponibles, los informes de los medios de comunicación y los foros de usuarios pertinentes. A continuación, los resultados de estos cuestionarios fueron analizados y depurados por los autores del estudio, que colaboraron con los investigadores en las tareas de aclarar y actualizar la investigación hasta julio de 2014.

2. LEGISLACIÓN Y REGULACIÓN

Al igual que las plataformas y servicios de Internet pueden utilizarse con fines legítimos como la expresión personal, la educación, el empleo y el comercio, también pueden emplearse con fines ilegítimos como el robo, el fraude, el acoso, la infracción de derechos de autor y la difamación. La línea que separa un fin legítimo de otro ilegítimo se ve influida de manera significativa por el contexto político, religioso y cultural, lo que da lugar a múltiples interpretaciones de tales fines en todo el mundo. Reconociendo tal tensión, sobre todo en el contexto de la expresión, la Declaración Universal de Derechos Humanos (DUDH), el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) y otros instrumentos internacionales de derechos humanos contemplan ciertas limitaciones al derecho a la libertad de expresión, protegiendo en todo caso la esencia del mismo. Como el antiguo Relator Especial La Rue subrayó en su informe de 2011, las restricciones solo son compatibles con las normas internacionales de derechos humanos cuando:

- se basan en normas, se contemplan en la legislación y se aplican de un modo transparente y predecible;
- son necesarias y proporcionales, sirviéndose del medio menos restrictivo para alcanzar el objetivo;
- son conformes con los fines citados en el PIDCP: necesidad de proteger los derechos o la reputación de otros, la seguridad nacional y el orden público, la salud o la moral públicas.

En 2011, el Comité de Derechos Humanos, en su Observación General nº. 34, determinó que las limitaciones concebidas para proteger la "moral pública" "han de entenderse en el contexto de la universalidad de los derechos humanos y el principio de no discriminación". Las restricciones aplicadas por intermediarios deben evaluarse con arreglo a lo dispuesto en estos estándares internacionales.

Aunque la norma sea la responsabilidad limitada y la autorregulación, existen excepciones en las que se hace responsables a los intermediarios por los contenidos de los usuarios que, en opinión de otros, infringen lo dispuesto sobre privacidad o difamación, o en otras leyes. En 2015, una sentencia confirmó tal responsabilidad en el asunto del Tribunal Europeo de Derechos Humanos de *Delfi* v. *Estonia* sobre difamación, y señaló que un portal de noticias debe ser consciente de sus contenidos en todo momento, y no limitarse a suprimirlos cuando el material en cuestión se somete a su atención. Los jueces discrepantes en este asunto señalaron que tal postura no difería mucho de la restricción anterior.

Cuando se atribuye tal responsabilidad a los intermediarios, las empresas se ven obligadas a efectuar sus propias tareas de seguimiento y filtrado para evitar posibles repercusiones. A su vez, esto contribuye a un proceso de controles previos a la publicación en el que algunos gobiernos se apoyan en las empresas del sector privado para regular los contenidos en línea, por fuera de todo proceso legal y rendición de

cuentas pública. Por otro lado, una genuina autorregulación en la que se toman como referencia las normas internacionales de derechos humanos puede servir en ocasiones para proteger la libertad de expresión y el respeto por las limitaciones normativas a la restricción, con arreglo a la DUDH y el PIDCP.

2.1 COMPROMISOS DEL ESTADO Y LIMITACIONES A LA EXPRESIÓN

Mientras que la tecnología, los modelos de negocio y el alcance de las actividades empresariales llevadas a cabo por los intermediarios de Internet han evolucionado drásticamente en las dos últimas décadas, los tipos de objetivos reguladores que persiguen los Estados se mantienen en buena medida inalterados, aún cuando los métodos utilizados para alcanzar tales objetivos sí han avanzado. En muchos casos, se debate la conformidad de las normativas de los Estados con las normas del PIDDP y la ejecución de estas. Aunque los distintos tipos de limitación deben ajustarse a los fines legítimos, a menudo no cumplen con las garantías de necesidad, proporcionalidad y proceso legal debido para su ejecución. La tendencia predominante consiste en que el exceso en las limitaciones ataña a la difamación delictiva, la seguridad nacional y pública, la incitación al odio, las elecciones, la protección de la infancia, la blasfemia y la propiedad intelectual.

Cuando las limitaciones son legítimas, siguen existiendo numerosas complejidades. Aunque el derecho a la privacidad se encuentre establecido, no se ha definido con exhaustividad, particularmente en la era digital. En este sentido, los límites a la expresión para proteger la privacidad pueden prestar una atención insuficiente a la necesidad de excepciones de interés público que den prioridad al derecho a saber de la población. Por otro lado, en el informe de 2012 de la UNESCO titulado *Global Survey of Internet Privacy* (Estudio global sobre el respeto de la privacidad en Internet) se concluye que las leyes sobre privacidad que solo procuran una protección débil pueden ejercer un efecto negativo en la libertad de expresión.

Otro ejemplo de dificultad en el equilibrio se observa en el caso de los agentes que pretenden coartar la libertad de expresión, con el fin de proteger la reputación de determinados ciudadanos, vinculado a su vez a una cierta noción de privacidad. Tal ejemplo viene a colación en la actualidad en la Unión Europea, dado el asunto de Google España v. AEPD, descrito sucintamente como un caso que establece un “derecho al olvido”, basado en “un derecho a dejar de figurar” en los motores de búsqueda en todos los países de esta área. Como se refiere más adelante en el presente capítulo, la resolución del Tribunal Europeo de Justicia de mayo de 2014 pone de relieve que el deseo de una persona de eliminar información negativa sobre sí mismo de Internet puede entrar en conflicto con el derecho de otros a recibir e impartir tal información. Críticos como el profesor de Harvard Jonathan Zittrain han propuesto un derecho de réplica como alternativa preferible para el equilibrio entre reputación y libertad de expresión.

Otro caso de equilibrio complejo atañe al modo en que puede garantizarse el derecho a la vida, la libertad y la seguridad de las personas preservando al mismo tiempo la esencia de los derechos a la privacidad y la libertad de expresión. Este caso ocupa un lugar central en los debates sobre la vigilancia digital. En 2014, la Alta Comisionada para los Derechos Humanos de la ONU instó a la reforma de las leyes sobre vigilancia, y aludió a las recomendaciones de la sociedad civil mundial respecto a la aplicación de los principios de "necesidad y proporcionalidad" combinados con una sólida rendición de cuentas, transparencia y mecanismos de reparación. Sin embargo, una encuesta entre expertos de 18 países efectuada en 2014 puso de relieve que la reforma en materia de vigilancia ha sido escasa. En muchos países, las nuevas leyes han seguido ampliando los poderes de la administración pública en esta materia. Se ha documentado que la vigilancia ejerce un efecto inhibidor en la libertad de expresión en diversas jurisdicciones.

2.2 RESPONSABILIDAD DE LOS INTERMEDIARIOS

Como se ha señalado anteriormente, un aspecto esencial del papel de los intermediarios en el fomento de la libertad de expresión es su responsabilidad legal, que atañe a su vez a la cuestión de lo que sucede cuando una persona utiliza un servicio intermediario para publicar, compartir o acceder a contenidos que infringen las leyes de un determinado país. La clave es la medida en que a los intermediarios se les puede o se les debe exigir responsabilidades legales por las actividades de sus usuarios. Las disposiciones sobre responsabilidad de los intermediarios formalizan las expectativas de la administración pública respecto al modo en que estos han de gestionar los contenidos o las comunicaciones de terceros. En muchas jurisdicciones, tales disposiciones jurídicas definen las circunstancias bajo las que los intermediarios pueden beneficiarse de una responsabilidad limitada, al establecer los criterios que estos deben seguir para eludir sanciones civiles o incluso penales en algunos casos por las acciones de los usuarios.

2.2.1 Modelos de responsabilidad de los intermediarios

Abundan los gobiernos en regiones como Europa, América del Norte, partes del sudeste de Asia y América Latina con leyes que abordan de manera específica la responsabilidad de los intermediarios. En otras regiones, y en particular en África, los gobiernos consideran actualmente la adopción de disposiciones legales al respecto. En términos generales, donde existen tales regímenes, se aplican tres modelos de responsabilidad de los intermediarios: responsabilidad estricta, responsabilidad condicional, e inmunidad amplia. Los requisitos y matices concretos de tales modelos varían de una jurisdicción a otra, los definen los gobiernos, y los tribunales se ocupan de ahondar en su aclaración. Algunos intermediarios cumplen de manera explícita los mandatos jurídicos relativos a su responsabilidad sirviéndose al efecto de la adopción de medidas como la autorregulación basada en la ejecución de sus condiciones de servicio.

- **Responsabilidad "global" o estricta**: el intermediario es responsable de los contenidos de terceros, aún cuando no tenga conciencia de que tales contenidos son ilegales (o ni siquiera que existen). La única manera de evitar la responsabilidad en tales circunstancias consiste en supervisar, filtrar y suprimir contenidos de modo proactivo y antes de su publicación si es probable que contravengan la legislación. Aún así, el seguimiento y la eliminación de contenidos no exime al intermediario de responsabilidad si un contenido infractor se pasa por alto. Los regímenes de responsabilidad global no distinguen entre intermediarios: todos, con independencia de su dimensión o función, son responsables.

- **Responsabilidad condicional**: el intermediario puede quedar exento de responsabilidad por el contenido de terceros si se cumplen ciertas condiciones, como la retirada del mismo tras su notificación ("notificación y retirada"), la comunicación al creador del contenido de la infracción tras la recepción de la notificación anterior ("notificación y comunicación"), o la desconexión de los infractores reiterados tras previo aviso. Si un intermediario incumple tales disposiciones, puede que deba asumir daños y perjuicios. A diferencia del modelo de "responsabilidad estricta", este modelo de responsabilidad limitada no obliga a los intermediarios al seguimiento y filtrado proactivo de contenidos para evitar responsabilidades. La variedad de "notificación y retirada" de la responsabilidad condicional se ha criticado al ser considerado susceptible de abusos; por otra parte, se afirma que facilita la autocensura al colocar al intermediario en una posición cuasijudicial y encargarle la evaluación de la legalidad de los contenidos. El modelo es aún más susceptible de abusos cuando carece de elementos de garantía procesal, como la oportunidad de recurrir una retirada de los contenidos. De hecho, el sistema de "notificación y retirada" incentiva que los intermediarios eliminen los contenidos de inmediato tras recibir una notificación, en lugar de invertir recursos en determinar la validez del requerimiento y correr el riesgo de tener que ir a juicio. Como consecuencia, ciertos contenidos legítimos pueden acabar siendo censurados.

- **Inmunidad amplia**: en este modelo, se exime al intermediario de responsabilidad respecto a diversos contenidos de terceros, sin distinguir entre funciones de los intermediarios, ni tipos de contenido.

Dado el papel fundamental que los intermediarios y las leyes que rigen su actividad desempeñan en la libertad de expresión en Internet, en los debates mantenidos a escala internacional se ha tendido a procurar el establecimiento de buenas prácticas y principios comunes. Por ejemplo, en diciembre de 2011, el Consejo de la OCDE incluyó la "responsabilidad limitada de los intermediarios" como uno de los 14 principios recomendados para la formulación de políticas de Internet, con el fin de "promover y proteger el libre flujo de información global en la Red". Tales principios hacen hincapié asimismo en la importancia de la transparencia, las garantías procesales, la rendición de cuentas y una formulación de políticas integradora y abordada por múltiples partes interesadas. Un consejo asesor compuesto por diversos grupos de la sociedad civil avaló tal recomendación.

Una tendencia emergente en la política en materia de responsabilidad de los intermediarios es su evolución hacia un mecanismo jurídico que permita a los gobiernos transponer sus propias interpretaciones de las limitaciones a la libertad de expresión a Internet, incluso más allá de las jurisdicciones nacionales. Dependiendo del contexto nacional, social e histórico, los gobiernos inciden en la restricción de diferentes tipos de contenido, y los intermediarios infractores pueden enfrentarse a acciones penales como la entrada en prisión, a sanciones civiles como la imposición de multas, o a una revocación de sus licencias de actividad. Las complejidades en este caso se asocian al lugar en el que se mantienen los contenidos, el emplazamiento de los autores, y la localización de la sede principal de los intermediarios.

2.2.2 Nota especial: Responsabilidad de los intermediarios en África

Aunque el uso de Internet crece a una enorme velocidad en los países en desarrollo, existen pocas disposiciones jurídicas relativas a la responsabilidad de los intermediarios en numerosas áreas de África. La ausencia de tales disposiciones genera una incertidumbre normativa y procesal. En un informe de 2014 a cargo de una ONG internacional con estatus consultivo con el Consejo Económico y social de la ONU, la Asociación para el Progreso de las Comunicaciones (APC) argumentaba que la falta de protección para los intermediarios en los países africanos hace que estos tomen la iniciativa en la restricción de los contenidos en sus redes y plataformas, dando lugar a lo que puede resultar una restricción indebida de la libertad de expresión de los usuarios.

Al mismo tiempo, muchos países africanos forman parte de la tendencia emergente a la creación de regímenes de responsabilidad de los intermediarios, en parte como respuesta a los enfoques de ciertos organismos internacionales e importantes socios comerciales y asistenciales respecto a la protección de los derechos de propiedad intelectual y la garantía de que los intermediarios tomen medidas contra los materiales que infringen derechos de autor en sus redes y plataformas. Respecto a los países que adoptan tales regímenes, los grupos de la sociedad civil a los que les atañe la libertad de expresión, como la APC, han manifestado su inquietud en cuanto a posibles elecciones de elementos específicos de los regímenes de otros países con el fin de establecer a su vez sistemas restrictivos y selectivos. Dado que la supervisión por parte de los intermediarios de posibles contenidos ilegales podría poner en peligro el derecho de los usuarios de Internet a la privacidad y la libertad de expresión, se considera que unas leyes consolidadas en materia de protección de datos y privacidad constituyen una importante salvaguarda para garantizar que no se abuse de los regímenes de responsabilidad de los intermediarios con fines de vigilancia o supervisión arbitrarios. De hecho, aunque la ausencia de tales regímenes menoscaba la libertad de expresión, la mera existencia de un régimen de esa índole no garantiza una protección más firme ni para los intermediarios, ni para la libertad de expresión en Internet en general. Además, las condiciones de servicio propias de los intermediarios pueden adaptarse de manera inadecuada a las normas sobre libertad de expresión. La competencia de los tribunales y la presencia de entidades capaces de defender las normas internacionales de derechos

humanos en Internet son clave para garantizar la protección de los intermediarios y la libertad de expresión en línea.

2.3 AUTORREGULACIÓN Y CORREGULACIÓN

Las leyes no son la única fuente de restricción de los contenidos en Internet: las normas privadas de una empresa, como sus "condiciones de servicio" también pueden coartar la libertad de expresión. En 2011, los cuatro relatores internacionales para la libertad de expresión han declarado que la autorregulación constituye una "herramienta efectiva para abordar la incitación al odio", que "debe promoverse". En algunas jurisdicciones, los sistemas de elaboración y aplicación de las normas sobre la expresión en Internet combinan elementos de autoridad pública y privada, dando lugar a mecanismos de ejecución basados en la autorregulación y en la corregulación. El ámbito de aplicación y el alcance de tales mecanismos lo conforman a su vez en gran medida los contextos jurídicos y normativos de los Estados. De este modo, existe una notable fluidez e interconexión entre la regulación pública y la privada. La tendencia predominante consiste en que los intermediarios de Internet utilicen en cierto grado la autorregulación y la ejecución privada de la normativa. Los marcos constitucional, jurídico y normativo específicos de una determinada jurisdicción y, en particular, su régimen de responsabilidad de los intermediarios, conforma a su vez el alcance y la naturaleza de los mecanismos de autorregulación y corregulación aplicados. Ya en 2003 la autorregulación y la corregulación se percibían de manera favorable. Así, en una declaración del Consejo de Europa se animaba a la adopción de la "la autorregulación o la corregulación de los contenidos difundidos en la Red" por parte de los países miembros. Si se pretende que tales sistemas no se utilicen con fines de censura, deberán gestionarse con arreglo a criterios y procesos conformes con las normas internacionales sobre libertad de expresión. El ecosistema de opciones puede desarrollarse como sigue:

- **Autorregulación de las empresas**: En lo que atañe a las empresas consideradas individualmente, se trata de actuaciones que van desde las medidas adoptadas por estas para bloquear o eliminar el spam o los virus, al establecimiento y la ejecución de las "condiciones de servicio", las normas que los usuarios deben convenir en respetar para utilizar el servicio. Las condiciones de servicio de una empresa pueden ser muy similares a los requisitos jurídicos y normativos, mientras que otras compañías prohíben contenidos que son legales, pero a los que consideran indeseables o incompatibles con el propósito o la naturaleza de su servicio. Dentro del marco jurídico de al menos una jurisdicción, a las empresas del sector privado se les suele permitir que elaboren sus propias condiciones respecto a lo que constituye un contenido "indeseable". No obstante, dado que los grandes intermediarios actúan en la práctica como espacios cuasipúblicos, algunos activistas han argumentado que estas empresas han de asumir la responsabilidad de evaluar las consecuencias de sus normas privadas para los derechos humanos, con el fin de reducir al mínimo el efecto negativo en los derechos de los usuarios, y que tal responsabilidad debería

conformar sus respectivas políticas y prácticas. Algunos gobiernos promueven activamente la autorregulación, o incluso presionan a las empresas privadas para que se autorregulen como alternativa a la legislación o la regulación formales, que resultan de manera inherente menos flexibles y, normalmente, más contundentes que los mecanismos privados.

- **Autorregulación colectiva**: un grupo de entidades privadas pueden crear de manera conjunta códigos de conducta sectoriales, o establecer normas técnicas comunes que todos los participantes convienen en respetar.

- **Corregulación**: una tendencia emergente de la autorregulación, sobre todo en la Unión Europea, se lleva a la práctica como alternativa a la acción reguladora tradicional. Se trata de un régimen normativo que conlleva la regulación privada y es promovido activamente, o incluso respaldado, por el Estado a través de la legislación, la financiación u otros medios de apoyo público o participación institucional, y que ha venido a denominarse "corregulación". Este modelo contempla un impulso de la asunción de responsabilidades respecto a las decisiones de los intermediarios de Internet. No obstante, también puede propiciar que estas empresas asuman un papel en el que sus decisiones se atengan a unas normas de menor alcance que los principios internacionales relativos a las limitaciones de la libertad de expresión y la privacidad.

En los tres estudios de caso del presente capítulo se examinan diversos modelos de autorregulación y corregulación. Los defensores de la autorregulación de las empresas argumentan que es preferible a la regulación de la administración pública porque la coordinación es más flexible y más efectiva, desalienta conductas legales, pero indeseables en el contexto del propósito de un determinado servicio, ayuda a los consumidores a evaluar y elegir entre productos y servicios, y puede aminorar los costes. Por su parte, los críticos advierten de que las frecuentes deficiencias de la autorregulación en lo que atañe a la rendición pública de cuentas y las garantías procesales pueden dar lugar a que se dejen de proteger valores democráticos y se desatiendan estándares básicos de la justicia.

2.4 PRESENTACIÓN DE LOS ESTUDIOS DE CASO

Una vez establecidas las cuestiones relativas al contexto jurídico y normativo, en los tres siguientes apartados se analizan los PSI, los motores de búsqueda y las redes sociales, y se examina la medida en que se respetan los derechos de las personas cuando su libertad de expresión depende de los intermediarios de Internet del sector privado. Los tres estudios de caso ilustran el modo en que la libertad de expresión de un usuario de Internet gira en torno a la relación entre las políticas y las prácticas de una empresa, la política de la administración pública y las cuestiones jurisdiccionales. Entre las preguntas clave figuran las siguientes: ¿en qué medida realizan las empresas esfuerzos concertados para respetar los derechos de los usuarios frente a los requerimientos de

la administración y los marcos jurídicos que no siempre son conformes con las normas internacionales de derechos humanos? ¿Cómo repercuten las condiciones de servicio privadas en la libertad de expresión? Además de las limitaciones de los contenidos, ¿en qué medida las prácticas de protección de datos y las políticas de privacidad de las empresas, combinadas con los requisitos de vigilancia de la administración pública, determinan si los usuarios pueden expresarse libremente o no?

Un mayor entendimiento de estas cuestiones por parte de todas las partes interesadas puede contribuir a fomentar la libertad de expresión en Internet, asistiendo a los gobiernos en la formulación de leyes que protejan los derechos en línea y facilitando el respeto de los intermediarios por los derechos de los usuarios; ayudando a las empresas a mejorar sus políticas y prácticas de promoción de la libertad de expresión a través de sus servicios; y asistiendo a la sociedad civil en la tarea de exigir responsabilidades a las administraciones públicas y las empresas.

3. ESTUDIO 1: PSI - VODAFONE, VIVO/TELEFÔNICA BRASIL, BHARTI AIRTEL Y SAFARICOM

3.1 INTRODUCCIÓN

Los PSI permiten que los usuarios accedan a Internet y utilicen la Red a través de una línea fija o de conexiones inalámbricas. Habilitan la transmisión de datos con origen o destino en otros intermediarios a través de sus redes. Los PSI pueden ser de titularidad pública, o encontrarse parcial o plenamente privatizados. Muchos los gestionan empresas cuya actividad original se centraba en los servicios telefónicos tradicionales y móviles previamente a la expansión y la adopción de servicios de Internet. Las empresas que actúan como PSI también pueden prestar otros servicios, como las llamadas de voz, el alojamiento web, la computación en la nube, el registro de nombres de dominio, el correo electrónico, y otros. El presente estudio de caso se centra en las funciones esenciales de un PSI como proveedor de acceso a Internet a través de servicios inalámbricos o de línea fija.

Como se señala en los Principios rectores del diálogo de la industria, las telecomunicaciones pueden favorecer la apertura y la transparencia, y atañen a los gobiernos en lo que se refiere a la protección de la seguridad pública. Los PSI desempeñan un papel fundamental en la tarea de facilitar el derecho a la libertad de expresión, dado que el acceso a Internet constituye un requisito previo para posibilitar el libre flujo de información en todo el mundo. Actúan como "guardianes" de Internet al disponer de acceso directo a las comunicaciones por voz o datos en sus redes, y de la capacidad técnica para restringir tales comunicaciones. Los PSI cuentan además con la capacidad para recabar, almacenar y acceder a los datos personales de los usuarios y el contenido de sus comunicaciones, así como a metadatos como las direcciones de IP, los datos del registro de llamadas y la ubicación. Pueden encontrarse con mandatos judiciales, e incluso injerencias extrajurídicas a través de presiones ejercidas por conductos no formales, para que proporcionen acceso a dicha información, así como con requerimientos judiciales para que faciliten actividades de seguimiento y vigilancia en tiempo real. Por tales motivos, las funciones de los PSI a nivel de red pueden afectar a la libertad de expresión de los usuarios en otros servicios de los intermediarios, como los motores de búsqueda y las plataformas de redes sociales.

Los modelos de negocio de los PSI suelen exigir la inversión de un volumen sustancial de equipos, recursos humanos e infraestructuras físicas en las jurisdicciones en las que actúan ellos, o los proveedores de servicios de telecomunicación. En este sentido, sus políticas y prácticas con influencia en la libertad de expresión se ajustan mejor al contexto político y jurídico de una jurisdicción que las de otros tipos de intermediario como los

motores de búsqueda o las plataformas de redes sociales fuera de su jurisdicción de origen. En cualquier caso, las PSI sí que ejercen control sobre diversas decisiones, políticas y prácticas empresariales que afectan a la libertad de expresión en Internet.

3.1.1 Las empresas

En el presente estudio de caso se examinan los siguientes PSI:

- **Vivo Telecommunications**, también conocida como Telefônica Brasil, inició sus actividades en 1993. En mayo de 2014, con 79 millones de abonados de telefonía móvil, Vivo, que ofrece servicios a estos usuarios, así como de banda ancha y cable, se había convertido en la mayor compañía de telecomunicaciones en Brasil,

- **Bharti Airtel** es una empresa multinacional de telecomunicaciones india constituida en 1995. Ofrece servicios de telefonía móvil 2G, 3G y 4G, comercio móvil, servicios de línea fija, banda ancha DSL de alta velocidad, IPTV, DTH y servicios a empresas, incluidos servicios de larga distancia nacionales e internacionales a empresas de transporte en 20 países. Airtel está catalogada como el cuarto mayor operador de telefonía móvil del mundo, con una base de clientes superior a los 200 millones de abonados.

- **Vodafone** es una empresa multinacional de telecomunicaciones con sede en el Reino Unido y constituida en 1991. Se trata del segundo mayor proveedor de telecomunicaciones del mundo, con una base de abonados de más de 430 millones de clientes y empresas de explotación en 21 países, además de empresas conjuntas como Safaricom en Kenya, a la que Vodafone denomina su “operador asociado local”.

- **Safaricom** es el mayor operador de telefonía móvil de Kenya, con 21 millones de abonados. Según Bloomberg Industries, en marzo de 2014, Safaricom contaba con el 67% del mercado de telefonía móvil kenyano, así como con el 79% del de tráfico de voz, y el 96% del de mensajes de texto. Su propiedad corresponde a Vodafone en un 40%; el Gobierno de Kenya posee el 35% y las acciones restantes se lanzaron en el Mercado de Valores de Nairobi en junio de 2008.

A continuación figura un resumen de las conclusiones generales de este estudio de caso, haciendo hincapié en las cuestiones de mayor alcance establecidas al considerar las experiencias de estas empresas.

3.2 RESTRICCIONES DIRECTAS A LA LIBERTAD DE EXPRESIÓN

Las restricciones aplicadas por los PSI se practican "al nivel de red" porque impiden o limitan el acceso de los usuarios a Internet en sí, o a determinados contenidos en línea, oportunidades de expresión o servicios ofrecidos por otros tipos de intermediario. Las restricciones a nivel de red empleadas por los PSI afectan a la naturaleza y el alcance de las restricciones aplicadas por otros intermediarios.

3.2.1 Filtrado a nivel de red

Los filtros son programas informáticos especializados que pueden restringir el acceso a sitios web completos, a determinados tipos de servicios en línea, páginas o contenidos específicos en algunos sitios, o páginas web que contienen ciertos términos clave. El filtrado impuesto por el Estado lo suelen llevar a cabo los PSI, y puede requerirse como una de las condiciones para que la empresa en cuestión obtenga la licencia de actividad en una jurisdicción. El Estado también puede instalar mecanismos de filtrado centralizados a través de puntos de intercambio de Internet que actúan como pasarelas para el tráfico en la Red entre diferentes jurisdicciones, y entre las redes gestionadas por distintos PSI. Instituciones privadas o locales como escuelas y bibliotecas pueden establecer filtros en sus propias redes locales para bloquear el acceso a ciertos contenidos. Los filtros también pueden instalarse en los hogares, muy habitualmente por padres que tratan de controlar el contenido al que pueden acceder sus hijos. Dada la disponibilidad de filtros informáticos que los padres pueden controlar en sus redes domésticas propias, los expertos internacionales se han preguntado por qué debería exigirse legalmente a los PSI que filtren los contenidos. Para ciertos tipos de contenido, como los de incitación al odio, dotar a los usuarios de capacidades de alfabetización mediática e informacional, y la autorregulación, se perciben en ocasiones como opciones más propicias para defender la libertad de expresión que la regulación directa y la aplicación de medidas legales. En cualquier caso, se considera con preocupación la delegación de una excesiva capacidad de ejecución de actuaciones en los intermediarios privados. En los apartados que siguen se hace hincapié fundamentalmente en el filtrado exigido por el Estado y aplicado por los PSI, así como en otras modalidades de filtrado que tales proveedores pueden establecer para aplicar sus propias normas, o para participar en la autorregulación y la corregulación colectiva del sector.

Dependiendo del contexto jurídico, los PSI pueden recibir peticiones, recomendaciones y órdenes de filtrado de la administración pública, terceros privados y/o organizaciones reguladoras. Tales órdenes pueden comunicarse caso por caso directamente al PSI, o en forma de una "lista negra" general. Los PSI en ciertas jurisdicciones adoptan medidas de autorregulación o corregulación, entre las que figuran el examen de ciertos contenidos en sus redes con arreglo a sus estándares empresariales, así como la colaboración con líneas de asistencia directa y órganos reguladores y sectoriales para identificar contenidos infractores. Los PSI también pueden ofrecer a los usuarios la opción de aplicar filtros a

sus redes domésticas o de oficina. La libertad de expresión puede verse afectada a consecuencia del filtrado, de la ejecución práctica de este, y de la transparencia de la administración pública y las empresas respecto a cómo y por qué se efectúa el filtrado. La mayoría de las empresas incluyen en sus condiciones de servicio la prohibición de determinados tipos de contenido y actividades en sus redes. La especificidad varía, pero la tendencia predominante es al uso de términos generales para englobar un gran número de formas de contenido no permitidas.

Los PSI filtran una amplia gama de tipos de contenido en respuesta a las peticiones que se les formulan, de conformidad con la legislación y con arreglo a sus condiciones de servicio propias. En los países considerados en el presente estudio de caso, entre los tipos comunes de contenidos filtrados por los PSI conforme a órdenes de la Administración o mandatos judiciales figuran los materiales que se consideran infractores de derechos de autor, la pornografía, las imágenes de abusos a menores, las difamaciones, los casos de incitación al odio, las expresiones relacionadas con las elecciones, y los materiales sensibles en relación con la seguridad nacional. En general, los contratos de licencia y la legislación limitan en gran medida las opciones a disposición de los PSI para poner en cuestión los requerimientos de filtrado formulados por las administraciones públicas. Se incluyen aquí decisiones sobre: 1) cumplir o no una petición; 2) el tipo de notificación pública y explicación de la restricción ofrecidas por el proveedor de servicios; y 3) la pertinencia y la ocasión de suprimir los filtros aplicados a un determinado contenido. Unas leyes de excesivo alcance o aplicadas con escasa coherencia pueden dan lugar a una utilización igualmente poco coherente del filtrado en un país, así como al filtrado de sitios web completos en lugar de los contenidos infractores en tales sitios, en contradicción con el principio de necesidad y proporcionalidad. El filtrado excesivamente amplio se conoce asimismo como “filtrado colateral”, debido a los daños colaterales que puede infligir en la libertad de expresión.

Las iniciativas de autorregulación y corregulación que atañen a PSI varían en gran medida con arreglo al contexto nacional. Las medidas de autorregulación en forma de filtros “adecuados para las familias” ofrecidos por los PSI a los usuarios en sus conexiones personales pueden dar lugar al riesgo de que el proveedor de servicios desempeñe la función combinada de juez, jurado y policía: el PSI es responsable de determinar los criterios que deben incluirse en el filtro, de aplicar este, y de atender las quejas respecto a los sitios web catalogados erróneamente. En ocasiones, las medidas que comienzan

como regímenes de autorregulación pueden convertirse más adelante en regulación, o formalizarse en la legislación.

RECUADRO: Tendencia emergente: "Filtrado ascendente"

La práctica del "filtrado ascendente" por parte de los PSI puede menoscabar la libertad de expresión. Cuando las empresas comienzan a filtrar en una jurisdicción, otras jurisdicciones a las que presta servicio el proveedor pueden verse afectadas por tales prácticas. Tal es el resultado del "legado" de un filtro (u otro componente técnico) establecido en la red del PSI, lo que se conoce como "filtrado ascendente". La consecuencia es que el contenido considerado ilegal en una jurisdicción y restringido posteriormente seguirá restringiéndose en otra jurisdicción, en la que podría ser legal.

3.2.2 Interrupciones del servicio y restricción

En ocasiones, las administraciones públicas ordenan la interrupción de la red o la restricción de los servicios de Internet a escala regional o nacional, aludiendo a motivos relacionados con la prevención del terrorismo, el mantenimiento del orden público o la evitación de disturbios. La restricción puede afectar a toda la red, o a un servicio concreto. En muchas jurisdicciones, los PSI deben atenerse a tales órdenes, o corren el riesgo de recibir sanciones legales. También pueden restringir o suspender la red o un servicio para tareas de mantenimiento o por averías técnicas. El cierre de toda una red o la restricción de un servicio en un área extensa constituye un golpe de gran alcance que repercute en todos los contenidos, a riesgo de incumplir los principios de proporcionalidad y necesidad reconocidos internacionalmente. Pueden adoptarse asimismo otras medidas de alcance más limitado, como las órdenes de la administración pública o de los PSI para dar por finalizado o suspender el acceso de un determinado usuario a Internet o a servicios de telefonía móvil. Las empresas de telecomunicaciones móviles también reciben órdenes de la administración exigiéndoles que envíen mensajes a través de sus redes que pueden inhibir la libertad de expresión, sobre todo si los mensajes no se emiten en nombre de la administración pública, porque tales medidas dan lugar a la transmisión forzosa de cierta información a los usuarios, aún cuando no restrinjan la información.

En general, los PSI solo restringen la red en su totalidad para su mantenimiento, o por motivos ajenos a su control, pero sí suspenden o eliminan más a menudo cuentas de usuarios. Las circunstancias respecto al momento en que el servicio o la red podrían verse afectados con arreglo a la política de la empresa difieren. Todos los PSI se reservan el derecho a dar por terminado, suspender o moderar el servicio por el abuso de este o la infracción de los plazos y condiciones de la empresa. Los PSI se enfrentan a decisiones difíciles respecto al modo de cumplir con sus obligaciones, y de comunicar tal cumplimiento al público.

3.2.3 Neutralidad de la red

La "neutralidad de la red" es el principio con arreglo al cuál, los PSI deben tratar todos los datos equitativamente, sin priorizar datos o servicios por ningún motivo, incluidos los de índole comercial o política. La neutralidad de la red es importante para la libertad de expresión, porque preserva la capacidad de elección de las personas y su derecho a acceder a los contenidos, aplicaciones, servicios y equipos de Internet. Los PSI disponen de acceso a tecnologías que les permiten analizar, bloquear o ralentizar contenidos y servicios. Estas prácticas, que se derivan de motivos económicos, regulación de la banda ancha, y restricción de los contenidos, pueden poner en peligro la neutralidad de la red. Los expertos recomiendan una mayor transparencia por parte de las empresas en cuanto al modo de funcionamiento de sus servicios de banda ancha, a los tipos de actividades de gestión de redes en las que participan, y al modo en que tales actividades podrían afectar a los clientes. En todas las jurisdicciones, gobiernos y reguladores se afanan por comprender el modo y la pertinencia de proteger la neutralidad de la red mediante la ley, y qué responsabilidad deben asumir las empresas en la tarea de garantizar tal neutralidad. A pesar de una tendencia emergente de las jurisdicciones a la propuesta de legislación, siguen existiendo varias brechas en la regulación en torno a la neutralidad de la red. En este sentido, las prácticas varían de una empresa a otra. La polémica ha surgido en los casos en los que se aplica una "tasa cero" a cierto servicio o paquete de contenidos, en el sentido de que no se exigen costes de conectividad, como en el caso de la iniciativa "internet.org" de Facebook. El argumento a favor de tales opciones consiste en que la provisión de libre acceso a una parte (subvencionada) de Internet es mejor que nada. De un modo u otro, hay cuestiones relativas a la libertad de expresión y el derecho a la información que es necesario considerar.

3.3 PRIVACIDAD

Los proveedores de servicio disponen de acceso a una extensa información acerca de sus abonados, incluidos metadatos y contenidos de comunicaciones. De acuerdo con el informe de 2014 sobre "El derecho a la privacidad en la era digital" de la Alta Comisionada para los Derechos Humanos de la ONU, los proveedores de servicios de Internet deben adoptar una declaración de políticas explícita en la que se esboce su compromiso con el respeto de los derechos humanos en todas sus actividades", y "han de establecer asimismo políticas de diligencia debida apropiadas para identificar, evaluar, prevenir y atenuar todo efecto adverso". Asimismo, en el informe se sostiene que "incluso la mera posibilidad de que la información de las comunicaciones se capture genera una injerencia en la privacidad, con un efecto inhibidor potencial en los derechos, incluidos los de libertad de expresión y de asociación".

Únicamente algunas de las empresas investigadas en este estudio de caso publican políticas de privacidad aplicables a los servicios específicos que se ofrecen a escala local, o explican con claridad y exhaustividad qué datos de los usuarios recogen, durante

cuánto tiempo los utilizan, y qué hacen con ellos. A pesar de los mandatos jurídicos en numerosas jurisdicciones en los que se definen los plazos durante los que deben conservarse los datos, las empresas estudiadas no especifican en sus condiciones de servicio o políticas de privacidad el período de tiempo exacto durante el que conservan los datos. En la mayoría de los países analizados, los requisitos jurídicos obligan a los usuarios a presentar una identificación emitida por la administración pública al suscribir los servicios. Tales requisitos suelen aplicarse a los servicios tanto de pospago, como de prepago, y difieren de la solicitud de información personal a los usuarios por parte de los PSI para la realización de transacciones comerciales. Algunas jurisdicciones obligan legalmente a los PSI a verificar esta información antes de prestar servicio al usuario. Esta práctica reduce en gran medida el margen para la participación anónima en Internet, ya que la conducta de los usuarios en línea no solo puede ser objeto de seguimiento, sino que también puede vincularse a su identidad real sin las protecciones de la privacidad que otorgan las normas internacionales que cubren las limitaciones legítimas de derechos.

3.4 TRANSPARENCIA

En su informe de 2012 titulado *Opening the Lines: A Call for Transparency from Governments and Telecommunications Companies* (Apertura de líneas de comunicación: Una llamada a la transparencia de los gobiernos y las compañías de telecomunicaciones), la GNI recomienda que los PSI y los gobiernos sean transparentes respecto a la legislación aplicable y las licencias de actividad, las peticiones de contenidos y metadatos de los usuarios por parte de la administración pública, y los requerimientos de esta respecto al filtrado y los mensajes de texto enviados a través de la red de los PSI sin atribución. La transparencia respecto a leyes, políticas, prácticas, decisiones, argumentos y resultados en lo que atañe a la privacidad y las restricciones a la libertad de expresión permiten a los usuarios adoptar decisiones fundadas sobre sus propias acciones y expresión en Internet. Por tanto, la transparencia es importante para la capacidad de los usuarios de ejercer sus derechos a la privacidad y la libertad de expresión.

La práctica y el alcance de la transparencia por parte de las empresas y la administración pública respecto a las tareas de vigilancia, filtrado y restricciones del servicio varían entre jurisdicciones. En ninguno de los países estudiados se exige por ley a los PSI que sean transparentes respecto a su política o su práctica de filtrado, las restricciones del servicio, o las medidas de vigilancia. Para los PSI y los servicios de telecomunicaciones, la capacidad de actuar de manera transparente con los clientes y los usuarios depende enormemente de que el propio gobierno sea transparente o no, y también de si los marcos jurídicos permiten unos niveles significativos de transparencia por parte de las empresas. En las jurisdicciones estudiadas, existe escasa transparencia de la administración pública respecto a la naturaleza y el volumen de peticiones oficiales dirigidas a los PSI en materia de filtrado o restricción del servicio. Las administraciones no ofrecen resúmenes ni estadísticas oficiales sobre el número y el tipo de órdenes de restricción que emiten. En ocasiones, reconocen las restricciones o responden a las acusaciones de restricción

en los medios de comunicación, o a las consultas de otras ramas de la administración pública, aunque tales casos no son habituales ni sistemáticos. La tendencia predominante de los PSI examinados en este caso es a una falta de transparencia respecto a la medida en que llevan a cabo filtrados, a las políticas en esta materia, y a la explicación de los requisitos jurídicos al respecto. Algunas leyes no prohíben explícitamente a los PSI que revelen información sobre vigilancia y filtrado, pero cuando se les piden aclaraciones, las autoridades realizan declaraciones que entran en conflicto con las prácticas existentes.

3.5 REPARACIÓN

En el caso de los PSI en las jurisdicciones examinadas en este estudio, puede ofrecerse una reparación potencial a los usuarios a título individual, o a todo un grupo de ellos, cuyo derecho a la libertad de expresión se haya conculcado. La reparación puede comprender una investigación, un informe o explicación públicos, la restitución del contenido o de la conexión, o la dotación de medios alternativos que permitan a los usuarios expresarse. Así, los juzgados o tribunales, las empresas y los órganos reguladores pueden ocuparse de la reparación. La forma de reparación a disposición de los usuarios depende de la jurisdicción de estos y de la empresa. Los mecanismos de reclamación y resolución de conflictos pueden complementar los sistemas de compensación y reparación proporcionados por la administración pública, o servir como alternativa a los mismos. Algunas administraciones exigen que las empresas instituyan mecanismos privados de queja y reparación, y la obtención de esta a través de los tribunales puede llevar mucho tiempo y resultar caro en muchos países. Se han llevado a cabo escasos estudios internacionales en lo que atañe a las buenas prácticas de los órganos de protección del consumidor en el tratamiento de los casos relacionados con las telecomunicaciones.

3.6 CONCLUSIONES

Los PSI desempeñan un papel fundamental en la conexión de los usuarios con un inmenso caudal de conocimientos, oportunidades y posibilidad de expresión. Sin embargo, en opinión de algunos usuarios, las empresas han de esforzarse más para proteger la libertad de expresión. Empresas como Vodafone han señalado que oponerse a los requerimientos de la administración pública puede suponerles un riesgo elevado en cuanto a su actividad empresarial y la seguridad de sus empleados locales. Por otro lado, en ocasiones, el cumplimiento pueden dar lugar a que las empresas corran el riesgo de minar la confianza de sus usuarios.

Pueden extraerse varias observaciones generales de los resultados de este estudio de caso:

- ***Las administraciones públicas y las empresas ofrecen una escasa, si no nula, transparencia respecto a las restricciones de la expresión aplicadas por los PSI, o a través de estos***. Se observa una tendencia predominante a una grave carencia de transparencia por parte de las administraciones y las empresas en diversas jurisdicciones, acerca de diversos aspectos básicos de las prácticas de filtrado. A raíz de las revelaciones de Edward Snowden en 2013, las iniciativas públicas de diálogo e investigación se han centrado en la transparencia respecto a la privacidad y las peticiones de vigilancia, y se ha hecho mucho menos hincapié en la transparencia de las prácticas que repercuten directamente en la libertad de expresión de los usuarios de Internet.

- ***En lo que se refiere a la vigilancia, la transparencia de la administración pública es limitada, y pocas empresas defienden los intereses de sus usuarios***. Dos países publican informes anuales en los que se revisa el alcance de la vigilancia por parte de la administración pública. Vodafone publica directrices de política inequívocas respecto al modo en que gestiona las peticiones de datos de los usuarios por parte de la administración, mientras que a los suscriptores de otros servicios no se les aclara cómo se protege su privacidad frente a las presiones de la administración pública o de otra índole. Tal incertidumbre se agrava por la falta de información sobre tales peticiones de datos de los usuarios. En 2014, Vodafone era la única empresa que refería el número de solicitudes de datos de los usuarios que recibía de agencias públicas. Se requiere un volumen significativo de información sobre los usuarios, aunque no se facilitan cifras en cuanto al cumplimiento. Vodafone era asimismo la única empresa objeto de este estudio que reclamaba abiertamente una mayor transparencia de la administración y reformas jurídicas que le permitiesen informar con mayor detalle de las peticiones de vigilancia y datos de los usuarios.

- ***Las prácticas de las empresas en materia de protección de datos y privacidad varían enormemente, en un contexto en el que las leyes de protección de datos se encuentran en estado de transformación en todo el mundo***. Se observa una tendencia predominante a que la existencia de leyes de privacidad poco desarrolladas se acompañe de unas políticas menos consolidadas en dicha materia por parte de los PSI. En los países con una legislación más débil o incipiente, los PSI revelan mucha menos información acerca de sus prácticas en materia de privacidad.

- ***Resulta difícil para los particulares exigir responsabilidades a las empresas y las administraciones públicas por las acciones emprendidas a través de los PSI que restringen la libertad de expresión de los usuarios de un modo incompatible con las normas internacionales de derechos humanos***. En algunas jurisdicciones, los reguladores del sector pueden ofrecer vías para que los usuarios tengan la posibilidad de denunciar la existencia de contenidos infractores, o las prácticas de los PSI que conculquen sus derechos. No obstante, la compensación por las infracciones cometidas por los PSI o las agencias públicas respecto a la libertad de expresión de los usuarios se han circunscrito a sanciones económicas, lo que pone de relieve que el reconocimiento y las consecuencias de tales infracciones son limitados.

- ***Los compromisos públicos asumidos por algunas empresas con los principios de los derechos humanos constituyen un primer paso importante, pero queda mucho camino por recorrer***. Como se ha indicado anteriormente, en 2013, un grupo de operadores y proveedores de telecomunicaciones, incluidos PSI, pusieron en marcha el Diálogo de la industria de las telecomunicaciones: Principios sobre libertad de expresión y privacidad, con un conjunto de "principios rectores" influido por los Principios Rectores sobre las empresas y los derechos humanos de las Naciones Unidas. Vodafone y Telefónica figuraron entre los nueve miembros del Diálogo de la industria (DI), y sus informes de 2014 se presentan en el sitio web del DI como resultado del compromiso de estas empresas con la provisión anual de información sobre "los progresos realizados en la aplicación de los principios y, cuando proceda, sobre los principales eventos que se produzcan al respecto".

El Diálogo de la industria ha señalado que aborda el estudio colectivo de las buenas prácticas en materia de transparencia empresarial en su sector, así como "el modo de implementar mecanismos de reclamación de nivel operacional". Los miembros también han actuado colectivamente para colaborar con las administraciones públicas. Como se refiere en su primer informe anual, la intención del Diálogo de la industria es "seguir abogando por una mayor transparencia gubernamental respecto al uso y el alcance de la vigilancia de las comunicaciones, y a las acciones cuyo efecto es la restricción del contenido de las comunicaciones, de conformidad con nuestros principios". El efecto concreto de tales actividades y compromisos empresariales en los usuarios de Internet no se ha estudiado aún de manera sistemática. En cualquier caso, las actividades de las empresas miembro del Diálogo de la industria hasta la fecha indican que la acción colectiva, combinada con una más amplia implicación de las partes interesadas, ha propiciado que los PSI adopten medidas que no habían estado dispuestos a adoptar previamente por iniciativa propia. El Diálogo de la industria no ha reconocido aún que ganaría aún más en términos de credibilidad mediante la adopción de un proceso de aseguramiento para verificar si las empresas aplican sus compromisos, como las evaluaciones de terceros llevadas a cabo por la GNI.

4. ESTUDIO 2: MOTORES DE BÚSQUEDA – GOOGLE, BAIDU Y YANDEX

4.1 INTRODUCCIÓN

Los **motores de búsqueda** constituyen una vía fundamental para que los usuarios de Internet encuentren información y accedan a la misma. Son importantes para la libertad de expresión, porque actúan como intermediarios entre aquellos que buscan información, y los que la publican en línea. A la mayoría de las páginas web no las indizan los motores de búsqueda y, por tanto, no pueden encontrarse en los resultados que ofrecen estos. Incluso Google, el motor de búsqueda de mayor dimensión y popularidad del mundo, ha indizado únicamente un pequeño porcentaje de las páginas web existentes. Existen tres razones principales de esta situación: a) las páginas web no se han encontrado aún, o no las pueden encontrar las "arañas" o robots de rastreo porque ningún otro sitio de Internet contiene vinculo a dichas páginas; b) resultan "invisibles" para las arañas porque los propietarios de las páginas web y las bases de datos en línea han optado por bloquearlas; c) la estructura de base de datos de la mayoría de sitios web "oculta" las páginas respecto a su descubrimiento por una araña externa.

Cada motor utiliza su propio algoritmo de búsqueda, una compleja fórmula matemática que decide qué resultados mostrar, y en qué orden, en respuesta a la consulta específica del usuario. Las decisiones del algoritmo respecto a lo que es más pertinentes para el usuario que realiza la búsqueda dependen en parte de los elementos en la URL de la página web, los titulares y otros contenidos. Los que desean que su contenido sea visualizado por grandes audiencias pueden "optimizar" sus sitios web, por ejemplo, para incorporar una versión dirigida a dispositivos móviles, o para maximizar la probabilidad de que su página figure entre los primeros resultados mostrados por el motor de búsqueda. Dos motores de búsqueda no generarán los mismos resultados, ni el mismo número de resultados para una misma consulta, salvo que sus logaritmos, arañas e índices sean idénticos.

En la libertad de expresión en relación con los motores de búsqueda intervienen tres posibles partes: 1) los usuarios que buscan información; 2) los creadores y operadores de los sitios web que están indizados por los motores, o podrían estarlo; y 3) los motores de búsqueda cuyos logaritmos han sido considerados por diversos expertos y la jurisprudencia reciente al respecto como una modalidad de proceso editorial, aunque no tan directo como el de un medio de comunicación. En este apartado se examina el modo en que las jurisdicciones conforman las políticas y las prácticas de los motores de búsqueda en relación con la restricción y la manipulación de contenidos, así como el grado de influencia de las leyes y reglamentos de otras jurisdicciones. También se analiza

la manera en que tres empresas diferentes con su sede principal en tres contextos nacionales muy distintos han abordado los retos relacionados con la libertad de expresión en Internet.

Las empresas

Este apartado se centra en tres motores de búsqueda gestionados por empresas que prestan otros servicios además de los de búsqueda:

Baidu domina en China, con una cuota de mercado situada entre el 60 y el 70% de la mayor base de usuarios de Internet en el mundo, con más de 600 millones.

Yandex cuenta con más del 60% de la cuota de mercado en la Federación Rusa, un país de 84,4 millones de usuarios de Internet.

Google es el principal motor de búsqueda en el mundo. Su cuota de mercado en los Estados Unidos (con unos 280 millones de usuarios de Internet) asciende al 67,5%. La cuota de mercado de Google es mucho mayor en los países en los que no existe un competidor local importante, con un 97% en India, y un 90% en Europa. En la Federación Rusa, tal cuota se sitúa en torno al 25%, y en menos del 2% en China.

Las cuestiones generales planteadas a raíz de este estudio de caso se presentan a continuación.

4.2 REPERCUSIÓN DEL FILTRADO DE REDES EN LOS MOTORES DE BÚSQUEDA

La libertad de expresión de los usuarios de motores de búsqueda puede verse afectada cuando estos son objeto de los filtros aplicados por PSI. Si se filtra la página inicial del motor de búsqueda, el servicio resulta plenamente inaccesible para los usuarios que acceden a Internet a través del PSI o la red nacional de que se trate. Los PSI también pueden filtrar únicamente determinadas páginas de resultados de los motores de búsqueda que contengan URL o términos clave concretos, haciendo que el servicio sea parcialmente utilizable, siempre que el usuario no busque contenido filtrado por el PSI.

Habitualmente, el operador del motor de búsqueda carece de control sobre el filtrado aplicado por los PSI, y no desempeña ningún papel en esa tarea. Sin embargo, la naturaleza y la medida del filtrado efectuado por los PSI en una jurisdicción dada afecta al modo en que los motores de búsqueda aplican a su vez sus propias restricciones. Así, previamente al análisis de las políticas, las prácticas y la ejecución de las restricciones por parte de los tres motores de búsqueda considerados, es necesario describir el alcance y la naturaleza del filtrado de tales motores por los PSI en cada país objeto del presente estudio de caso. En las cuatro jurisdicciones examinadas en dicho estudio, se observaron cuatro enfoques diferentes respecto al filtrado de los motores de búsqueda:

- Sin filtrado de motores de búsqueda
- Filtrado de sitios web, pero no de motores de búsqueda
- Filtrado limitado de motores de búsqueda
- Filtrado generalizado de motores de búsqueda con carácter internacional y desconexiones temporales para desalentar el uso.

4.3 MEDIDAS ADOPTADAS POR LOS MOTORES DE BÚSQUEDA

Los entornos jurídicos de las jurisdicciones de origen de las empresas conforman enormemente sus políticas y prácticas en materia de restricción de contenidos. En cualquier jurisdicción dada, los operadores de los motores de búsqueda pueden restringir o manipular los contenidos con arreglo a alguna o a la totalidad de las acciones que siguen:

1. supresión de páginas específicas, o incluso de sitios web completos, del índice del motor de búsqueda;
2. programar la araña para que no añada ciertas páginas, sitios web, o sitios que incluyen cierto contenido;
3. programar el algoritmo del motor de búsqueda para que no presente resultados para ciertas consultas;
4. programar el algoritmo para favorecer o "ponderar" ciertos tipos de páginas web por encima de otras;
5. influir en la interpretación del usuario de ciertos resultados de la búsqueda mediante la adición de notas explicativas, advertencias, o declaraciones en la publicidad adjunta a los resultados.

Como ocurre con los proveedores de servicios examinados en el estudio de caso anterior, los motores de búsqueda pueden restringir los contenidos a petición de una autoridad gubernamental u otra parte externa, o para hacer valer sus propias condiciones de servicio y otras normas o procedimientos privados.

4.3.1 Personalización

En 2005, Google comenzó a personalizar los resultados de las búsquedas para todos los usuarios con sesión iniciada, con arreglo a sus preferencias e intereses aparentes con arreglo a su historial de búsquedas. En 2009, la personalización se extendió a todas las búsquedas en Google, aunque el usuario no hubiese iniciado sesión, sobre la base de los registros de *cookies* del navegador. Los críticos han manifestado su preocupación por el efecto de la personalización en la libertad de expresión, ya que dota a un mismo sitio web de más o menos visibilidad respecto a diferentes usuarios dependiendo de

sus hábitos de navegación previos. La repercusión plena de la personalización en la libertad de expresión a escala mundial sigue sin aclararse. Algunos han argumentado que no se trata tanto del grado de personalización, sino de la medida en que el usuario puede comprender y controlar los factores que afectan a sus búsquedas. En un reciente estudio académico de las búsquedas en Google se observó que la personalización varía ampliamente en función de la consulta, y que es mucho menos medible en el caso de las consultas efectuadas en Google cuando no se ha iniciado sesión. En Baidu y Yandex también existe personalización.

4.3.2 Europa y el "derecho al olvido"

Aún cuando actúan en entornos jurídicos en los que la libertad de expresión es objeto de una firme protección, los motores de búsqueda no constituyen árbitros plenamente neutrales de la información. En todo el mundo se efectúan ajustes en el algoritmo de búsqueda con el fin de proteger a los usuarios del correo no deseado o *spam*, del *malware* y del robo de identidad, y a los menores de la explotación sexual, y de cumplir la legislación en materia de propiedad intelectual. Se llevan a cabo muchos más ajustes en respuesta a las peticiones privadas y de la administración pública en jurisdicciones específicas de todo el mundo. El papel de los motores de búsqueda actualmente se enfrenta a un nuevo conjunto de retos en Europa, y potencialmente en todo el mundo, con la resolución judicial que establece el "derecho al olvido" en toda la Unión Europea.

En un informe de la UNESCO de 2012, se hizo hincapié en las tensiones inherentes entre la privacidad y la libertad de expresión. Una de estas numerosas fuentes posibles de tensión se plantea entre el deseo del usuario de eliminar la información negativa sobre su persona de Internet, y el derecho de los demás a recibir e impartir información. El 13 de mayo de 2014, el Tribunal Europeo de Justicia falló en el asunto de Google España v. AEPD, iniciado contra Google por un ciudadano español que argumentó que una notificación de subasta de su vivienda embargada que figuraba en los resultados de búsqueda de Google constituía una violación de su derecho a la privacidad. De acuerdo con la resolución del Tribunal, a los usuarios de Internet en Europa les asiste ahora el derecho a exigir que los motores de búsqueda eliminen los vínculos a páginas web sobre su persona que resulten "inadecuados, no pertinentes y excesivos en relación con los fines del tratamiento". Por otra parte, el derecho de la persona a la privacidad se antepone, "como norma general", al interés del público en encontrar información. Al mismo tiempo, el interés público puede resultar preponderante, por ejemplo, en los casos de personalidades públicas.

La resolución se dictó bajo fuertes críticas de grupos defensores de la libertad de expresión como ARTICLE 19, el Comité para la Protección de Periodistas e Index on Censorship, que advirtió que el exceso en la aplicación de los derechos de privacidad puede incidir en la libertad de prensa. Esta postura es conforme con otra en la que se reconoce que la libertad de prensa consiste en el derecho a utilizar la libre expresión para comunicarse con el público en general, y que, aunque retirar los vínculos a determinados contenidos no infringe per se la expresión original, elimina gran parte de la relevancia de la edición

en la era digital. Otros defensores de los derechos digitales argumentan que la cobertura de los medios y la comunidad vinculada a la libertad de expresión sobrerreaccionaron, señalando que Google no borraba datos, sino que bloqueaba meramente los vínculos derivados de los resultados de las búsquedas. Por otra parte, a Google se le otorgó un notable poder discrecional respecto a la respuesta a cada peticiones, y no está obligada a retirar ningún resultado previamente a una resolución judicial al respecto.

A finales de mayo de 2014, Google presentó un marco rudimentario para el cumplimiento de la resolución, así como para cubrirse ante ulteriores casos basados en la misma. Creó un sitio web público en el que los usuarios residentes en Europa podían solicitar que su nombre se desvinculase de ciertos resultados de las búsquedas. Las supresiones solo se efectuarían en los sitios web de búsqueda de Google específicos de la Unión Europea, y los contenidos suprimidos se mantendrían visibles en el motor de búsqueda mundial, Google.com. La notificación de que tales supresiones habían tenido lugar aparecería en la página de resultados de la búsqueda.

Como miembro de la Global Network Initiative, Google abordó la necesidad de conciliar el cumplimiento de la resolución con sus compromisos de la GNI de actuar con transparencia respecto al modo en que se restringen los contenidos, así como de interpretar las peticiones oficiales relativas a tal restricción de la manera más rigurosa posible. El 11 de julio de 2014, Google refirió que había recibido 70.000 peticiones de restricción respecto a 250.000 sitios web desde mediados de mayo. Las peticiones se revisaban manualmente, y la empresa había instituido además una política de notificación a los sitios web cuando el vínculo a una de sus páginas se suprimía. El periódico *The Guardian* fue uno de los primeros medios de comunicación en recibir notificaciones respecto a la retirada de los vínculos a algunos de sus artículos de sus resultados de búsqueda en los Estados Unidos. Jimmy Wales, fundador de la Wikipedia, condenó este proceso tildándolo de "censura", después de que su organización recibiera la notificación de que varios vínculos a contenidos del sitio se habían eliminado en cumplimiento de las peticiones formuladas por las personas que eran objeto de dichos contenidos.

Google estableció además un consejo asesor encargado de investigar cómo debería equilibrarse la privacidad con la libertad de expresión. David Drummond, Primer Vicepresidente y Primer Ejecutivo de Asuntos Jurídicos, escribió que, aunque algunas de las peticiones eran claramente ilegítimas, como en el caso de los políticos que trataban de ocultar fechorías cometidas en el pasado, muchas otras resultaban comprensibles. En el tercer trimestre de 2014, la empresa llevó a cabo varias sesiones de consulta pública por toda Europa, y publicó un cuestionario en línea con el fin de recabar los comentarios de los interesados. Entre las preguntas del cuestionario figuraban las siguientes: ¿cuál es la naturaleza del derecho a la privacidad de una personalidad pública y cuáles son los límites de tal derecho? ¿Cómo deberíamos distinguir los contenidos de interés público de los que carecen de este? ¿Les asiste a los ciudadanos un derecho a la información sobre la naturaleza, el volumen y los resultados de las peticiones de supresión de contenido dirigidas a los motores de búsqueda?

Entretanto, tras la resolución, surgió una tendencia a la adopción de cambios similares en todo el mundo. Por ejemplo, los reguladores en materia de privacidad que asistieron al foro de las Asia Pacific Privacy Authorities (APPA, Autoridad sobre Privacidad e Asia y el Pacífico), celebrado en junio de 2014 en Corea, examinaron la posibilidad de "colaborar con Google y otros motores de búsqueda", y debatir posteriormente la cuestión en la siguiente reunión de las APPA, en diciembre de 2014. Las consecuencias de adoptar y aplicar normas similares en otras jurisdicciones comenzaron a ser objeto de debate. Este se suscitó igualmente a raíz de la declaración de un tribunal francés, que señaló que no bastaba con suprimir los contenidos únicamente en las versiones nacionales de su sitio (p. ej., Google.fr, Google.es), cuando Google.com, disponible en Europa, mantenía los vínculos correspondientes. El efecto en este caso podría consistir en bloquear el acceso a Google.com desde Europa, o que la propia empresa bloqueara la información designada en relación con las consultas procedentes de direcciones IP en Europa. Si la alternativa consistía en que el motor de búsqueda aplicara la resolución europea a las actividades en todo el mundo de Google.com, tal opción constituiría una extralimitación de una jurisdicción extraterritorial que no resultaría sostenible a escala global. Como se ha señalado anteriormente, una solución pendiente aún de consideración consiste en un mecanismo aplicado por los motores de búsqueda que hace posible un "derecho a la réplica" en lo que ataña a los vínculos que los usuarios consideren problemáticos.

Lo que puede indicar este caso en concreto, junto con el de *Delfi v. Estonia*, es una tendencia emergente de los tribunales a crear, en vez de a aplicar, políticas y precedentes, como resultado de la ausencia de políticas y leyes previas establecidas por autoridades públicas representativas en respuesta a la evolución tecnológica.

4.4 CONSERVACIÓN Y RECOGIDA DE DATOS Y VIGILANCIA

La conservación de datos de los usuarios por parte de los motores de búsqueda, combinada con un mayor conocimiento de las prácticas de vigilancia de la administración, parece haber repercutido en la confianza de la población en dichos motores. Con el análisis de los datos de tendencias (de búsqueda) de Google disponibles públicamente antes y después de junio de 2013 (cuando Edward Snowden comenzó a publicar sus revelaciones sobre la vigilancia practicada por los gobiernos a través de los intermediarios de Internet), se pretendió encontrar "pruebas empíricas de un efecto inhibidor en la disposición de los usuarios a utilizar términos de búsqueda [sensibles]". Se examinaron los datos de tráfico de búsquedas correspondientes a 282 términos en 11 países. Nueve países mostraron un descenso en el tráfico de búsquedas correspondiente a términos clasificados en la categoría de "susceptibles de acarrear problemas con el Gobierno de los Estados Unidos", y un aumento en el caso de los términos "no susceptibles de acarrear problemas". En los Estados Unidos, la magnitud de tal caída fue del 2,2%. Tales estudios indican que, al menos en algunas sociedades, la toma de conciencia respecto a la falta de privacidad y la existencia de cierto nivel de vigilancia generalizada puede

empezar a ejercer cierto efecto inhibidor en la libertad de expresión de los usuarios de motores de búsqueda. La preocupación por la recogida de datos a cargo de dichos motores ha propiciado un auge de alternativas que declaran abstenerse del seguimiento o el almacenamiento de los datos digitales de los usuarios.

4.5 TRANSPARENCIA

Los miembros de la Global Network Initiative se comprometen específicamente a "respetar y proteger la libertad de expresión de sus usuarios" en el curso de la respuesta a las peticiones de la administración pública respecto a la retirada de contenidos o la entrega de datos de los usuarios. Se obligan además a rendir cuentas en lo que se refiere al cumplimiento de tal compromiso. Existen dos componentes de la responsabilidad pública asumida por los miembros de la GNI: la "valoración y evaluación independientes" para determinar si las empresas se atienen o no a su compromiso con los principios de la GNI, y además, la "transparencia con el público". Dos años después del lanzamiento oficial de la GNI con tres empresas miembro en 2008, la práctica de lo que se ha venido a denominar "informes de transparencia" se convirtió en una tendencia emergente.

4.6 REPARACIÓN

Hay dos colectivos cuyos derechos a la libertad de expresión podrían verse afectados por los motores de búsqueda: los usuarios de Internet en general, y los creadores y operadores de los sitios web, incluidos aquellos que cuentan con blogs y sitios web personales, las organizaciones de la sociedad civil, y los medios de comunicación. Otras partes pueden tener motivos de queja, y formulan reclamaciones al respecto, en relación con otros derechos, como en el caso de los creadores de contenidos preocupados por los vínculos a sitios para compartir archivos que infringen la propiedad intelectual. En el presente apartado se incide en los mecanismos de reparación y reclamación relacionados únicamente con la libertad de expresión, y no en los que abordan otros derechos. Ninguno de los motores de búsqueda estudiados cuenta con mecanismos de queja, reclamación o reparación que puedan utilizar los usuarios de Internet que creen que su libertad de expresión se ha infringido debido al modo en que un determinado motor de búsqueda gestiona sus contenidos.

Google ofrece un mecanismo para que los propietarios de los sitios web recusen la retirada de enlaces a sus sitios web con arreglo a la Ley sobre derechos de autor en el milenio digital (DMCA por sus siglas en inglés) de los Estados Unidos. Desde que la empresa comenzó a aplicar la resolución europea del "derecho al olvido", Google ha restituido los enlaces a algunos artículos de noticias que se restringieron inicialmente. Con todo, el proceso de tramitación de los recursos de restitución es poco claro. Previamente al establecimiento del nuevo formulario web de Google sobre el "derecho al olvido" a raíz

de la resolución del Tribunal Europeo, ninguno de los motores de búsqueda estudiados había dispuesto mecanismos para que los usuarios procurasen una reparación si creían que los resultados de las búsquedas menoscababan sus derechos a la privacidad o relativos a su reputación. Mientras que los europeos han utilizado con éxito los juzgados para procurar reparaciones por las presuntas violaciones de su privacidad cometidas por motores de búsqueda, los demandantes no han cosechado tal éxito al utilizar los tribunales para obtener reparación por las restricciones aplicadas por los motores de búsqueda a los enlaces a sus sitios web.

4.7 CONCLUSIONES

Las políticas y prácticas de los motores de búsqueda en cuanto a la restricción y la manipulación de contenidos las conforman sus respectivas jurisdicciones de origen, y en diverso grado, las leyes y reglamentos de otras jurisdicciones. Sobre la base del análisis de las tres empresas con sede principal en tres contextos nacionales muy diferentes, las conclusiones fundamentales pueden resumirse como sigue:

- ***las diferencias en los regímenes de filtrado de los PSI ejercen una notable influencia en el modo en que los motores de búsqueda restringen sus propios resultados de búsqueda, y en la medida en que aplican tal restricción.***

- ***Cuanto más estricto sea el régimen de responsabilidades en una jurisdicción determinada, más probablemente se retirarán los contenidos, ya sea a iniciativa propia de la empresa, o previo requerimiento sin opción a la recusación.***

- ***Aunque la restricción de contenidos se aplica en los motores de búsqueda a petición de las autoridades, también se emplea por otros motivos en todas las jurisdicciones, incluso por razones que tales motores consideran que redundan en interés propio, de los usuarios, o del público en general***. Este hecho contradice una percepción pública generalizada de que los motores de búsqueda son árbitros neutrales de la información. Ha surgido cierto consenso entre las empresas y los defensores de la libertad de expresión respecto a las buenas prácticas por parte de los motores de búsqueda en la gestión de las demandas y las peticiones de retirada de contenidos formuladas por la administración pública desde el punto de vista de dicha libertad, como evidencian los principios y directrices de aplicación de la Global Network Initiative. No obstante, no existe un consenso claro entre las distintas partes interesadas respecto al modo en que los motores de búsqueda debe respetar la libertad de expresión en lo que se refiere al diseño algorítmico y otras restricciones de los contenidos no relacionadas con los requerimientos de la administración pública.

- ***La transparencia por parte de las empresas y de los gobiernos desempeña un papel esencial en el fomento de la confianza pública en las prácticas de los motores de búsqueda, y en la tarea de garantizar que la libertad de expresión no se restrinja por motivos ilegítimos o accidentales***. Existen diversos

ejemplos que ilustran por qué es importante que los gobiernos sean transparentes con sus ciudadanos respecto a las peticiones de restricción dirigidas a los motores de búsqueda, así como a las medidas de filtrado a nivel de red que repercuten directamente en los usuarios. Resulta igualmente importante que las empresas actúen de manera transparente con sus usuarios respecto a los contenidos que se suprimen a petición del gobierno o de terceros, y a las razones de tal supresión.

- ***La preocupación por la privacidad aumenta, pero solo una de las tres empresas estudiadas (Google) ha abordado tal inquietud de un modo público y sincero***. Muchos usuarios esperan que las empresas de las que se sirven para encontrar información, y para que se pueda encontrar sus contenidos propios, sean más francas en lo que se refiere a la información relacionada con los derechos. Se trata de disponer de tanta información sobre las prácticas de recogida, almacenamiento y puesta en común de datos como permita la ley, y de proteger los datos en la mayor medida posible, en el marco de las realidades de su respectivo contexto jurídico y político.

- ***La implicación de las partes interesadas, el compromiso con los principios, y los marcos de reparación son elementos importantes para los intermediarios mundiales en la tarea de abordar las tensiones entre la libertad de expresión y otros derechos, así como situaciones difíciles en materia de regulación***. El compromiso de Google con la GNI desde la puesta en marcha de la organización en 2008, y su contribución al desarrollo de los principios de la Iniciativa desde 2006, han reforzado la capacidad de la empresa para respetar la libertad de expresión y rebatir los requerimientos de los gobiernos que no considera conformes con las normas de derechos humanos. No obstante, en lo que se refiere a otras cuestiones relacionadas con la libertad de expresión y la privacidad y no vinculadas a tales requerimientos, no ha surgido aún un consenso entre los interlocutores globales respecto a un marco de principios.

5. ESTUDIO 3: PLATAFORMAS DE REDES SOCIALES – FACEBOOK, TWITTER, WEIBO, Y IWIW.HU

5.1 INTRODUCCIÓN

Las redes sociales en Internet desempeñan un papel esencial en el ámbito de la interacción social y la expresión, al ofrecer una plataforma que permite la democratización de la publicación de contenidos e información. Al posibilitar la puesta en común y la agregación de contenido generado por los usuarios, las redes sociales son percibidas por algunos como factores que transforman las audiencias en productores de información, proporcionando nuevas herramientas para la cohesión social y con el potencial para que los ciudadanos puedan exigir responsabilidades a los gobiernos. Las redes sociales, como la mayoría de empresas de Internet que ofrecen servicios gratuitos, obtienen sus beneficios de dirigir anuncios publicitarios a sus clientes. Las empresas terceras adquieren publicidad para aparecer en las redes sociales porque esperan que estos servicios puedan identificar compradores potenciales dentro de su base de usuarios mediante la recogida y el tratamiento de datos. Por tanto, los usuarios "pagan" por los servicios gratuitos que utilizan con su información personal y su privacidad. Las plataformas evolucionan a medida que desarrollan nuevas vías para que los usuarios creen y compartan datos. Las redes sociales han elevado asimismo la visibilidad y el alcance de algunos medios de comunicación tradicionales, por ejemplo, mediante el retuiteo de enlaces o la puesta en común de otros contenidos en línea, difundiendo así la información ampliamente y con mayor rapidez que los medios convencionales.

Muchos sistemas jurídicos consideran a las redes sociales como "alojadores de contenidos", porque los usuarios crean contenido en sus plataformas, y a los terceros se les permite publicar y compartir información. Dado que permiten que contenidos privados se compartan públicamente, las redes sociales desdibujan la línea que separa las esferas pública y privada, y plantean cuestiones en cuanto a las expectativas apropiadas respecto a la expresión en tales plataformas. Debido al alcance y la repercusión de la expresión generada por los usuarios y la actividad de estos en las redes sociales, para una empresa no resulta fácil encontrar un equilibrio entre el compromiso con la libertad de expresión, el cumplimiento de la legalidad, y las expectativas de los usuarios, con el deber fiduciario de las empresas de obtener beneficios. En el presente apartado se examinan las políticas y las prácticas de varias plataformas de redes sociales en diversos contextos nacionales. Se concluye que la capacidad de dichas plataformas para respetar la libertad de expresión de los usuarios depende en gran medida de los contextos jurídico y regulador nacionales, y en particular, del contexto del país de origen de la empresa. Al mismo tiempo, las empresas cuentan con numerosas opciones a su disposición

respecto al modo de gestionar y diseñar sus plataformas. Las elecciones que realizan ejercen un efecto fundamental en la libertad de expresión de los usuarios.

Empresas examinadas:

Facebook (www.facebook.com) es una red social con su sede principal en los Estados Unidos y fundada en 2004. En agosto de 2015, la empresa contaba con 1.490 millones de usuarios activos al mes, de los que un 83,1% se encontraban ubicados fuera de Norteamérica. Facebook permite a sus usuarios registrados mantener un perfil personal a través del cual pueden compartir información personal y de contacto, fotografías, artículos y ubicaciones; comunicarse con otros usuarios a través de mensajes privados o públicos; buscar e incorporar como "amigos" a otros usuarios, a los que pueden "etiquetar" en fotos o ubicaciones; e incorporarse a grupos e interactuar con otros miembros. Facebook se encuentra disponible en Internet, y mediante aplicaciones específicas en varios sistemas operativos móviles.

Twitter (www.twitter.com) es una plataforma de "microblogging" con sede en los Estados Unidos y fundada en 2006. En agosto de 2015 contaba con 316 millones de usuarios activos al mes, que envían 500 millones de mensajes ("tuits") al día. El 77% de los usuarios de Twitter residen fuera de los Estados Unidos. Twitter permite que los usuarios registrados intercambien mensajes de 140 (o menos) caracteres a través de su sitio web, aplicaciones móviles o SMS. Los usuarios pueden reenviar tales mensajes mediante su "retuiteo", además de buscar y "seguir" a otros usuarios. Las personas no registradas también pueden leer los tuits de los usuarios, siempre que estos mantengan su perfil público (configuración por defecto). Puede accederse a Twitter en Internet y a través de múltiples aplicaciones móviles. Los tuits pueden organizarse mediante etiquetas o *hashtags* (el signo de almohadilla o *hash* # seguido de un término o frase), lo que permite a los usuarios agrupar los mensajes relacionados. Si una etiqueta recibe un elevado volumen de "retuits", se alude a la misma como "trending". Twitter no "exige la utilización de un nombre real, ni la verificación del correo electrónico, ni la autenticación de la identidad".

Weibo (www.weibo.com) es una plataforma china de microblogging fundada en 2009, que se escindió de Sina previamente a la cotización oficial de sus acciones en los Estados Unidos en abril de 2014. En mayo de 2015 contaba con 198 millones de usuarios activos al mes. Los usuarios cuentan con perfiles personales, publican mensajes de 140 caracteres (denominados *weibo*, que significa "microblog" en chino), y comentan otros *weibo*, una función que proporciona "una manera sencilla para que los ciudadanos y las organizaciones chinas se expresen públicamente en tiempo real".

iWiW (anteriormente www.iwiw.hu, 'quién es quién internacional") es una red social húngara ya desaparecida que dio por finalizadas sus actividades en julio de 2014 debido a la reducción de su base de usuarios. Se fundó en abril de 2002 como wiw.hu ("quién es quién"), y pasó a denominarse iWiW en octubre de 2005, cuanto trato de expandirse, sin éxito, y comenzó a ofrecer su plataforma en numerosos idiomas. En abril de 2006 fue adquirida por T-Online, la unidad de negocio de Magyar Telekom y, en 2008, se fusionó

con Origo.hu. Hasta 2011 solo se podía acceder a esta red por invitación. En enero de 2013 contaba con 4,7 millones de usuarios registrados.

Las redes sociales son populares en todo el mundo, pero se utilizan de manera diferente en distintos contextos culturales y políticos. Facebook y Twitter son dos de las redes sociales más populares, con amplias bases de usuarios internacionales y, por tanto, un estudio de estos servicios pueden arrojar luz sobre las cuestiones de la libertad de expresión en un entorno transnacional. iWiW y Weibo son entidades de ámbito fundamentalmente nacional. Weibo resulta especialmente interesante porque el mercado chino de las redes sociales es altamente competitivo, aunque aislado de la competencia exterior. Se eligió a iWiW porque representaba un servicio de red social nacional compitiendo en un contexto lingüístico y cultural local contra competidores globales.

Se refiere a continuación la relevancia en términos generales del estudio de caso de estas empresas.

5.2 REPERCUSIÓN DEL FILTRADO DE PSI EN LAS PLATAFORMAS DE REDES SOCIALES

Los gobiernos pueden exigir a los PSI que filtren las plataformas de redes sociales mediante el bloqueo del acceso al sitio web en su conjunto, a determinados contenidos, grupos o páginas. Tal filtrado también puede efectuarse en los puntos de intercambio de Internet nacionales. Las empresas que gestionan plataformas de redes sociales carecen de control sobre las acciones que llevan a cabo los gobiernos y los PSI para proceder a su filtrado. Algunas redes sociales como Facebook, Twitter y Google han manifestado su oposición al filtrado a nivel de red en general. Sin embargo, las empresas sí ejercen control sobre sus condiciones de servicio y el modo en que responden a las peticiones de la administración pública o de otra índole para que retiren contenidos o desactiven cuentas en sus plataformas. Las decisiones de las empresas sobre tales restricciones en las plataformas pueden afectar a su vez a la decisión de los gobiernos de filtrar o no al nivel de red.

Los gobiernos optan por restringir o bloquear las redes sociales mediante el filtrado a nivel de red en determinadas circunstancias:

- ***Diferencias de las normas jurisdiccionales***: A diferencia de los PSI, las redes sociales no requieren una presencia física en un país para acceder a los usuarios del mismo. Sin embargo, algunos gobiernos emplean la amenaza del filtrado a nivel de red con el fin de obligar a las empresas internacionales a cumplir su legislación.
- ***En nombre del mantenimiento de la unidad o la seguridad nacionales.***
- Cuando se percibe una ***necesidad en tiempo real de controlar y mantener el orden público***.

5.3 SUPRESIÓN DE CONTENIDOS Y DESACTIVACIÓN DE CUENTAS

Aunque las plataformas de redes sociales pueden ser objeto de un filtrado a nivel de PSI sobre el que carecen de control directo, las redes sociales sí disponen de sus propios mecanismos para bloquear o restringir de otro modo los contenidos de los usuarios. Generalmente, exigen a los usuarios que creen una cuenta para poder compartir contenidos. Los operadores de las distintas plataformas pueden restringir los contenidos compartidos por sus usuarios en la plataforma de que se trate de varias maneras: bloqueando su acceso a los usuarios de determinadas jurisdicciones, o cerrando (desactivando) las cuentas de los usuarios que publiquen ciertos contenidos. Estas acciones pueden emprenderse como medidas de autorregulación para aplicar normas privadas, o en cumplimiento de los requerimientos del gobierno u otras entidades, o de otros requisitos legales como la respuesta a las órdenes judiciales en asuntos civiles. En algunos casos, los usuarios pueden ser sancionados por sus expresiones legítimas en Internet. La posibilidad de tener que asumir responsabilidades legales por parte de la red o del usuario puede dar lugar asimismo a la autocensura.

En el cuadro que sigue se ofrece una visión general de los diferentes modos en que se concreta la restricción de contenidos, de los motivos, y de las partes afectadas.

Cuadro 3: Factores clave que afectan a la restricción de contenidos por parte de las plataformas de redes sociales:

Motivo de la restricción:	¿El contenido infringe las condiciones de servicio?	Modos de aplicación:	¿a quién afecta?
• peticiones del gobierno	• posiblemente	• supresión completa del contenido en cuestión	• todos los usuarios
• peticiones con arreglo a la ley (p. ej., notificaciones de retirada de contenidos por infracción de derechos de autor, órdenes judiciales en asuntos civiles)	• posiblemente	• bloqueo del contenido en cuestión para un grupo de usuarios o una jurisdicción en concreto (el contenido sigue siendo accesible para otros)	• solo los usuarios en una determinada jurisdicción
• autorregulación a iniciativa propia (condiciones de servicio y otra aplicación de normas privadas)	• habitualmente	• filtrado automatizado (proactivo) de determinados tipos de contenidos preidentificados	• solo ciertos grupos de usuarios (p. ej., de edad)
• denuncia de los usuarios (respecto a la infracción de las condiciones de servicio por otros usuarios)	• habitualmente		

5.4 PRIVACIDAD

Las redes sociales constituyen auténticas "minas de oro" de información privada, en las que se revela de todo, desde las preferencias políticas, a la orientación sexual. Los usuarios confían de manera implícita a las redes sociales sus datos personales, y los gobiernos formulan peticiones de la información privada de los usuarios cuando llevan a cabo investigaciones civiles, penales e incluso de seguridad nacional. Todas las empresas examinadas aquí cuentan con políticas de privacidad de algún tipo, en las que se explica cómo se utiliza la información de los usuarios, pero tales políticas rara vez resultan claras y exhaustivas. Además, la configuración por defecto tiene consecuencias significativas en cuanto a la privacidad, ya que los seres humanos están sujetos al "sesgo por defecto" (tendencia a asumir sin más la configuración por defecto). Las empresas examinadas no ofrecen mucha información sobre la conservación de los datos.

En 2015, el Relator Especial de la ONU para la Promoción y Protección del Derecho a la Libertad de Opinión y de Expresión, y en 2014 la Alta Comisionada para los Derechos Humanos de la ONU, destacaron la importancia del anonimato, en cuanto a su vinculación con el derecho a la privacidad, para el ejercicio y la protección de los derechos humanos en la era de Internet. Muchas plataformas de redes sociales, pero no todas, exigen que sus usuarios se registren con su nombre real, y aplican estas políticas en diverso grado y de diferente manera.

5.5 TRANSPARENCIA

5.5.1 Transparencia respecto a las peticiones del gobierno y conformes a derecho

Tanto Facebook, como Twitter publican conjuntos de datos que han venido a denominarse "informes de transparencia".

En el "informe sobre solicitudes gubernamentales" de **Facebook** se informó por primera vez de la restricción de contenidos en abril de 2014. Facebook hace referencia únicamente al número de solicitudes gubernamentales que ha atendido, pero no informa de la cifra total de tales solicitudes recibidas. Tampoco incluye las órdenes judiciales ni las notificaciones de retirada de contenidos por infracción de derechos de autor en sus cifras. En el informe de transparencia de Facebook se detallan las solicitudes gubernamentales de datos de usuarios, incluida la información sobre tasas de cumplimiento y tipos de solicitud. No obstante, se proporciona únicamente información muy básica e incompleta sobre las peticiones de restricción de contenidos.

Twitter ha informado de las peticiones de supresión de contenidos desde su primer informe de transparencia en 2012. Además de lo que revela Facebook, en el informe de Twitter se incluye la tasa de cumplimiento, los contenidos suprimidos, y las notificaciones

de retirada de contenidos por infracción de derechos de autor. Twitter se distingue de Facebook al publicar las copias de las solicitudes de restricción y retirada de contenidos que recibe en el sitio web sobre "efectos inhibidores". En sus informes sobre solicitudes gubernamentales de datos, Twitter proporciona detalles de los tipos de petición y las tasas de cumplimiento, así como de la información facilitada a las autoridades en situaciones de emergencia.

Weibo no publica un informe de transparencia debido a restricciones jurídicas y, al parecer, los medios fuera de Internet y en línea rara vez mencionan las restricciones de contenido de ámbito estatal.

iWiW no publicó ningún tipo de informe de transparencia antes del cierre de sus actividades.

5.5.2 Transparencia sobre la autorregulación

Aunque Facebook y Twitter se han esforzado en potenciar la transparencia respecto al modo en que gestionan las peticiones de la administración pública y las solicitudes formuladas conforme a derecho, comparten mucha menos información con los usuarios o el público en general en cuanto a la manera en que aplican sus propias condiciones de servicio. Ninguna de las empresas estudiadas facilitan información sobre los contenidos que restringen con arreglo a la política de la empresa, ni estadísticas sobre denuncias externas de las infracciones de las normas de la compañía. Ninguna de estas empresas han publicado datos acerca del número, la fuente o el objeto de tales casos.

Aunque todas las redes sociales refieren los contenidos que prohíben, ninguna de las empresas examinadas proporcionó mucha información pública sobre los procedimientos de evaluación de contenidos. Fuentes del sector han descrito las normas y los procedimientos internos para evaluar contenidos en conversaciones con las partes interesadas, celebradas bajo la condición de no atribución, si bien tales procesos, en general, no se hacen públicos. El público en general suele tener conocimiento de ejemplos específicos a través de los casos a los que se alude en diversos artículos de medios de información.

5.5.3 Notificación a los usuarios

Las empresas no actúan de manera sistemática en cuanto a la tarea de informar a los usuarios de cuándo restringen sus contenidos o entregan los datos de estos. Si los contenidos se suprimen debido a una infracción de derechos de autor, tanto Twitter, como Facebook están obligadas legalmente conforme a la DMCA de los Estados Unidos a notificar lo sucedido al usuario, y a informar del modo de presentar un recurso. Por otra parte, ambas empresas se comprometen a informar a los usuarios de las ocasiones en las que se soliciten sus datos, salvo que la situación constituya una emergencia, o la empresa tenga prohibido por ley facilitar tal información.

En el caso de los contenidos que Facebook retira en aplicación de sus propias Normas comunitarias y Declaración de derechos y responsabilidades (DDR), la empresa se compromete a advertir a los usuarios, pero Twitter no aclara si actúa del mismo modo en el caso de los contenidos que infringen sus condiciones. Si atiende una petición de restricción de contenidos extranjera, Twitter notifica al público la restricción mediante una notificación de "tuit retenido", que también utiliza en los casos de retirada de contenidos por infracción de derechos de autor. Como se refirió anteriormente, Twitter solo restringe las cuentas en la jurisdicción cuyas autoridades hayan formulado una petición válida. Facebook muestra un mensaje más genérico, que reza "este contenido no se encuentra disponible actualmente", lo que puede tener muchos significados, y se desconoce cuál es el aplicable en cada situación concreta. Cuando se restringen contenidos en Weibo, a los demás usuarios que traten de acceder a la publicación se les notifica que el contenido en cuestión se ha suprimido, y se les dirige a un enlace para obtener más información. Los usuarios han denunciado que Weibo "camufla" los mensajes de manera que siguen siendo visibles únicamente para su autor, lo que da lugar a que algunos autores desconozcan que sus contenidos se han restringido.

5.6 REPARACIÓN

Ninguna de las empresas examinadas ofrecen una vía inequívoca para la reparación de los usuarios que se enfrentan a la retirada de imágenes o textos, o a restricciones funcionales, como la incapacidad para cargar fotos. Facebook puede retirar páginas por una presunta infracción de *spam*, pero los usuarios pueden recurrir. En el caso de las cuentas suspendidas, tanto Twitter, como Facebook ofrece una opción de recurso. Cuando se desactivan cuentas por infringir las condiciones de Facebook, los usuarios pueden enviar un recurso cumplimentado en un formulario específico al efecto. No existe información sobre el plazo que lleva la tramitación de una solicitud, en qué consiste el procedimiento de toma de decisiones, o la gravedad de las infracciones que dan lugar a una suspensión de cuenta. La página de información de Twitter también es breve a este respecto, pero ofrece una mayor explicación sobre el modo de recurrir. Una excepción es la que constituyen los derechos de autor, ya que la legislación de Estados Unidos al respecto exige que Twitter y Facebook notifiquen al usuario que publicó inicialmente el contenido, y que le informen de los recursos. No queda claro qué tipo de vías de reparación ofrecía iWiW, en su caso. **Weibo** no ofrece una opción directa de recurso ni un formulario web; en cambio, se anima a los usuarios a dirigirse a la empresa por correo electrónico e indicar si 1) no están de acuerdo con las medidas de los administradores; 2) no están satisfechos con las respuestas de los administradores tras la comunicación; y 3) tienen alguna duda respecto a otras cuestiones administrativas. En Weibo, la escasa información sobre medios de reparación ha dado lugar a la necesidad de depender en gran medida de datos anecdóticos. La restricción de contenidos para ser poco coherente.

5.7 CONCLUSIONES

En la interacción entre la política y la práctica de los intermediarios de las redes sociales y los contextos normativos y jurídicos nacionales específicos, las empresas se encuentran mejor capacitadas para maximizar el respeto por los derechos de los usuarios en las jurisdicciones donde las leyes son relativamente compatibles con las normas de derechos humanos internacionales en materia de libertad de expresión y privacidad. El contexto jurídico del país en el que se ubique la sede principal de la empresa resulta especialmente relevante para el respeto de los derechos de los usuarios. Las empresas de las redes sociales cuyos gobiernos no inhiben tales esfuerzos han avanzado de manera significativa en cuanto a la transparencia y la asunción de responsabilidades en el tratamiento de las peticiones de la administración pública. En cualquier caso, la libertad de expresión puede verse enormemente influida en una dirección positiva o negativa por las normas, procesos y mecanismos propios de las empresas respecto a asuntos entre los que figuran la aplicación de las condiciones de servicio, la privacidad de los usuarios, y la identidad. Las empresas son mucho menos transparentes y dispuestas a asumir responsabilidades con el público respecto a estas cuestiones.

El análisis de Facebook, Twitter, Weibo e iWiW apunta a las siguientes conclusiones:

- ***las acciones de los gobiernos contra los usuarios de redes sociales pueden limitar el espacio para la expresión.*** A los usuarios se les sanciona en ocasiones por su expresión en línea, y se exponen a este respecto a multas, o incluso a su detención. La falta de claridad respecto a qué expresión se permite, junto con unas políticas restrictivas, puede dar lugar a la autocensura. Las empresas que gestionan plataformas de redes sociales pueden ayudar siendo claras y transparentes sobre sus prácticas de restricción de contenidos, configuraciones de privacidad y políticas de intercambio de datos. También pueden asistir a los usuarios en los casos en los que las sanciones no son conformes con las normas internacionales de derechos humanos.

- Las redes sociales no atienden necesariamente todas las peticiones de supresión de contenidos; por ejemplo, Twitter solo ha atendido el 11% de tales peticiones, lo que pone de relieve que las ***redes sociales sí disponen de cierto margen de maniobra para recusar las solicitudes de restricción de contenidos***. Puede resultar más fácil resistir las presiones de los países distintos al de la jurisdicción de origen de la red, pero incluso en el país de origen, algunas empresas no cumplen todas las peticiones. De las cuatro redes sociales analizadas aquí, únicamente Twitter y Facebook publican sus criterios, si no el proceso efectivo, para tratar las peticiones de retirada de contenidos formuladas por gobiernos y/o terceros. Tales ***políticas publicadas ayudan a los usuarios a comprender en qué circunstancias pueden ser retirados sus contenidos a raíz de una petición externa, y pueden proporcionar a las empresas un marco más claro para rebatir las peticiones de retirada que no sean conformes con las garantías procesales o los derechos humanos internacionales***.

- ***Las redes sociales no actúan de manera sistemáticamente transparente respecto a las solicitudes de retirada de contenido formuladas por los gobiernos***. De las cuatro plataformas de redes sociales examinadas, solo Twitter y Facebook informan de las solicitudes gubernamentales, arrojan luz de manera relevante sobre el modo en que se aplica la ley a sus plataformas. Twitter comparte asimismo las peticiones de retirada de contenido en sí, cuando le resulta posible, con el sitio web sobre "efectos inhibidores", y notifica al público a través de mensajes en su plataforma los casos en los que se restringen contenidos con arreglo a una petición de la administración. En las distintas jurisdicciones, los gobiernos no son plenamente transparentes en cuanto a la naturaleza y el alcance de la restricción de contenidos y las solicitudes de datos de los usuarios.

- ***Algunas redes sociales no explican cómo comparten los datos de los usuarios con las autoridades y otros agentes.*** Facebook y Twitter han publicado directrices de política sobre el modo de responder a las solicitudes de datos de usuarios formuladas por órganos autorizados extranjeros y nacionales. A los usuarios de los otros servicios no se les informa del modo en que se protegerá su privacidad frente a las solicitudes formuladas por gobiernos u otros agentes.

- ***Ninguna de las empresas examinadas publica datos sobre las restricciones de autorregulación***, como, por ejemplo, cuántas cuentas se desactivaron por suplantación de personalidad, o cuántos infractores reincidentes fueron suspendidos. A medida que las redes sociales en Internet se convierten cada vez más en una plataforma fundamental para la expresión de los ciudadanos en línea, los usuarios y otras partes interesadas muestran un notable interés en la existencia de normas y procesos de ejecución de las mismas que resulten claros y predecibles y que, en cierto grado, se sometan a una supervisión independiente. La ausencia de tal rendición de cuentas socava la legitimidad de los intermediarios como plataformas para la libertad de expresión de los usuarios.

- Al disponer de un volumen significativo de información personal, ***las redes sociales asumen una especial responsabilidad con el respeto por el derecho de los usuarios a la privacidad***, lo que constituye un requisito para la expresión individual.

- ***La obligación de utilizar el "nombre real" puede ejercer un grave efecto inhibidor en la expresión, y requiere una ejecución flexible con el fin de evitar una repercusión negativa en la libertad de expresión de los usuarios.*** La mayoría de los gobiernos no requieren con arreglo a la legislación que las redes sociales verifiquen la identidad de sus usuarios. Las empresas pueden considerar las consecuencias para la privacidad y la libertad de expresión de aplicar una política de utilización del nombre real, llevando a cabo a tal efecto una evaluación de la repercusión en los derechos humanos.

- Los principios de la GNI en cuanto a libertad de expresión y privacidad, así como las directrices de aplicación que los acompañan, han constituido una fuente de sólida orientación para las empresas, y en términos más generales, los intermediarios de

Internet que forman parte de la Iniciativa. Las directrices de la GNI sobre transparencia y el proceso de atención de las peticiones gubernamentales, fundamentadas en las normas internacionales de derechos humanos, han repercutido en las prácticas empresariales de los tres tipos de intermediarios estudiados en el presente capítulo. Sin embargo, se observa una ausencia flagrante de principios, directrices y estándares similares respecto a las prácticas de autorregulación de las empresas, incluida la aplicación de las condiciones de servicio. Dada la falta de transparencia y coherencia en el modo en que las empresas aplican sus condiciones de servicio y otras normas privadas, y la repercusión de tal aplicación en la libertad de expresión de los usuarios de Internet, ***existe una clara necesidad de desarrollar directrices y estándares de "buenas prácticas" en materia de reparación y transparencia en la autorregulación de los intermediarios***.

6. GÉNERO

De los 81 países considerados en el Índice Web de 2013 de la Fundación World Wide Web, solo la mitad contaba con políticas nacionales para tratar la igualdad de género en Internet. Los autores del informe del Índice Web de 2013 destacan que la "falta de enfoque político y en las políticas la agrava el que no se recaben estadísticas desagregadas por género". Como consecuencia, "la manera en que el género afecta al acceso a Internet y el uso de la Red no se entiende bien aún". Para determinar la relación con las funciones de los intermediarios, conviene ofrecer una breve visión global de la cuestión del acceso básico a Internet para las mujeres respecto a los varones. A este análisis le sigue el examen de la manera en la que la restricción de contenidos en algunos países ha afectado al acceso de las mujeres a la información sobre salud y a la consideración de las cuestiones de género. En el último apartado se examinan los asuntos relacionados con el acoso dirigido a las mujeres, y cómo este afecta a la libertad de expresión de este colectivo en Internet, al inhibir su participación en la sociedad de la información digital.

6.1 ACCESO A INTERNET

El acceso a Internet ha capacitado a las mujeres, lo que les ha reportado beneficios económicos y una mayor igualdad de género. Sin embargo, a escala mundial, existe una brecha de género significativa en el acceso de banda ancha. Entre los factores que afectan a tal acceso en el caso de las mujeres figuran las desigualdades educativas y de renta, y estas son más acusadas en los países en desarrollo. Donde más repercute la falta de acceso y de una infraestructura de Internet es en las áreas rurales de renta baja, y a las mujeres con la mayor gravedad. Al mismo tiempo, se observa una tendencia creciente entre las mujeres a acceder a la Red a través de teléfonos inteligentes. Entre las intervenciones a través de políticas para superar la brecha de género figuran la ampliación del acceso a plataformas asequibles, la formulación de planes nacionales que permitan un aumento de la penetración de la banda ancha, y el tratamiento de las restricciones del mercado que repercuten en el carácter asequible de las plataformas de Internet.

6.2 GÉNERO Y RESTRICCIÓN DE CONTENIDOS

En algunos países, los defensores de los derechos de las mujeres han exigido restricciones más amplias sobre los contenidos pornográficos y "obscenos" en Internet, argumentando que existe una conexión entre la visualización en línea de tales materiales y la violencia ejercida contra las mujeres fuera de Internet. Algunas mujeres afirman que sus derechos se conculcan cuando los intermediarios se abstienen de restringir contenidos publicados

en la Red sin la intención expresa de infligirles daño. Sin embargo, la capacidad de las mujeres para acceder y difundir información e ideas sobre sexualidad puede verse reprimida asimismo por las restricciones, y cabe la posibilidad de que se apropien de la legislación entre cuyos objetivos figura la protección de la mujer para atender otros fines. Las empresas de Internet, incluidos los motores de búsqueda, no suelen restringir la información médica relacionada con las mujeres, pero el tratamiento de la desnudez femenina en las redes sociales ha sido objeto de una encendida polémica. Por otra parte, las leyes encaminadas a restringir la pornografía también se utilizan en algunos países para eliminar otros contenidos. Las empresas siguen afanándose por encontrar el equilibrio adecuado en relación con leyes de amplio alcance que puede ser objeto de una extensa gama de interpretaciones.

6.3 ACOSO POR RAZÓN DE SEXO

Debido a la facilidad con la que pueden cometerse actos de acoso y amenaza a través de las plataformas de las redes sociales, entre los que figuran el acecho, la incitación al odio, el "ciberacoso", el porno vengativo, la atención sexual no deseada y la coerción sexual, puede observarse una tendencia emergente en los debates sobre la responsabilidad de los intermediarios de ayudar a prevenir y abordar el acoso por razón de sexo en Internet. En el capítulo adjunto sobre la tarea de contrarrestar la incitación al odio en Internet figuran ejemplos a este respecto.

6.3.1 Regulación

Pueden apreciarse tendencias divergentes respecto a la legislación relativa al acoso sexual en Internet: algunos países han desarrollado leyes específicas, otros cuentan con disposiciones generales que podrían comprender la consideración del acoso sexual en línea, y otros carecen de legislación que aborde esta cuestión. Una categoría específica de acoso en línea que ha aparecido como tendencia emergente en los debates de los responsables de formulación de políticas y los defensores de los derechos de género es la del denominado "porno vengativo". Los infractores son a menudo ex cónyuges o ex novios resentidos, o "trolls" en línea que publican lo que la Conferencia Nacional de Legislaturas Estatales de los Estados Unidos ha definido como "fotografías o vídeos de desnudos o sexualmente explícitos en Internet publicados sin el consentimiento de los interesados, aún cuando la fotografía o el vídeo en cuestión se tomase con consentimiento". Desde 2014, al menos cinco países y 25 estados de los Estados Unidos han prohibido el porno vengativo, y varios otros han abordado esta cuestión a través del derecho de responsabilidad civil y penal, y de leyes contra la pornografía o sobre la privacidad.

6.3.2 Políticas y prácticas de intermediarios

Un tratamiento negativo en los medios y la presión ejercida por los grupos de la sociedad civil ha llevado a algunos intermediarios a tomar la iniciativa y adoptar mecanismos de prevención y respuesta al acoso sexual. No obstante, la capacidad de respuesta y la aplicación varían en función del grado de compromiso y consideración del asunto por parte de la empresa, de la presión pública, y de la ejecución de las disposiciones legales al respecto. En un estudio de 2014 en el que se examina el modo en que Facebook, Twitter y YouTube tratan la violencia contra las mujeres, la APC concluyó que, aunque los enfoques de las empresas respecto a la violencia contra las mujeres difieren, y las empresas "han dedicado algún esfuerzo a responder a las inquietudes de los usuarios", "no han hecho lo suficiente". En el informe de la APC se insta a los intermediarios de Internet a equilibrar su compromiso con la libertad de expresión con otros derechos humanos "como el de no ser víctima de actos de discriminación y violencia". Como se destaca en el informe, en ocasiones, las empresas plantean mecanismos para denunciar los abusos únicamente después de ser objeto de fuertes críticas públicas. Al mismo tiempo, al igual que las plataformas de las redes sociales constituyen espacios en los que hombres y mujeres se exponen al acoso sexual y por motivos de género, también hacen posible que los activistas luchen contra el acoso y promuevan la sensibilización respecto a estas cuestiones. En algunos casos, estas campañas han logrado concitar la atención nacional sobre los asuntos considerados, y han motivado un cambio político y de las políticas.

6.4 CONCLUSIÓN

En el apartado anterior se determinó que empresas de escala mundial como Twitter y Facebook actúan con mucha menor transparencia y disposición a asumir responsabilidades respecto al modo en que aplican sus condiciones de servicio, que en cuanto a la manera en que atienden las peticiones de la administración pública. El estudio de la APC citado en este apartado refuerza la necesidad de promover el diálogo y la comunicación con todas las partes interesadas acerca del modo en que las plataformas de las redes sociales desarrollan y exigen el cumplimiento de sus normas. Las empresas pueden colaborar más estrechamente con los usuarios, los defensores de los derechos humanos de toda índole y los gobiernos si el problema de la violencia de género en Internet debe abordarse de un modo que sostenga y proteja la libertad de expresión en la Red. De hecho, el problema de la violencia de género en Internet subraya la urgente necesidad de un proceso de múltiples partes interesadas encaminado a desarrollar principios, estándares y directrices de "buenas prácticas" respecto al modo en que las plataformas de redes sociales pueden comunicarse con los usuarios, y escucharles, en lo que se refiere al desarrollo y la ejecución de sus condiciones de servicio.

7. CONCLUSIONES GENERALES

Las conclusiones de este capítulo ponen de relieve los retos fundamentales para realizar el primer principio de la universalidad de Internet: los derechos humanos. Se basa en los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, con arreglo a los cuáles, los Estados tienen la obligación principal de proteger los derechos humanos, las empresas son responsables de respetarlos, y ambos deben desempeñar un papel en la provisión de mecanismos de reparación a aquellos cuyos derechos han sido violados. Los estudios de caso señalan las dificultades que afrontan los intermediarios de Internet para que se respete en la mayor medida posible el derecho de los usuarios a la libertad de expresión cuando los Estados no cumplen con su propio deber de protección. En los casos anteriores se destaca la manera en que todos los Estados disponen de margen para la mejora. Sin embargo, también está claro que los intermediarios de Internet cuentan con una capacidad considerable para influir en los resultados que afectan a la libertad de expresión de los usuarios de la Red, aún cuando el entorno jurídico y regulador no respalde plenamente la consecución de tal objetivo.

7.1 DEBER DE PROTEGER DEL ESTADO

Parte del deber del Estado de proteger los derechos humanos comprende la tarea de facilitar y sostener el respeto de los intermediarios por la libertad de expresión. Las conclusiones del presente capítulo ilustran cómo, en diverso grado, distintas políticas, leyes y normativas no se adecúan debidamente a ese aspecto particular de la obligación del Estado de proteger los derechos humanos. Entre las dificultades identificadas en los estudios de caso figuran las siguientes:

1. las características de los regímenes de responsabilidad de los intermediarios, o la ausencia de los mismos, así como los objetivos normativos de estos regímenes, afectan a la capacidad de los intermediarios para respetar la libertad de expresión. Limitar la responsabilidad de los intermediarios respecto a los contenidos publicados o transmitidos por terceros resulta fundamental para que prosperen los servicios de Internet que facilitan la expresión.

2. Las leyes, políticas y normativas que exigen a los intermediarios la restricción, el bloqueo y el filtrado de contenidos en numerosas jurisdicciones no son suficientemente compatibles con las normas internacionales de derechos humanos en materia de libertad de expresión.

3. Las leyes, políticas y prácticas relacionadas con la vigilancia a cargo del gobierno y la recogida de datos de los intermediarios, en caso de compatibilidad insuficiente con las normas de derechos humanos, minan la capacidad de los intermediarios para proteger adecuadamente la privacidad de los usuarios.

4. Los contratos de concesión de licencia pueden afectar a la capacidad de los intermediarios para respetar la libertad de expresión. Esto se aplica a los PSI en todos los países, y a las redes sociales y los motores de búsqueda, en algunos.

5. Aunque las garantías procesales exigen en general que la aplicación de la legislación y la toma de decisiones sean procesos transparentes y públicamente accesibles, los gobiernos se muestran con frecuencia opacos respecto a las peticiones a las empresas para la restricción de contenidos, a la entrega de datos de los usuarios, y a otros requisitos en materia de vigilancia. Esto dificulta que los ciudadanos puedan exigir las responsabilidades debidas a los gobiernos y las empresas cuando el derecho a la libertad de expresión de los usuarios se restringe indebidamente, ya sea de manera directa mediante la injerencia en los contenidos, o indirecta, al poner en peligro la privacidad de los usuarios.

7.2 RESPONSABILIDAD DE RESPETAR DE LAS EMPRESAS

Las políticas y prácticas propias de las empresas afectan a la libertad de expresión de los usuarios de Internet de manera tanto positiva, como negativa. En los estudios de caso se plantean las cuestiones de la aplicación de las condiciones de servicio, las políticas en materia de identidad, las prácticas sobre transparencia, la medida en la que las empresas están dispuestas o capacitadas para rebatir las peticiones de los gobiernos, y las políticas relacionadas con la privacidad y la conservación y la protección de datos. Entre las conclusiones principales figuran las siguientes:

1. A pesar de la reciente tendencia a la “elaboración de informes de transparencia”, el desempeño de las empresas es poco consistente en cuanto a lo que revelan y al modo en que se comunica la información. Por otra parte, las empresas actúan de manera poco transparente respecto al modo en que aplican sus condiciones de servicio y responden a las peticiones privadas.

2. Las empresas con políticas y prácticas inequívocas respecto a la gestión de las peticiones de restricción de contenidos ocupan una posición más sólida para rebatir las leyes y reglamentos locales que no se ajustan a las normas internacionales por limitaciones legítimas.

3. A menudo, las decisiones internas de las empresas de restringir ciertos tipos de contenido y aplicar sus propias normas privadas son acogidas favorablemente por los gobiernos como vía para tratar los problemas antes de que estos pasen a considerarse asuntos para los tribunales y la aplicación de la ley. Al mismo tiempo, los procesos internos de regulación y aplicación de la normativa carecen de transparencia o de mecanismos de supervisión independientes que contribuirían a garantizar que tales procesos se mantuvieran exentos de errores y abusos. Los usuarios en la mayoría de los países examinados refirieron incidentes en los que los

intermediarios adoptaron medidas contra determinados contenidos que no parecían infringir las condiciones establecidas, o en los que estas se aplicaban de una manera excesivamente lateral, dando lugar a un efecto negativo en la libertad de expresión y, a menudo, sin medios de recurso adecuados.

4. Las empresas en los tres estudios de caso recababan tipos de datos similares, aunque las políticas de conservación e intercambio con terceros diferían ampliamente, al igual que la medida en que las empresas informaban a los usuarios acerca de la existencia y el contenido de las políticas. La mayoría de las empresas no explicaron con claridad el modo en que gestionan las peticiones de datos de usuarios formuladas por los gobiernos, ni ofrecieron información sobre la cifra real de tales peticiones o el nivel de atención de las mismas. Aunque la legislación es un factor que contribuye a algunas de estas diferencias, los factores específicos de las empresas también influyen.

5. Que a los usuarios se les permita o no utilizar un servicio o crear una cuenta sin que esta se tenga que vincular a su identidad emitida por la administración, o sin la obligación de emplear su nombre real, repercute en la libertad de expresión de los usuarios en muchas de las jurisdicciones analizadas.

7.3 ACCESO A MEDIOS DE REPARACIÓN

La reparación constituye el tercer pilar esencial de los Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos, y atribuye a los gobiernos y las empresas la obligación de proporcionar acceso a los usuarios a una reparación efectiva. Se trata de un área en la que tanto los gobiernos, como las empresas tienen mucho margen para la mejora. Entre los distintos tipos de intermediario, jurisdicciones y modalidades de restricción, los usuarios cuyos contenidos o acceso para la publicación se restringe, y aquellos que desean acceder a tales contenidos, cuentan con medios poco coherentes, limitados o inefectivos para recurrir las decisiones de restricciones, ya sea en respuesta a órdenes de la administración, solicitudes de terceros, o con arreglo a la política de la empresa. Aunque algunas empresas han redoblado recientemente sus esfuerzos para proporcionar mecanismos de recurso y reclamación, y comunicar su existencia a los usuarios, las normas se aplican de manera poco coherente y sin garantías procesales.

7.4 MOTIVOS DE PREOCUPACIÓN

Las políticas y las prácticas de las empresas pueden combinarse con contextos jurisdiccionales para producir resultados que repercuten negativamente en la libertad de expresión. Se han planteado varias categorías comunes de dificultades:

- Una legislación de excesivo alcance y unos regímenes de responsabilidad rigurosos dan lugar a que los intermediarios se excedan en el cumplimiento de las solicitudes

gubernamentales, de un modo que pone en peligro el derecho de los usuarios a la libertad de expresión, o a que restrinjan los contenidos de manera generalizada en previsión de las peticiones de los gobiernos, aún cuando estas nunca se reciban, o los contenidos podrían considerarse legítimos en un juzgado nacional.

- Los intermediarios pueden someterse a diversas normativas jurídicas y, en ocasiones, corren el riesgo de que se les aplique una prohibición general por parte de autoridades en desacuerdo con un determinado contenido compartido a través de sus servicios. En ocasiones, los servicios de Internet resisten tales presiones mediante un estrechamiento de la cooperación con los gobiernos, el bloqueo de los contenidos únicamente en la jurisdicción de que se trate, o la supresión generalizada del contenido en cuestión.

- Las empresas optan por permitir o prohibir ciertos contenidos con arreglo a sus políticas internas, y también bajo la influencia de las obligaciones jurídicas que se derivan de resoluciones judiciales, órdenes de la Administración, demandas civiles, instrucciones de terceros, peticiones de grupos de seguimiento con los que coopera el intermediario, etc. Este sinnúmero de partes interesadas, agravado por la ambigüedad de los marcos jurídicos, da lugar a menudo a que quede poco claro para los usuarios individuales qué contenidos están permitidos, quién y cómo decide respecto a los contenidos autorizados, y las consecuencias potenciales de su expresión.

- La existencia y naturaleza de las políticas empresariales que se ocupan de la expresión en relación con el acoso sexual, la violencia de género y la explotación o la cosificación de las mujeres son desiguales. Esto se observa incluso en el mismo tipo de intermediario y la misma jurisdicción. En los tres estudios de caso, las empresas habían establecido mecanismos que permitían a los usuarios denunciar abusos relacionados con el género. Tales mecanismos pueden utilizarse con fines legítimos, como la denuncia de casos de acoso sexual, pero, a su vez, pueden emplearse en ocasiones en situaciones de extralimitación que ponen en peligro los derechos legítimos a la libertad de expresión de los usuarios.

7.5 INTERMEDIARIOS Y GOBERNANZA DE INTERNET

En 2005, el Grupo de trabajo sobre la gobernanza de Internet de la ONU definió la "gobernanza de Internet" como "el desarrollo y aplicación por parte de los gobiernos, el sector privado y la sociedad civil, en sus respectivos roles, de principios compartidos, normas, reglas, procedimientos en la toma de decisiones, y programas que moldean la evolución y uso de la Internet". Así, aunque el término "gobernanza de Internet" se utiliza a menudo en los medios de comunicación y los debates públicos en un sentido limitado para describir las funciones técnicas de formulación de políticas y coordinación de organizaciones como la Corporación de Asignación de Nombres y Números de Internet (ICANN por sus siglas en inglés), el concepto se formuló originalmente para

englobar un conjunto más amplio de procesos de determinación de políticas y prácticas que conforman el funcionamiento de Internet a todas las escalas. El papel de elaboración de políticas de los intermediarios de Internet (y las políticas que afectan a sus actividades) constituye una forma de gobernanza de Internet definida en términos generales. Por tanto, resulta útil situar las conclusiones del presente capítulo en el contexto de los debates mundiales sobre los principios de formulación de políticas de Internet que ejercen un efecto directo en los intermediarios.

El Foro para la Gobernanza de Internet (IGF) anual, cuya creación se encargó en la Agenda de Túnez para la Sociedad de la Información, constituye una plataforma para que las distintas partes interesadas debatan toda la gama de cuestiones que rodean a dicha gobernanza, aunque sin un mandato para establecer políticas. Se constituyeron varias "coaliciones dinámicas" para contribuir a los trabajos en curso relacionados con la sociedad de la información, dando lugar a la aparición en 2008 de la Internet Rights and Principles (IRP) Dynamic Coalition (Coalición Dinámica sobre los Derechos y Principios de Internet), integrada por numerosas partes interesadas. La Coalición IRP elaboró una Carta de Derechos Humanos y Principios de Internet, con un conjunto de diez principios fundamentales presentados en 2011, incluidos los principios de libertad de expresión y privacidad. La reunión de la IGF celebrada en septiembre de 2014 en Estambul asistió a la puesta en marcha de una nueva coalición dinámica sobre "responsabilidad de las plataformas", centrada en una categoría específica de intermediarios, a saber, las "redes sociales y otros servicios en línea interactivos", para debatir "soluciones concretas e interoperables para la protección de los derechos humanos de los usuarios de las plataformas". Esta nueva coalición dinámica cuenta con un potencial similar para contribuir a la formulación de normas para los servicios de redes sociales, motores de búsqueda y otros tipos de intermediarios que pueden definirse como "plataformas" de expresión. Podría actuar como centro de referencia para el desarrollo de unos principios más sólidos basados en los derechos humanos, y de mecanismos de rendición de cuentas respecto a diversas formas emergentes de autorregulación y corregulación.

8. RECOMENDACIONES

Las recomendaciones que siguen son aplicables en diverso grado a gobiernos, empresas, la sociedad civil, y organizaciones internacionales. Si se pretende respetar y proteger debidamente la libertad de expresión en Internet, todos estos agentes deben encontrar vías de colaboración entre fronteras para mejorar los marcos jurídicos y normativos, establecer y aplicar buenas prácticas empresariales, y fomentar la sensibilización y la participación entre los usuarios de Internet y los ciudadanos en general. La regulación y la aplicación de la ley en relación con la expresión en línea, con independencia de que las lleven a cabo los gobiernos o las empresas, han de ser compatibles con las normas internacionales de derechos humanos, y son procesos respecto a los que deben rendirse cuentas con arreglo a tales normas. Las recomendaciones que figuran a continuación se ofrecen como primeros pasos en esa dirección, con la esperanza de promover un debate ulterior y la generación de un mayor consenso internacional.

8.1 POLÍTICAS Y MARCOS JURÍDICOS ADECUADOS

Los objetivos de política, jurídicos y normativos que afectan a los intermediarios han de ser coherentes con las normas de los derechos humanos universales si se pretende que los Estados protejan la libertad de expresión en Internet, y que las empresas respeten esta en la mayor medida posible. Los gobiernos han de asegurarse de que se han adoptado marcos jurídicos y políticas para abordar las cuestiones que se deriven de la responsabilidad o la ausencia de responsabilidad de los intermediarios. Los marcos jurídicos y las políticas que afectan a la libertad de expresión y la privacidad deben adaptarse a los distintos contextos, sin transgredir normas universales, y han de ser conformes con las normas de derechos humanos, incluido el derecho a la libertad de expresión, y contener un compromiso con los principios de la garantía procesal y la equidad. Además, deben ser precisos y fundamentarse en un entendimiento claro de la tecnología de la que deben ocuparse, eliminando toda inseguridad jurídica que, de otro modo, brindaría una oportunidad al abuso o a que los intermediarios pudieran actuar de un modo que restrinja la libertad de expresión por miedo a las responsabilidades.

Con el fin de avanzar en la fundamentación de los procesos públicos y privados de formulación de políticas, se requieren muchos más estudios globales cualitativos y cuantitativos sobre la repercusión de las políticas y las prácticas empresariales, los modelos de negocio y las opciones de diseño en la libertad de expresión. Actualmente se carece de encuestas exhaustivas realizadas a usuarios de Internet en todo el mundo sobre el modo en que los intermediarios afectan a la libertad de expresión de las personas en diferentes contextos. También se requieren más estudios sobre el modo en que los marcos jurídico, normativo y de políticas afecta a la capacidad de los intermediarios para respetar los derechos de los usuarios, y sobre su efecto en los usuarios de Internet en términos más generales. Este capítulo constituye una mera aproximación inicial

en su examen del modo en que determinadas políticas y prácticas de las empresas afectan a la libertad de expresión en diferentes jurisdicciones. Se requiere información más detallada sobre la relación causaefecto entre políticas, prácticas y resultados. Tal información equipará mejor a todas las partes interesadas para optimizar y ajustar sus políticas, prácticas y estrategias de fomento de la protección y el respeto de los derechos de libertad de expresión de los usuarios de Internet en todo el mundo.

8.2 FORMULACIÓN DE POLÍTICAS POR MÚLTIPLES PARTES INTERESADAS

Las leyes, normativas y políticas de la administración, así como las políticas empresariales serán compatibles más probablemente con la libertad de expresión si se desarrollan en consulta con todas las partes afectadas y se tienen en cuenta sus intereses. En un auténtico proceso "multipartito" intervienen todas las partes interesadas a las que puede afectar la política en cuestión desde el comienzo, y no basta con recabar opiniones después de que se hayan establecido los parámetros básicos y se hayan determinado las directrices principales.

8.3 TRANSPARENCIA

La transparencia es importante para demostrar que las acciones en materia de gobernanza y aplicación de la legislación se atienen a principios, normas y condiciones especificados previamente. Una mayor transparencia por parte de los gobiernos respecto a las peticiones y los requerimientos que se dirigen a las empresas y pueden afectar la libertad de expresión y la privacidad de los usuarios constituye un prerrequisito para la rendición de cuentas en la gobernanza pública de Internet. La transparencia de las empresas también representa un prerrequisito para la rendición de cuentas en cuanto al modo en que los intermediarios responden a las peticiones de los gobiernos, así como a su propia "gobernanza" privada, lo que resulta necesario no solo para la protección de la libertad de expresión de los usuarios, sino también para la capacidad de las empresas para obtener y mantener la confianza del público en sus servicios.

En este contexto, se consideran dos tipos de transparencia: cualitativa y cuantitativa. La primera exige que los gobiernos pongan a disposición del público las leyes, las interpretaciones jurídicas, los procedimientos administrativos y otras medidas relacionadas con la restricción y la vigilancia de los contenidos. En el caso de las empresas, la transparencia cualitativa conlleva la comunicación con los usuarios sobre los procesos de respuesta a las peticiones del gobierno, y de aplicación de las normas y procesos internos de la compañía. La transparencia cuantitativa alude a la publicación de datos agregados acerca de las peticiones de los gobiernos y las tasas de cumplimiento, así como otros datos que ayudan a los usuarios de Internet a comprender qué tipos

de contenidos se eliminan, bajo qué auspicios, y por qué motivo. La GNI y el Centro para la Democracia y la Tecnología han formulado varias recomendaciones en materia de transparencia, dirigidas a los gobiernos y relativas a la restricción de contenidos. Se recomienda unas medidas de transparencia similares a los gobiernos en cuanto a la provisión de información cualitativa y cuantitativa sobre vigilancia. Las empresas podrían revelar información agregada sobre el número de peticiones de datos de los usuarios y de vigilancia en tiempo real que reciben, y acerca del modo en que responden a las mismas, al menos con una periodicidad anual. Los gobiernos podrían promulgar reformas legales que propicien claramente tal transparencia, y las empresas deberían estar en condiciones de revelar la existencia y los datos básicos de los requisitos técnicos de vigilancia que les impongan los gobiernos.

8.4 PRIVACIDAD

Proteger el derecho a la privacidad de los usuarios es fundamental para que prospere la libertad de expresión. Los intermediarios deben adoptar buenas prácticas en lo que respecta a la privacidad, y aplicar políticas claras y comprensibles sobre los datos de los usuarios que recaban y almacenan, el modo en que los gestionan, con quién los comparten, y bajo qué circunstancias pueden acceder las autoridades a tales datos. Tales políticas deben destacarse y ser de fácil acceso. En el caso de los gobiernos, sus políticas, reglamentos, leyes y prácticas de aplicación de estas que afecten a la privacidad de los usuarios, incluidas las que atañen a la recogida de datos y la vigilancia para la ejecución de las leyes, han de ser conformes con los principios esenciales de los derechos humanos. Los Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones, desarrollados por una coalición mundial de grupos de la sociedad civil entre finales de 2012 y mayo de 2014, recogen 13 principios a los que gobiernos y empresas pueden referirse para garantizar que la vigilancia de las comunicaciones se lleve a cabo de un modo acorde con las normas internacionales de derechos humanos.

8.5 EVALUACIÓN DE EFECTOS EN LOS DERECHOS HUMANOS

La protección de la libertad de expresión en Internet se reforzaría si los gobiernos llevaran a cabo evaluaciones de efectos en los derechos humanos para determinar el modo en que las leyes, reglamento o políticas propuestos pueden afectar a la libre expresión de los usuarios en Internet, y a su privacidad, tanto a escala nacional, como mundial, y publicaran los resultados de tales evaluaciones. Las empresas también pueden efectuar estos estudios para determinar la manera en que sus políticas, prácticas y operaciones afectan a la libertad de expresión de los usuarios de Internet, y adaptar sus actividades en consecuencia, adoptando estrategias de atenuación de los posibles daños identificados

en las evaluaciones. La mejor manera de fundamentar estos procesos de valoración es la implicación de las partes interesadas cuyos derechos de libertad de expresión corran el mayor riesgo en la Red, incluidos los medios de comunicación y los grupos de la sociedad civil capaces de representar tales intereses.

8.6 LA AUTORREGULACIÓN DEBE SOMETERSE A LOS PRINCIPIOS DE GARANTÍA PROCESAL Y RENDICIÓN DE CUENTAS, Y SER CONFORME CON LAS NORMAS DE DERECHOS HUMANOS

Las legislaciones nacionales deben reforzar las garantías procesales y la adhesión a las normas internacionales de derechos humanos con el fin de proteger los derechos de los usuarios de Internet, si bien los principios rectores también son fundamentales para la legitimidad de los intermediarios como custodios de los contenidos en línea. Deben constituir un punto de referencia para los procesos de aplicación de las condiciones de servicio privadas. Esto es conforme con las normas internacionales que exigen que toda limitación de la libertad de expresión se especifique en la normativa y sea predecible, apartándose así de las de carácter arbitrario o retroactivo. La autorregulación debe atenerse además a los principios de necesidad, proporcionalidad y fin legítimo convenido internacionalmente. En el contexto de la creación de una experiencia segura para los usuarios, las restricciones de contenidos aplicadas por los intermediarios no solo han de ser tan reducidas como sea posible, sino también deben evitar el conflicto con principios fundamentales de los derechos humanos como la no discriminación, un elemento vinculado a la cuestión de la neutralidad de la red. Con el fin de identificar y atenuar los posibles efectos adversos en la libertad de expresión de los usuarios, los intermediarios pueden llevar a cabo evaluaciones de efectos en los derechos humanos en su sistema de autorregulación.

En 2014, la Internet Society propuso diversos principios y recomendaciones respecto a los procesos e instituciones autorreguladores, incluidas distintas vías específicas para que los mecanismos de autorregulación generen prácticas responsables y transparentes. Unas normas equilibradas y proporcionales, las garantías procesales y las salvaguardas judiciales son esenciales. Las revisiones periódicas deben incorporarse a tales sistemas.

8.7 REPARACIÓN

A los usuarios de Internet les asiste el derecho a una reparación efectiva cuando sus derechos los restrinjan o conculquen los intermediarios, los Estados, o una combinación de ambos. Ha de posibilitarse la formulación de quejas y la obtención de reparaciones de los intermediarios privados, así como de las autoridades públicas, incluidas las instituciones de derechos humanos de escala nacional. Al procurar la reparación por

restricciones o infracciones del derecho a la libertad de expresión en línea, a los usuarios de Internet no debe exigírseles necesariamente la puesta en marcha de acciones legales ante los tribunales. Las vías para lograr una reparación deben encontrarse públicamente disponibles, y ser conocidas, accesibles, asequibles y capaces de proporcionar una compensación apropiada.

Dependiendo del contexto nacional, los mecanismos de reclamación y reparación proporcionados por los Estados pueden incluir sistemas de compensación provistos por las autoridades encargadas de la protección de datos, las instituciones nacionales de derechos humanos, los procedimientos judiciales y las líneas de asistencia directa. Los mecanismos de reclamación y reparación dispuestos por los intermediarios privados y los regímenes reguladores privados han de proporcionar mecanismos para recibir y responder a las quejas formuladas por los usuarios de Internet, como una de las dimensiones de la autorregulación. Tales mecanismos han de ser accesibles, seguros y apropiados desde el punto de vista lingüístico y cultural. La cuestión de si un medio de reparación significativo se encuentra disponible para los usuarios cuyos derechos de libertad de expresión se han restringido o conculcado debe examinarse como parte de un proceso de evaluación de efectos en los derechos humanos que aplique la empresa. Dependiendo de la reclamación y del daño identificado, la reparación podría comprender, aunque no necesariamente, una compensación económica. Entre las medidas significativas de reparación pueden figurar asimismo el reconocimiento, la disculpa y el compromiso de abordar el problema en el futuro; someterse a una investigación independiente o una supervisión en curso; o la participación en entidades multipartitas de ámbito regional o sectorial con el fin de aclarar y atenuar la posible restricción o violación de los derechos de los usuarios.

8.8 EDUCACIÓN PÚBLICA E INFORMACIÓN, Y ALFABETIZACIÓN MEDIÁTICA E INFORMACIONAL

El concepto multidimensional de la alfabetización mediática e informacional comprende el conjunto de competencias que necesitan los ciudadanos para participar plenamente en las sociedades del conocimiento. En su relación con los intermediarios de Internet, los ciudadanos requieren diversas capacidades relacionadas con las cuestiones de la libertad de expresión. Las empresas y los gobiernos deben contribuir al fomento de tales competencias, de manera tanto formal, como informal. Los Estados tienen la obligación de proporcionar información accesible y clara al público, de manera que los usuarios de Internet puedan no solo comprender y ejercer efectivamente sus derechos, sino también reconocer cuándo se han restringido, conculcado o se ha interferido en su ejercicio de otro modo. Las restricciones estatales a la libertad de expresión no solo deben perseguir un fin legítimo y atenerse a la legislación sobre derechos humanos, sino que también han de darse a conocer claramente a los ciudadanos. La información pública debe incluir instrucciones concretas sobre los mecanismos oficiales de reclamación y reparación.

El respeto de los derechos de los usuarios de Internet por parte de los intermediarios privados exige asimismo la información y la comunicación con los primeros acerca de sus derechos, del modo en que su expresión puede restringirse con arreglo a las condiciones de servicio del intermediario, los motivos de tales restricciones y la razón por la que eran necesarias, y otra información requerida para adoptar una decisión fundada respecto a la posibilidad de utilizar o no el servicio. Conviene alentar e incentivar a las instituciones educativas para que incluyan la información sobre los derechos de los usuarios de Internet en sus planes de estudio en materia de derechos humanos, educación cívica y administración pública. Del mismo modo, es pertinente animar e incentivar a los medios de comunicación para que incluyan contenidos que contribuyan a promover el debate público fundado sobre los derechos de los usuarios de Internet, y las obligaciones de los Estados y las empresas de proteger y respetar tales derechos.

8.9 MECANISMOS GLOBALES DE RENDICIÓN DE CUENTAS

Tanto las empresas como los gobiernos pueden asumir compromisos con la ejecución de los principios esenciales de la libertad de expresión y la privacidad. En el entorno digital actual, conectado por redes de escala mundial, tales principios deben ejecutarse de un modo local y globalmente responsable. Otro enfoque respecto a la rendición de cuentas en el caso de las empresas se basa en la evaluación y la certificación a cargo de organizaciones multipartitas independientes. La GNI, una coalición integrada por un gran número de partes interesadas, exige a sus miembros que se sometan a evaluaciones periódicas, como parte de un mecanismo de rendición de cuentas para la adhesión a sus principios y sus directrices de ejecución, centrado en el modo en que las empresas gestionan las peticiones de la administración pública. No obstante, las directrices de ejecución y la evaluación de la GNI no incluyen actualmente cuestiones relativas a la privacidad de los consumidores, ni a la aplicación de las condiciones de servicio. Puede que sea necesario desarrollar otras organizaciones y mecanismos para mejorar la rendición de cuentas y la transparencia en estas áreas si la GIN no puede incluirlas en el futuro.

En cuanto a los Estados, un grupo de 27 gobiernos se han incorporado a la Freedom Online Coalition, en la que los países miembros convienen en colaborar para promover “la libertad de expresión, de asociación, y de reunión, así como la privacidad en Internet en todo el mundo”. En abril de 2014, los miembros de la coalición publicaron la Declaración de Tallin, un conjunto de “Recomendaciones para la libertad en Internet”. Se han constituido tres grupos de trabajo integrados por múltiples partes interesadas. La Coalición celebra una conferencia anual a la que se invita a representantes de empresas y de la sociedad civil. En cualquier caso, está por ver si surgirá algún mecanismo mediante el que los gobiernos puedan ser comparados con diversas referencias y se les puedan exigir responsabilidades por parte de distintos interlocutores mundiales respecto a la medida en que se hayan atenido a tales recomendaciones. Los intermediarios de

Internet se verán sometidos a fuertes presiones para que cumplan plenamente con su responsabilidad de respetar los derechos humanos, salvo que los gobiernos atiendan su propia obligación de proteger los derechos humanos, incluida la libertad de expresión y la privacidad en la Red.

9. CONCLUSIÓN

El presente capítulo se ha centrado en el papel de los tres tipos de intermediarios de Internet en cuanto al fomento de la libertad de expresión, prestando atención asimismo a los contextos normativo, jurídico y de políticas en los que desarrollan su actividad. Con la investigación no se pretende obtener una muestra representativa o estática de agentes, sino más bien extrapolar conceptos más generales. Se han identificado diversas tendencias, con un aumento general de la concienciación y las acciones emprendidas por los propios intermediarios y los gobiernos respecto a la relevancia de los PSI, los motores de búsqueda y las redes sociales para la libertad de expresión.

Con el análisis anterior se ha pretendido asistir a todas las partes interesadas, así como a los propios intermediarios, en la tarea de determinar el modo en que la capacidad de control inherente a la mediación de los contenidos de Internet puede optimizarse en lo que respecta a la libertad de expresión, así como al derecho a la privacidad. De esta manera, los intermediarios de Internet pueden contribuir a la evolución de las sociedades del conocimiento que, a su vez, resultan fundamentales para el fomento de la democracia, el desarrollo sostenible y la paz en todo el mundo.

VI. LA SEGURIDAD DE LOS PERIODISTAS

1. VISIÓN GENERAL

En este capítulo se examinan las tendencias recientes en el terreno de la seguridad de los periodistas, se presentan las estadísticas de la UNESCO correspondientes a 2013 y 2014, y se lleva a cabo un seguimiento de otras situaciones hasta agosto de 2015. Se emplea el marco del anterior informe de la UNESCO sobre *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios*, encargado por los Estados miembros en la Resolución 53 de la 36ª Conferencia General de la UNESCO, que cubrió el período anterior comprendido entre 2007 y mediados de 2013, y en concreto, los temas de la seguridad física, la impunidad, el encarcelamiento de periodistas, y una dimensión de género de las cuestiones[7]. Por otra parte, en el capítulo se examinan las tendencias recientes al refuerzo de las normativas internacionales, al desarrollo de mecanismos prácticos, la mejora de la cooperación entre organismos, la mayor colaboración con el sistema judicial y las fuerzas de seguridad, y la investigación.

En el presente capítulo se observa asimismo que la tasa de asesinatos de periodistas alcanzó un máximo en 2012, cuando la UNESCO registró 123 casos, y se ha producido un ligero descenso en los dos años posteriores. En cualquier caso, el número de periodistas asesinados sigue siendo muy elevado. A lo largo del período, una pequeña proporción de Estados miembros en los que se han producido asesinatos de periodistas han proporcionado una respuesta sobre la situación de la instrucción judicial de los casos. De los datos recibidos se deduce que la anterior tasa de impunidad se ha mantenido en un nivel elevado. Al mismo tiempo, han aumentado en gran medida la atención y las iniciativas de colaboración en materia de seguridad de los periodistas e impunidad a escala internacional, así como en ciertos países.

7 Véase UNESCO. 2015. Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios. París: UNESCO. http://unesdoc.unesco.org/images/0022/002270/227025e.pdf y Resolución 53, adoptada por la 46a sesión de la Conferencia General de la UNESCO en noviembre de 2011. Disponible en http://unesdoc.unesco.org/images/0021/002150/215084e.pdf.

2. SEGURIDAD FÍSICA

La UNESCO sigue siendo la agencia de la ONU con el mandato específico de defender la libertad de prensa y la libertad de expresión, y que se ocupa de genera mayor conciencia sobre los asesinatos de periodistas, trabajadores de los medios de comunicación y productores de medios victimizados como resultado de ejercer el periodismo[8]. Acabar con la impunidad de los delitos contra periodistas ha seguido siendo una parte importante de esta labor en 2013-2014. En este sentido, la Directora General de la UNESCO, mediante el mandato del Programa Internacional para el Desarrollo de la Comunicación (PIDCE) de la Organización, ha seguido condenando cada asesinato verificado durante el período revisado. Asimismo, ha continuado solicitando al Estado miembro en cuestión que facilite información voluntariamente sobre el seguimiento judicial de cada caso. Desde la resolución adoptada por el PIDCE en 2012[9], los Estados que contestan pueden indicar si desean que su respuesta se publique en la página web[10] de la UNESCO dedicada a esta cuestión, en la que se registran los asesinatos y figura la declaración de la Directora General.

En concreto, en 2013 y 2014, la Directora General de la UNESCO condenó públicamente los asesinatos de un total de 178 periodistas, trabajadores de los medios de comunicación y productores de medios sociales dedicados a actividades periodísticas

En 2013, la cifra ascendió a 91 fallecidos, reduciéndose en una cuarta parte respecto a 2012. No obstante, sigue siendo la segunda cifra más alta de periodistas asesinados desde 2006. Tras varios años de relativa calma en Iraq, el número de periodistas asesinados se elevó a 15 en este país en 2013, lo que lo convirtió en el más peligroso para dichos profesionales en ese año. Sin embargo, por comparación, el mayor y el segundo mayor número registrado de periodistas asesinados en Iraq correspondieron a las 33 muertes registradas en 2007, y las 29 de 2006.

En 2014, la Directora General emitió declaraciones públicas sobre ocho casos de asesinato de periodistas. El conflicto armado en curso en Siria ha seguido provocando estragos entre los periodistas, con diez asesinatos en 2014. En ese mismo año, en otras áreas[11], ocho periodistas fueron asesinados en Palestina, seis en Iraq, cinco en Libia y otros cinco en Afganistán. Siete periodistas perdieron la vida de este modo en Ucrania.

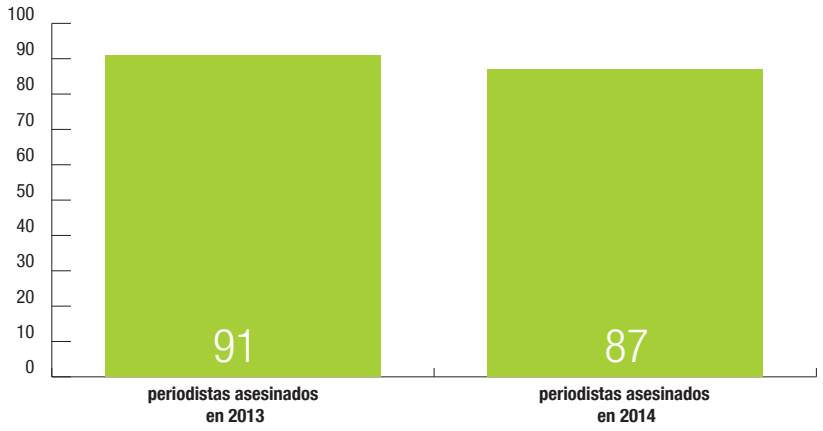
8 Véase la Resolución 196 EX/31 sobre seguridad de los periodistas y la cuestión de la impunidad adoptada en la 196ª Sesión del Consejo Ejecutivo de la UNESCO. Disponible en http://unesdoc.unesco. org/images/0023/002323/232337e.pdf.

9 La 28ª sesión del Consejo del PIDCE solicita a la Directora General "que ponga a disposición en el sitio web de la UNESCO, a petición de los Estados miembros interesados, la información facilitada oficialmente respecto a los asesinatos de periodistas condenados por la Organización".

10 Véase el sitio web dedicado "La UNESCO condena los asesinatos de periodistas en www.unesco.org/new/en/condemnation.

11 Se trata de áreas identificadas en el Informe de 2013 del Secretario General de la ONU sobre la protección de civiles en conflictos armados, que se remite al Consejo de Seguridad de Naciones Unidas cada 18 meses.

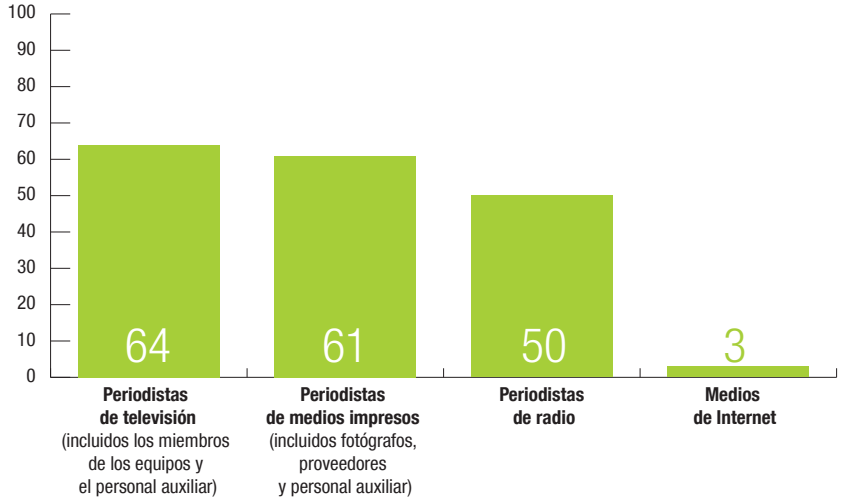
Número total de periodistas asesinados en 2013 y 2014



Como en años anteriores, la gran mayoría de periodistas asesinados residían en el país donde tuvo lugar el suceso. En 2013, siete de los 91 (8%) periodistas asesinados eran corresponsales extranjeros. En 2014, tal cifra experimentó un acusado aumento, hasta alcanzar cerca del 20% del total de fallecimientos (17 casos de 87). Doce de estos casos se produjeron en Siria y Ucrania

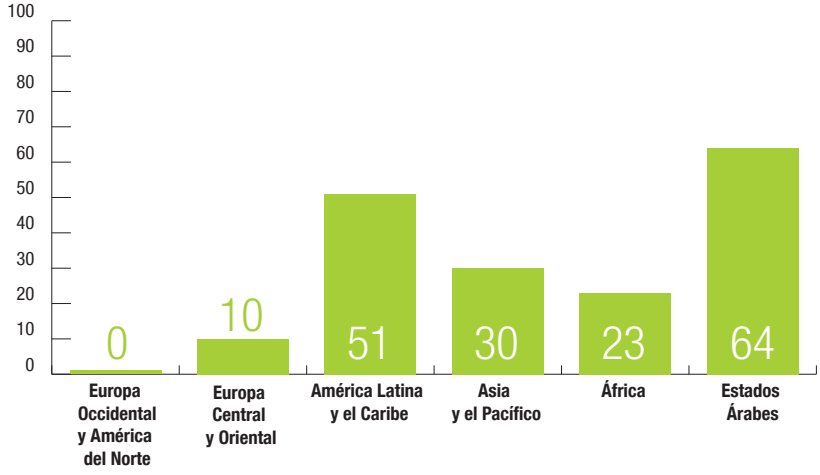
En cuanto al tipo de medio, los periodistas de televisión (incluidos los miembros de los equipos y el personal auxiliar) sufrieron la mayor pérdida, con 64 fallecidos en el período de 2013 y 2014. A estos les siguieron los miembros de los medios impresos (incluidos fotógrafos, proveedores y personal auxiliar), con 61 muertes. Los periodistas de radio asesinados ascendieron a 50. Tres periodistas que trabajaban fundamentalmente para medios de Internet fueron asesinados en el mismo período. Considerados conjuntamente, los "medios tradicionales" concentraron más del 98% de los fallecimientos de personas dedicadas a actividades periodísticas.

Periodistas asesinados por tipo de medio en el período 2013-2014



Desglosados por región, un total de 64 asesinatos de periodistas (36%) tuvo lugar en la región de los Estados Árabes, lo que la convirtió en el área más peligrosa para el trabajo de estos profesionales en 2013 y 2014. Un total de diez casos de asesinato de periodistas tuvo lugar en la región de Europa central y oriental, 23 se produjeron en la región africana, 30 en la de Asia y el Pacífico, y 51 en la de América Latina y el Caribe. No se registraron casos en la región de Europa occidental y América del Norte durante el período de dos años objeto de estudio[12].

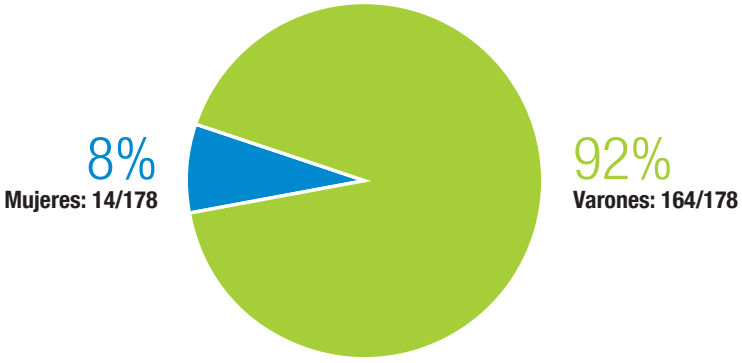
Cifra total de periodistas asesinados por región en el período 2013-2014



En el período considerado (2013 y 2014), la gran mayoría de los periodistas asesinados fueron varones. En concreto, 164 de los 178 periodistas que perdieron la vida por esta causa (92%).

12 El ataque a la revista francesa Charlie Hebdo se produjo justo después de dicho período.

Número de periodistas mujeres/varones asesinados en el período de 2013-2014



La seguridad digital de los periodistas, que también puede dar lugar a un peligro físico para estos y sus fuentes, comenzó a suponer un grave problema durante el período. Varias instituciones de los medios de comunicación sufrieron ataques en sus sitios web, intromisiones en sus comunicaciones electrónicas y la incautación de dispositivos digitales[13].

13 A estas actuaciones se hace referencia en las publicaciones de la UNESCO en 2015 *Building Digital Safety for Journalism: A Survey of Selected Issues, y Keystones to Foster Inclusive Knowledge Societies*, así como en el estudio realizado para la UNESCO por la Asociación Mundial de Periódicos sobre la protección de la confidencialidad de las fuentes en la era digital.

3. IMPUNIDAD

Una solicitud de información actualizada sobre la investigación y la instrucción judicial de los sucesivos asesinatos no resueltos de periodistas, condenados por la UNESCO, ha seguido enviándose cada año a los Estados miembros donde se producen tales fallecimientos. De los datos recibidos parece deducirse que la impunidad ha seguido constituyendo la tendencia predominante, y son pocos los autores de los asesinatos que son llevados ante la justicia.

La impunidad alude al efecto de la exención de castigo de aquellos que cometen un delito. Por tanto, apunta a un fallo potencial de los sistemas judiciales, así como a la creación de un entorno en el que los delitos contra la libertad de expresión quedan sin castigo. Estas características han seguido alimentando un círculo vicioso, y suponen una grave amenaza para la libertad de expresión. La práctica y la expectativa de la impunidad respecto a los casos de los periodistas tiene consecuencias para la impunidad en términos más generales. Los periodistas que trabajan sin miedo contribuyen a garantizar que otras violaciones de derechos no puedan ocultarse bajo un manto de oscuridad. Cuando los delitos contra periodistas continúan sin castigo, esta situación puede fomentar la violación de diversos derechos humanos, además del derecho a la libertad de expresión y a la libertad de prensa, así como otras formas de delincuencia. La eliminación de agentes, junto con los arrestos y detenciones arbitrarios, las desapariciones forzadas, el acoso y la intimidación, han seguido siendo tácticas que no solo silencian al periodismo, sino que también intimidan a la población para llevarla a practicar la autocensura.

En junio de 2012, el Relator Especial de la ONU para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión de la ONU[14] atribuyó las causas radicales de la impunidad a la falta de voluntad política para acometer las investigaciones, exacerbada por el temor a las represalias a manos de poderosas redes delictivas, a las deficiencias en el marco jurídico, el sistema judicial y los cuerpos policiales, a la falta de recursos, y a la negligencia y la corrupción.

En el más reciente Informe bienal del PIDCE del Director General sobre la seguridad de los periodistas y el peligro de la impunidad, publicado en 2014, se refiere que menos de uno de cada diez asesinatos de periodistas han dado lugar a una condena[15]. En el Informe se siguió instando a los Estados miembros a “informar al Director General de la UNESCO, con carácter voluntario, de las medidas adoptadas para evitar la impunidad de sus autores y comunicarle la situación de las investigaciones judiciales que se lleven a cabo sobre cada asesinato condenado por la UNESCO”.

14 El informe del Relator Especial de la ONU para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión (A/HRC/20/17) presentado ante la 20ª Sesión del Consejo de Derechos Humanos.

15 Este Informe se elabora con arreglo a las resoluciones adoptadas por el Consejo Intergubernamental del PIDCE de la UNESCO, en sus 26ª, 27ª, 28ª y 29ª sesiones en 2008, 2010, 2012 y 2014, respectivamente.

La tasa de respuesta de los Estados miembros sigue siendo baja, similar a tendencias anteriores[16]. En 2013, 17 de los 57 países[17] (30%) en los que se habían producido asesinatos de periodistas y estos no se habían resuelto respondieron a la solicitud formal de información. En 2014, 13 de 59 países[18] (22%) respondieron a la petición oficial. A 31 de agosto de 2015, 24 de 57 países[19] (42%) habían respondido a la última solicitud de información, lo que pone de relieve el posible inicio de una tendencia al alza.

Las respuestas recibidas en 2015 corresponden al 46% de los 641 casos sin resolver del período comprendido entre el 1 de enero de 2006 al 31 de diciembre de 2014. Se trata de un aumento en el volumen de información comparado con el período anterior. Entre 2006 y 2013, ambos años incluidos, se recibió información en un 22% de los casos no resueltos. Sin embargo, a pesar de una cobertura más amplia, sigue ocurriendo que no se recibe información alguna en más de la mitad de los casos.

Dentro de la información que la UNESCO si recibió de los Estados miembros, la proporción de casos acumulados que se declaran judicialmente resueltos ascendió al 5% en 2012, y al 8% en 2014. Aunque se observa una ligera subida del porcentaje, y aunque muchos otros casos se declaran como aún en curso, resulta evidente que la impunidad sigue constituyendo la tendencia predominante. Es posible extrapolar que tales porcentajes también se aplican a los casos de los que la UNESCO no recibió ninguna información, lo que significa que puede estimarse que la proporción total de casos resueltos continúa siendo extremadamente baja.

16 En 2011, se envió una petición oficial de información actualizada a los 38 países en los que tuvieron lugar asesinatos de periodistas, y 19 de ellos respondieron durante el período de 2011-2012, lo que supone una proporción del 50%. Si se considera el período más amplio de asesinatos cometidos entre 2007 y 2012, según se refiere en la versión de 2014 de Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios de la UNESCO, el 42% de los Estados miembros había proporcionado una respuesta a mediados de 2013.

17 En 2013, 17 países respondieron a la petición oficial: Bahrein, Bolivia, Brasil, Colombia, República de Congo, Croacia, República Democrática del Congo, Honduras, Kazajstán, Kenya, Perú, Federación Rusa, Sri Lanka, Tanzania, Túnez, Turkmenistán, y Vietnam. En ese mismo año, 40 países no respondieron: China, República Dominicana, El Salvador, Indonesia, Iraq, México, Pakistán, Filipinas, Turquía, Afganistán, Angola, Bangladesh, Bulgaria, Camboya, Camerún, Ecuador, Egipto, Eritrea, Georgia, Grecia, Guatemala, Guyana, Haití, India, Irán, Kirguistán, Líbano, Libia, Myanmar, Nepal, Nigeria, Palestina, Rwanda, Somalia, Sudán, Siria, Tailandia, Uganda, Venezuela y Yemen.

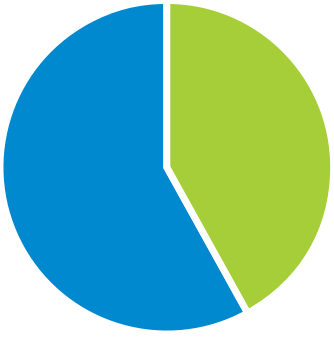
18 En 2014, 13 países respondieron a la petición oficial: Colombia, Honduras, Perú, Tanzania, China, El Salvador, Indonesia, Iraq, México, Pakistán, Filipinas y Turquía. En el mismo año, 46 países no respondieron a la petición; a saber: Afganistán, Angola, Bahrein, Bangladesh, Bolivia, Brasil, Bulgaria, Camboya, Camerún, República Centroafricana, Congo, Croacia, República Democráctica del Congo, Ecuador, Egipto, Eritrea, Georgia, Grecia, Guatemala, Guyana, Haití, India, Irán, Kenya, Kirguistán, Líbano, Libia, Malí, Myanmar, Nepal, Nigeria, Palestina, Paraguay, Federación Rusa, Rwanda, Somalia, Sudán del Sur, Sri Lanka, Sudán, Siria, Tailandia, Túnez, Turkmenistán, Uganda, Venezuela y Yemen.

19 A 1º de septiembre de 2015, 24 países habían respondido a la petición oficial: Bahrein, Brasil, Bulgaria, Colombia, República Dominicana, Ecuador, Egipto, El Salvador, Eritrea, Grecia, Guatemala, Haití, Honduras, Indonesia, México, Nigeria, Pakistán, Paraguay, Filipinas, Sri Lanka, Tanzania, Turquía, Ucrania y Venezuela. En ese mismo año, 33 países no respondieron: Afganistán, Angola, Bangladesh, Camboya, Camerún, República Centroafricana, Congo, República Democrática del Congo, Georgia, Guinea, Guyana, India, Irán, Iraq, Kenya, Kirguistán, Líbano, Libia, Malí, Myanmar, Nepal, Palestina, Perú, Federación de Rusia, Rwanda, Somalia, Sudán del Sur, Sudán, Siria, Tailandia, Túnez, Uganda y Yemen.

Tasa de respuesta de los Estados Miembros a la solicitud de información de la Directora General sobre la situación de las investigaciones judiciales sobre asesinatos de periodistas (2013, 2014, hasta el 31 de agosto de 2015)

30%
2013: 17/57 países

22%
2014: 13/59 países



42%
2015: 24/ 57 países

4. TENDENCIA AL ALZA EN LA CONSOLIDACIÓN DE LAS NORMAS INTERNACIONALES SOBRE SEGURIDAD DE LOS PERIODISTAS

Mientras que no se ha producido ningún cambio significativo en las tendencias de seguridad descritas anteriormente, en comparación con el período precedente, sí se han obtenido en cambio grandes avances en el ámbito normativo. Las normas internacionales sobre la seguridad de los periodistas se han reforzado notablemente en los dos últimos años. Esta tendencia se consolidó tras las reacciones mundiales a los asesinatos de periodistas en la publicación satírica Charlie Hebdo en París, Francia, a principios de 2015, cometidos con posterioridad a la brutal decapitación de periodistas en Siria. Aunque el ataque es posterior al período objeto de estudio, se destaca en el presente capítulo porque ocurrió en un contexto de consideración creciente de la cuestión a escala internacional, y dio lugar a una atención aún mayor por este asunto en todas las regiones, que incluyó una marcha de protesta encabezada por diversos líderes mundiales. Como ocurrió con el impacto acumulado de las imágenes de las decapitaciones de periodistas a manos de extremistas, y de los asesinatos particularmente violentos perpetrados por traficantes de drogas contra reporteros a lo largo de 2013 y 2014, los ataques de 2015 en París han dado lugar a una creciente sensibilización en todo el mundo respecto a la gravedad de estos crímenes.

Un indicador de la tendencia de mayor sensibilización es la actividad en el ámbito de las Naciones Unidas. Como se refiere con mayor amplitud más adelante, en el período de 2012 a 2015, tanto el Consejo de Seguridad de Naciones Unidas, como la Asamblea General, el Consejo de Derechos Humanos y la UNESCO adoptaron resoluciones y decisiones significativas en las que se condenan de manera inequívoca todos los atentados y actos de violencia contra periodistas. En varias de estas declaraciones se incluyeron acciones encaminadas a consolidar los mecanismos globales de seguimiento e información sobre seguridad, y se incidió además en la importancia de las medidas prácticas que deben adoptar los Estados miembros para acabar con la impunidad.

La Asamblea General de las Naciones Unidas, el órgano superior de toma de decisiones del sistema de la ONU, adoptó las Resoluciones A/RES/68/163 (en 2013) y A/RES/69/185 (en 2014), en las que se condenan firmemente todos los ataques a periodistas y trabajadores de los medios de comunicación, incluidos los actos de tortura, las ejecuciones extrajudiciales, las desapariciones forzosas y las detenciones arbitrarias, el acoso y la intimidación, tanto en situaciones de conflicto, como fuera de ellas. En las Resoluciones también se critica con firmeza la impunidad generalizada respecto a los ataques y los actos de violencia cometidos contra periodistas.

Por otra parte, con arreglo a la Resolución A/RES/68/163, la Asamblea General de la ONU estableció el 2 de noviembre como Día Internacional para poner fin a la impunidad de los crímenes contra periodistas, lo que constituyó un importante hito en el reconocimiento mundial de esta cuestión. La UNESCO, a la que se encargó facilitar las conmemoraciones del Día internacional, encabezó la ronda inicial con una serie de eventos entre los que figuraron una conferencia en el Tribunal Europeo de Derechos Humanos de Estrasburgo, Francia, junto con el Consejo de Europa, el Centre for Freedom of the Media (Centro para la Libertad de los Medios) de la Universidad de Sheffield, y la European Lawyer's Union (Unión de Abogados Europeos). Otras actividades localizadas se llevaron a cabo en Nueva York, Túnez, Accra y Abuja. Con estos eventos, la UNESCO procuró dirigirse a los miembros del sistema judicial, para sensibilizarles respecto al papel que pueden desempeñar en la tarea de poner fin a la impunidad, y al modo en que la atención prestada a la resolución de los casos de ataques a periodistas puede contribuir de manera más general al refuerzo del estado de derecho y los derechos humanos en la sociedad en su conjunto. En el evento de Estrasburgo se llevó a cabo además una evaluación a cargo de múltiples partes interesadas del Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad. El Plan fue avalado por la Junta de los Jefes Ejecutivos de la ONU en 2012, y valorado positivamente por la Asamblea General de Naciones Unidas en diciembre de 2013, en la Resolución A/RES/68/163.

En el Consejo de Derechos Humanos, la histórica Resolución A/HRC/RES/21/12 fue aprobada en 2012, y a esta le siguió en 2014 la Resolución A/RES/HRC/27/5, relativas en ambos casos a la seguridad de los periodistas. Estas Resoluciones instan a todas las partes a respetar sus obligaciones con arreglo a la legislación internacional sobre derechos humanos y el derecho internacional humanitario, y a los Estados a promover un entorno seguro y propicio para que los periodistas desarrollen su labor con independencia y sin injerencias indebidas.

En su 191ª Sesión, celebrada en abril de 2013, el Consejo Ejecutivo de la UNESCO aprobó su Plan de trabajo para abordar la seguridad de los periodistas y la impunidad de los delitos cometidos contra ellos. El Plan de trabajo, en el que se hace hincapié en la cooperación Sur-Sur, expone el enfoque de la UNESCO respecto a la seguridad, incluido el liderazgo del Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad. Posteriormente, el Consejo Ejecutivo de la UNESCO aprobó la Resolución sobre la seguridad de los periodistas y la cuestión de la impunidad en su 196ª Sesión del 20 de abril de 2015. Esta Resolución reforzó el trabajo en curso de la UNESCO en relación con el Plan de acción de la ONU, sobre la base de un enfoque multipartito en el que participan todos los agentes pertinentes, incluidas las autoridades nacionales, las agencias de la ONU, diversos grupos de la sociedad civil, representantes del ámbito académico y los medios de comunicación. La Resolución confirmó además que la misión de procurar la seguridad del periodismo comprende la seguridad de los productores de medios sociales, que desarrollan una extensa actividad periodística de interés público.

Por otra parte, el Consejo de Seguridad de la ONU también aprobó la Resolución 2222 (el 27 de mayo de 2015), en la que se insta a las partes en conflicto y a todos los Estados miembros a crear un entorno seguro mediante la legislación y en la práctica para que los periodistas ejerzan su profesión. También se insta al Secretario General de la ONU a incluir de manera sistemática en el "Informe sobre la protección de civiles en conflictos armados", que se elabora periódicamente, un subapartado sobre la cuestión de la seguridad y la protección de los periodistas, los profesionales de los medios de comunicación y otro personal afín.

Un indicio del reconocimiento cada vez mayor de la importancia de estas cuestiones es el creciente número de signatarios de estas resoluciones.

- Resolución A/RES/68/163 de la AGNU, adoptada en 2013: 54 signatarios[20]
- Resolución A/RES/69/185 de la AGNU, adoptada en 2014: 82 signatarios[21]
- Resolución del Consejo de Derechos Humanos A/HRC/21/12, adoptada en 2012: 52 signatarios[22]
- Resolución del Consejo de Derechos Humanos A/HRC/27/5, adoptada en 2014: 63 signatarios[23]

20 Los 54 países que siguen copatrocinaron la Resolución A/RES/68/163: Albania, Andorra, Argentina, Armenia, Australia, Austria, Azerbaiyán, Bélgica, Benín, Bosnia y Herzegovina, Brasil, Bulgaria, Canadá, Chile, Colombia, Costa Rica, Croacia, Chipre, República Checa, El Salvador, Estonia, Francia, Alemania, Ghana, Grecia, Hungría, Irlanda, Italia, Japón, Letonia, Luxemburgo, Maldivas, Malí, Malta, Mongolia, Marruecos, Países Bajos, Nigeria, Panamá, Paraguay, Perú, Polonia, Portugal, Qatar, República de Corea, Rumanía, San Marino, Serbia, Eslovaquia, Eslovenia, España, Túnez, Turquía, Estados Unidos de América, y Uruguay.

21 Los 82 países que siguen copatrocinaron la Resolución A/RES/69/185: Andorra, Argentina, Armenia, Australia, Austria, Azerbaiyán, Bélgica, Benín, Bosnia y Herzegovina, Brasil, Bulgaria, Burkina Faso, Cabo Verde, República Centroafricana, Chile, Colombia, Costa Rica, Croacia, Chipre, República Checa, Dinamarca, Egipto, El Salvador, Estonia, Finlandia, Francia, Georgia, Alemania, Ghana, Grecia, Guatemala, Honduras, Hungría, Islandia, Irlanda, Israel, Italia, Japón, Jordania, Letonia, Líbano, Libia, Liechtenstein, Lituania, Luxemburgo, Maldivas, Malí, Malta, México, Mónaco, Mongolia, Montenegro, Marruecos, República de Moldavia, Países Bajos, Nueva Zelanda, Noruega, Panamá, Paraguay, Perú, Polonia, Portugal, Qatar, República de Corea, Rumanía, San Marino, Serbia, Eslovaquia, Eslovenia, Somalia, España, Suecia, Suiza, República Centroafricana, Antigua República Yugoslava de Macedonia, Túnez, Turquía, Ucrania, Reino Unido de Gran Bretaña e Irlanda del Norte, Estados Unidos de América, y Uruguay.

22 Los 52 países que siguen copatrocinaron la Resolución A/HRC/21/12: Albania, Argentina, Australia, Austria, Bélgica, Bosnia y Herzegovina, Botswana, Brasil, Bulgaria, Colombia, Croacia, Chipre, República Checa, Dinamarca, Egipto, Estonia, Finlandia, Georgia, Alemania, Grecia, Guatemala, Honduras, Hungría, Islandia, Irlanda, Kenya, Letonia, Líbano, Libia, Liechtenstein, Lituania, Luxemburgo, México, Montenegro, Marruecos, Países Bajos, Nigeria, Noruega, Palestina, Perú, Polonia, Portugal, Qatar, República de Moldavia, Rumanía, Serbia, Eslovenia, Suecia, Suiza, Túnez, Turquía, y el Reino Unido de Gran Bretaña e Irlanda del Norte.

23 Los 63 países que siguen copatrocinaron la Resolución A/HRC/27/5: Argentina, Australia, Austria, Bélgica, Benín, Bosnia y Herzegovina, Brasil, Bulgaria, Burkina Faso, Canadá, República Centroafricana, Colombia, Costa Rica, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Georgia, Alemania, Grecia, Guatemala, Honduras, Hungría, Islandia, Irlanda, Israel, Italia, Letonia, Líbano, Libia, Liechtenstein, Lituania, Luxemburgo, Maldivas, México, Montenegro, Marruecos, Países Bajos, Nueva Zelanda, Nigeria, Noruega, Paraguay, Perú, Polonia, Portugal, Qatar, República de Moldavia, Rumanía, San Cristóbal y Nieves, Serbia, Eslovaquia, Eslovenia, España, Palestina, Suecia, Suiza, Antigua República Yugoslava de Macedonia, Túnez, Turquía, Reino Unido de Gran Bretaña e Irlanda del Norte, Estados Unidos de América, y Yemen.

La Resolución 196 EX/31 del Consejo Ejecutivo de la UNESCO, adoptada en abril de 2015, también recibió un elevado número de firmas, en concreto, las de 47 países[24]. Del mismo modo, el Consejo de Seguridad de las Naciones Unidas adoptó la Resolución UNSC 2222 (el 27 de mayo de 2015), con la firma conjunta de 49 países[25].

24 Los 47 países que siguen copatrocinaron la Resolución 196 EX/31 del Consejo Ejecutivo de la UNESCO: Albania, Andorra, Argentina, Australia, Austria, Brasil, Chipre, República Checa, Dinamarca, República Dominicana, El Salvador, Estonia, Finlandia, Francia, Gabón, Alemania, Grecia, Honduras, Islandia, Irlanda, Italia, Japón, Letonia, Liberia, Malawi, Marruecos, Namibia, Países Bajos, Nigeria, Noruega, Paraguay, Perú, Portugal, República de Corea, Serbia, Eslovaquia, Eslovenia, España, San Cristóbal y Nieves, Suecia, Suiza, Trinidad y Tobago, Túnez, Ucrania, Reino Unido de Gran Bretaña e Irlanda del Norte, Estados Unidos de América, y Uruguay.

25 Los 49 países que siguen copatrocinaron la Resolución UNSC 2222 del Consejo de Seguridad de la ONU: Albania, Angola, Australia, Austria, Bélgica, Bosnia y Herzegovina, Bulgaria, Canadá, Chad, Chile, Croacia, Chipre, República Checa, Dinamarca, Estonia, Finlandia, Francia, Alemania, Grecia, Hungría, Islandia, Israel, Italia, Japón, Jordania, Letonia, Líbano, Liechtenstein, Lituania, Luxemburgo, Malasia, Montenegro, Países Bajos, Nueva Zelanda, Nigeria, Noruega, Palau, Polonia, República de Moldavia, Rumanía, Serbia, Eslovaquia, Eslovenia, España, Suecia, Antigua República Yugoslava de Macedonia, Ucrania, Reino Unido de Gran Bretaña e Irlanda del Norte, y los Estados Unidos de América.

5. DESARROLLO DE MECANISMOS PRÁCTICOS PARA PROMOVER LA SEGURIDAD Y PONER FIN A LA IMPUNIDAD

También se registraron avances en el ámbito institucional en relación con la seguridad y la impunidad a lo largo de 2012 y 2013. Varios países en la región de América Latina han seguido desarrollando marcos oficiales e instituciones para abordar las cuestiones de la seguridad y la protección, basándose en muchos casos en la experiencia positiva de Colombia. Se trata de mecanismos que van de los sistemas de coordinación entre departamentos, a los foros multipartitos en los que participan representantes de los medios y la sociedad civil, pasando por la dotación de personal y presupuestos específicos. En Pakistán, una amplia coalición ha trabajado para contar con la participación de numerosos interlocutores, incluidos el gobierno y los diputados parlamentarios, en debates periódicos sobre seguridad e impunidad. En Serbia, una comisión de representantes de los medios de comunicación independientes, un ministerio y los servicios de seguridad, lograron el enjuiciamiento de cuatro personas por el asesinato de un periodista cometido 16 años antes.

En 2013, la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos (OACDH), en colaboración con el Relator Especial de la ONU para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión, publicó un informe en el que se ponen de relieve las iniciativas y las buenas prácticas relacionadas con la seguridad de los periodistas y la tarea de acabar con la impunidad. El informe contiene un resumen de la situación que afrontan los periodistas, la legislación aplicable y las iniciativas emprendidas por los Estados miembros, las agencias de las Naciones Unidas y otras organizaciones para la seguridad de este colectivo. Se identifican asimismo buenas prácticas que podrían contribuir a la creación de un entorno seguro y propicio para que los periodistas puedan ejercer libremente su profesión.

El 2 de abril de 2015, el Consejo de Europa puso en marcha una plataforma de Internet encaminada a proteger el periodismo y a promover la seguridad de quienes lo ejercen. La plataforma se diseñó para facilitar la compilación, el procesado y la difusión de información basada en hechos objetivos, verificada por los socios, y relativa a amenazas físicas graves a periodistas y otro personal de los medios, a amenazas a la confidencialidad de las fuentes utilizadas por los medios, y a diversas formas de intimidación política o judicial. La plataforma contempla la asociación del Consejo de Europa con el artículo 19, la Asociación de Periodistas Europeos, la Federación Europea de Periodistas, la Federación Internacional de Periodistas, y Reporteros Sin Fronteras.

La tendencia mundial a que el periodismo se ejerza cada vez más a través de medios digitales también se refleja en el aumento de las actividades de formación y las herramientas dirigidas a periodistas que se centran en la seguridad digital y, especialmente, en el ámbito de los dispositivos móviles. Se incluye aquí el desarrollo de aplicaciones de telefonía

móvil concebidas para que los periodistas puedan protegerse mejor. La *International Media Women's Foundation* (IWMF, Fundación Internacional de Mujeres en los Medios de Comunicación) ha desarrollado una de esas aplicaciones, denominada *Reporta*, que consta de funciones de "check-in" o registro, "alertas" y "SOS". Del mismo modo, el International Center for Journalists (ICFJ) desarrolla actualmente *Salama*, una aplicación para la evaluación de riesgos.

6. MEJORA DE LA COLABORACIÓN ENTRE AGENCIAS

En el período de 2013-2014, se reforzó la cooperación entre los órganos de la ONU en materia de seguridad. La OACDH y la UNESCO contribuyeron al Informe del Secretario General de la ONU sobre la Resolución de ejecución A/RES/68/163 sobre la seguridad de los periodistas y la cuestión de la impunidad. El Informe, que se presentó a la Asamblea General de la ONU, ofrece una visión general de las tendencias recientes de la seguridad de los periodistas y los trabajadores de los medios de comunicación, así como una compilación de las iniciativas emprendidas para garantizar su protección, junto con diversas recomendaciones.

La UNODC publicó en 2013 el *Estudio mundial sobre el homicidio*, en el que se ofrece una amplia visión de conjunto del homicidio intencional en todo el mundo. Se elaboró un subapartado sobre los asesinatos de periodistas con material aportado por la UNESCO.

El Departamento de Información Pública de las Naciones Unidas (UNDPI por sus siglas en inglés) transmitió la información relativa al desarrollo del Plan de Acción de las Naciones Unidas sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad a sus 63 Centros de Información de Naciones Unidas (UNIC) en todo el mundo. ONU Mujeres y la UNESCO han colaborado durante el período en asuntos que atañen a las periodistas. La cuestión de la seguridad de los periodistas también se ha incorporado de manera creciente al Marco de Asistencia de las Naciones Unidas para el Desarrollo (MANUD), con inclusión de los casos de Jordania, Nepal y Sudán del Sur.

Otras iniciativas de cooperación se llevaron a cabo entre la OACDH, la OIT y la UNESCO, y con el Foro Mundial para el Desarrollo de los Medios, en cuanto a la elaboración de un proyecto de indicadores para los objetivos de desarrollo sostenible (ODS). El ODS 16.10 consiste en “garantizar el acceso público a la información y proteger las libertades fundamentales, de conformidad con la legislación nacional y los acuerdos internacionales”. Los debates entre los grupos citados anteriormente dieron lugar al consenso respecto a un indicador propuesto en materia de seguridad para este objetivo en particular. El indicador propuesto, que podrá adoptarse a principios de 2016, es: “el número de casos comprobados de asesinato, secuestro, desaparición forzosa, detención arbitraria y tortura de periodistas, personal asociado de los medios, sindicalistas y defensores de los derechos humanos en los 12 meses anteriores.” Se prevé que estos indicadores puedan contribuir a que se generalice la interpretación de que la seguridad de los periodistas constituye una libertad fundamental por derecho propio, así como una meta del desarrollo sostenible, además de un factor capacitador que propicia la consecución de otros ODS.

7. HACIA UNA MAYOR PARTICIPACIÓN DEL SECTOR JUDICIAL EN EL TRATAMIENTO DE LA IMPUNIDAD

En los dos últimos años, ha aumentado la tendencia a una creciente colaboración con el sistema judicial en la lucha contra la impunidad, incluidas las iniciativas de refuerzo de capacidades dirigidas a jueces y abogados. La conferencia sobre impunidad celebrada en el Tribunal Europeo de Derechos Humanos en noviembre de 2014 ya se ha mencionado anteriormente. También en 2014, la UNESCO y el *Knight Center for Journalism in the Americas* de la Universidad de Texas en Austin colaboraron con el antiguo Relator Especial de la ONU para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión de la ONU y con el antiguo Relator Especial de la Organización de Estados Americanos en la provisión de un curso en línea masivo y abierto (CEMA) sobre la libertad de expresión, en el que se trató asimismo la seguridad de los periodistas. El curso, en el que participaron más de 800 agentes del ámbito jurídico durante un mes, se creó inicialmente para el Tribunal Supremo de México, y desde entonces ha atraído el interés de otros miembros del sector judicial de diversos lugares en la región de América Latina. Tal es el resultado de la semilla plantada por el PIDCE de la UNESCO en 2013. En 2015, el CEMA vuelve a impartirse con el apoyo de la UNESCO y el Gobierno del Estado de Coahuila de México.

En varias resoluciones, como la emitida en 2013 por el Tribunal Africano de Derechos Humanos y de los Pueblos, que ordenó la reapertura de la investigación sobre el asesinato del periodista de Burkina Norbert Zongo y otras tres personas, cometido en 1998, se observa un creciente reconocimiento de la importancia de la aplicación efectiva del Estado de Derecho. Una jurisprudencia similar caracterizó el fallo dictado en 2014 por el Tribunal de Justicia de la Comunidad Económica de los Estados del África Occidental, respecto al caso del periodista de Gambia Deyda Hydara, que fue asesinado en 2004[26].

26 Los referidos son ejemplos recientes. Un caso anterior es el de la sentencia de 2009 emitida por la Corte Interamericana de Derechos Humanos en el asunto de Ríos et al. v. Venezuela, en la que se estableció que las ejecuciones extrajudiciales exigían investigaciones que fueran oportunas y se llevaran a cabo de un modo formal, justo y efectivo.

8. CONSOLIDACIÓN DE LA COLABORACIÓN CON LAS FUERZAS DE SEGURIDAD NACIONALES

Un elemento esencial en la tarea de garantizar la seguridad de los periodistas es la interacción con las fuerzas de seguridad. Se trata de un aspecto especialmente relevante en épocas de máxima tensión y presión, como las elecciones, o en situaciones de protestas en las calles. La UNESCO comenzó a promover esta área de refuerzo de capacidades en 2013, con una serie de cursos de formación impartidos en Túnez con la colaboración del Ministerio del Interior, y la ayuda de los Países Bajos y la Agencia de Cooperación al Desarrollo Internacional (Sida) de Suecia. Esta serie de sesiones de formación se convirtieron en la base del nuevo manual de la UNESCO titulado *Freedom of Expression and Public Order* (Libertad de expresión y orden público). En 2015 se desarrollaron iniciativas de formación similares en Mogadiscio, Somalia, en cooperación con Relief International y la Misión de Asistencia de las Naciones Unidas para Somalia (UNSOM). Esta tendencia emergente al refuerzo de la colaboración entre las fuerzas de seguridad y los profesionales de los medios de comunicación puede redundar en beneficio tanto del orden público, como de la libertad de expresión.

9. PROMOCIÓN DE UNA AGENDA DE INVESTIGACIÓN SOBRE LA SEGURIDAD DE LOS PERIODISTAS

Durante el período se reforzó la seguridad gracias a una mejor comprensión de las cuestiones consideradas. En la revisión del Plan de acción de la ONU en Estrasburgo, en noviembre de 2014, se ampliaron conocimientos a través del debate sobre el modo en que los contextos en que se asesina a periodistas, incluida la voluntad y la capacidad políticas, exigen diversos tipos de apoyo, como la puesta en común de conocimientos, el refuerzo de capacidades, la concienciación de las partes interesadas, el fomento de la sensibilización, la formación sobre seguridad para periodistas, y el desarrollo de la documentación sobre los ataques, de manera que pueda ejercerse la justicia en el futuro.

Como refuerzo de los conceptos matizados desarrollados a lo largo del período de estudio, se ha elevado el nivel de conocimiento sobre las causas, los efectos y los medios de reparación en relación con la seguridad y la impunidad. Un ejemplo de esta actividad fue la aplicación experimental de los indicadores de seguridad del periodismo (ISP) de la UNESCO en Pakistán, Honduras, Guatemala y Liberia, así como la puesta en marcha de estudios completos de los ISP en Nepal, Iraq y Kenya.

Otro avance ha sido el creciente interés y el refuerzo de las actuaciones en lo que atañe a los miembros del ámbito académico y otros agentes que llevan a cabo tareas de investigación. En la estrategia de ejecución de 2012 del Plan de acción de la ONU se identificó una oportunidad significativa en el área de la investigación académica científica sobre la seguridad de los periodistas y la impunidad. Este reconocimiento se basó en la realidad de que, según se infiere de un análisis general al respecto, la investigación académica efectuada en los últimos 20 años ha dado lugar a un número relativamente reducido de estudios publicados. De estos, la mayoría se centra en los “reportajes de guerra”, o en la protección de periodistas en situaciones de conflicto armado, aunque más de la mitad de los ataques contra estos profesionales se produjeron en situaciones de conflicto no armado.

En un esfuerzo por impulsar una tendencia al aumento de la investigación en este ámbito, la UNESCO elaboró en 2014 una agenda de investigación de diez puntos, y la promovió en 2015 en las sesiones especiales impartidas en julio de ese año sobre la seguridad de los periodistas con ocasión de la Conferencia de la Asociación Internacional de Estudios en Comunicación Social (IAMCR por sus siglas en inglés) en Montreal, y la Conferencia de la *Global Communication Association* en Berlín. Más de 100 investigadores participaron en estas actividades. Paralelamente, varias universidades han manifestado su interés en colaborar con la UNESCO en el terreno de la investigación sobre seguridad.

10. ENCARCELAMIENTO DE PERIODISTAS

Como se señaló en la anterior edición de Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios de la UNESCO, el encarcelamiento de periodistas por ejercer su legítima labor fomenta una cultura de la autocensura e infringe los derechos más generales de la sociedad a obtener información. En dicha edición se añade que: "en términos de las limitaciones y sanciones justificables del ejercicio de la libertad de expresión que establecen los estándares internacionales, el encarcelamiento por el ejercicio legítimo del periodismo es una medida innecesaria y desproporcionada." Teniendo en cuenta su mandato, la UNESCO no se ocupa de la recogida ni del seguimiento sistemáticos de los datos relacionados con el encarcelamiento de periodistas[27]. En cualquier caso, se ha determinado que, de acuerdo con una amplia gama de fuentes y datos, la tasa de encarcelamiento de periodistas en todo el mundo, se mantuvo en un nivel elevado en 2013 y 2014. Se ha informado que entre 178 y 211 periodistas ingresaron en prisión en 2013, y que al menos 221 fueron encarcelados en 2014[28]. Estas cifras se comparan con las de 2012, en la que, según se refiere, al menos 232 periodistas fueron encarcelados, y las de 2011, en la que tal cifra se situó en 179. La desaparición forzosa o involuntaria de periodistas ha seguido constituyendo un problema. En estos casos que atañen a periodistas que, a menudo, denunciaron actividades delictivas o casos de corrupción antes de su desaparición, los agentes que procuran una compensación o la reapertura de las investigaciones han recurrido al Grupo de Trabajo sobre Desapariciones Forzadas o Involuntarias de la ONU y al Grupo de trabajo de las Naciones Unidas sobre la detención arbitraria.

27 Como se indicó en el primer informe, muchos gobiernos han mantenido que los periodistas en cuestión no habían sido encarcelados por el ejercicio de su profesión, sino por otros motivos, y el mandato de la UNESCO no contempla la tarea de evaluar qué casos se incluyen en esta categoría, ni esos otros motivos.

28 Basado en los datos públicos facilitados por importantes organizaciones internacionales defensoras de la libertad de prensa, como el Comité para la Protección de los Periodistas (CPJ) y Reporteros sin Fronteras (RSF).

11. PERSPECTIVA DE GÉNERO EN LA SEGURIDAD DE LOS PERIODISTAS

Aunque las mujeres representan menos del ocho por ciento del total (14 de 178) de periodistas asesinados en el período de 2013 y 2014, se ha producido un moderado aumento de la cifra total de mujeres periodistas asesinadas[29]. Por otra parte, las periodistas han seguido siendo objeto de otras formas de acoso y ataque.

En los dos últimos años, la UNESCO ha reforzado su apoyo a la investigación y las iniciativas de sensibilización en este ámbito de la seguridad de los periodistas. En marzo de 2014, la Organización, en colaboración con el *International News Safety Institute*, la *International Women's Media Foundation* y el Gobierno austríaco, presentaron los resultados de una encuesta titulada Violencia y acoso contra las mujeres en los medios de información: una visión global, en la que participaron casi 1.000 encuestados. Este estudio confía en despertar un mayor interés en la investigación sobre el asunto de la seguridad específica de las mujeres periodistas.

Por otra parte, en 2015, la UNESCO otorgó especial atención a la cuestión del género en su nueva publicación titulada *Building Digital Safety for Journalism: A Survey of Selected Issues*. (El fomento de la seguridad digital para el periodismo: encuesta sobre ciertas cuestiones). En la encuesta, que se centra en las amenazas digitales a los periodistas, se señala que las mujeres tienen más probabilidades que los varones de enfrentarse a respuestas negativas e incluso amenazantes en línea. Las periodistas en particular se exponen a un "doble ataque", ya que son destinatarias de este tipo de acciones por su condición de periodistas y de mujeres.

Como parte de una iniciativa más amplia de sensibilización en estas áreas, la UNESCO incluyó regularmente en el periodo considerado una importante perspectiva de género en sus actividades de concienciación de referencia, como las celebraciones del Día Mundial de la Libertad de Prensa. En los dos últimos años, este evento internacional ha incluido sesiones dedicadas a la seguridad de las periodistas, en las que se han impartido seminarios de formación y se han tratado otras cuestiones relacionadas con el género en los medios de comunicación. En 2015, en respuesta al 20º aniversario de la Declaración y la Plataforma de Acción de Pekín, la UNESCO organizó tres sesiones dedicadas sobre la cuestión del género y los medios durante la celebración del Día Mundial de la Libertad de Prensa en Riga, Letonia.

En abril de 2015, con el fin de hacer mayor hincapié en la importancia de la seguridad de los periodistas en todo el mundo, y en especial, en el papel que desempeñan las mujeres que ejercen esa profesión, el Director General de la UNESCO designó a Christiane Amanpour, corresponsal internacional jefe de la CNN, como Embajadora de Buena Voluntad de la UNESCO para la Libertad de Expresión y la Seguridad de los Periodistas, previamente a la celebración del Día Mundial de la Libertad de Prensa en dicho año.

29 Seis periodistas fueron asesinadas en 2013, y ocho en 2014.

12. CONCLUSIÓN

En este capítulo se han revisado las tendencias existentes en el terreno de la seguridad de los periodistas y la cuestión de la impunidad, con la ayuda de las estadísticas recabadas en 2013 y 2014, y con referencia a diversos acontecimientos de 2012 y 2015. Aunque los ataques a periodistas y el asunto de la impunidad han seguido constituyendo un grave problema, se han obtenido avances evidentes en otras áreas. Se trata en concreto del gran número de Estados miembros de la ONU que se han asociado a las Resoluciones de la Organización, y de la mejora en la tasa de respuesta a las consultas de la UNESCO en 2014, en comparación con 2013. Se han registrado otras mejoras, entre las que figuran la sensibilización, el refuerzo de instituciones y capacidades, y la generación de conocimiento. No resulta fácil calibrar si toda esta consolidación de las actuaciones ha contribuido en alguna medida a evitar que las estadísticas sean aún más graves de lo que lo son en realidad. Tampoco es fácil medir si su efecto se prolongará en el tiempo. Lo que está claro, en cualquier caso, es que existe un creciente impulso global hacia el establecimiento de una cultura en la que la seguridad de los periodistas y el fin de la impunidad estén garantizados. Parece probable que esta tendencia siga desarrollándose mientras persistan los problemas, y en la medida en que se cosechen éxitos, estos impulsarán la búsqueda de unas sociedades del conocimiento pacíficas, y la consecución de los objetivos de desarrollo sostenibles de las Naciones Unidas.

VII. ANEXOS

ANEXO 1: PERSONAS ENTREVISTADAS PARA CONTRARRESTAR LA INCITACIÓN AL ODIO EN INTERNET

Imran Awan, Vicedirector del Centro de Criminología Aplicada, Escuela de Ciencias Sociales, Universidad de la Ciudad de Birmingham, Reino Unido de Gran Bretaña e Irlanda del Norte.

Monika Bickert, Directora de Gestión de Políticas Mundiales, Facebook, Estados Unidos de América.

Drew Boyd, Director de Operaciones, *The Sentinel Project for Genocide Prevention*, Canadá.

Ian Brown, Profesor de Seguridad de la Información y Privacidad, Instituto de Internet de Oxford, Universidad de Oxford, Reino Unido de Gran Bretaña e Irlanda del Norte.

Laura Geraghty, No Hate Speech Movement, Reino Unido de Gran Bretaña e Irlanda del Norte.

Matthew Johnson, Director de Educación, MediaSmarts, Canadá.

Myat Ko Ko, Oficial de Programas de Myanmar, Justice Base, Myanmar.

Ciara Lyden, Directora de Política de Contenidos, Política de Productos, Facebook, Irlanda.

Andre Oboler, Primer Ejecutivo del Online Hate Prevention Institute, Australia.

Harry Myo Lin, Panzagar, Myanmar.

Nanjira Sambuli, Directora de Proyectos, UMATI, Kenya.

Christopher Wolf, Presidente, Comité Nacional de Internet, Liga Contra la Difamación, Estados Unidos de América.

ANEXO 2: PERSONAS ENTREVISTADAS PARA PROTECCIÓN DE LAS FUENTES PERIODÍSTICAS EN LA ERA DIGITAL

Rasha Abdulla, profesora asociada, Periodismo y Comunicación de Masas, Universidad Americana en El Cairo, Egipto.

Ricardo Aguilar, periodista de investigación, *La Razón*, Bolivia.

Rawda Ahmed, abogado, Red Árabe por la Información sobre Derechos Humanos, Egipto.

Mahasen Al Eman, Directora, Centro de Medios de Comunicación de la Mujer Árabe, Jordania.

Amare Aregawi, propietario, Media and Communications Center y Horn of Africa Press Institute, Etiopía.

Hans-Gunnar Axberger, Profesor de Derecho Constitucional, Universidad de Uppsala, Suecia.

Wendy Bacon, Profesora asociada, Australian Centre for Independent Journalism, Australia.

Martin Baron, Editor Ejecutivo, *The Washington Post*, Estados Unidos de América.

Peter Bartlett, socio, Minter Ellison, Australia.

Katarina Berglund-Siegbahn, asesora jurídica, Ministerio de Justicia, Suecia.

Catalina Botero Marino, antigua Relatora Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos, Estados Unidos de América.

Cliff Buddle, Redactor Principal, *South China Morning Post*, China.

Umar Cheema, periodista de investigación, *The News*, y fundador del Centro para el Periodismo de Investigación en Pakistán.

Zine Cherfaoui, Redactor Jefe, *El Watan*, Argelia.

Marites Dañguilan Vitug, Cofundadora y miembro del Consejo del Centro para el Periodismo de Investigación de Filipinas, Filipinas.

Yves Eudes, reportero, *Le Monde*, y confundador de Source sûre, Francia.

Tomaso Falchetta, responsable de asuntos jurídicos, Privacy International, Reino Unido de Gran Bretaña e Irlanda del Norte.

Javier Garza Ramos, Experto en seguridad y protección en el ámbito del periodismo, México.

Carlos Guyot, Redactor Jefe, *La Nación*, Argentina.

Silvia Higuera, Knight Center for Journalism in the Americas, Universidad de Texas, Austin, Estados Unidos de América.

Daoud Kuttab, periodista, Jordania.

Fredrik Laurin, Director de la Unidad de Investigación, Radio Pública de Suecia (SR), Suecia.

Ronaldo Lemos, Director, Instituto para la Tecnología y la Sociedad (ITS), Río de Janeiro, y Profesor, Facultad de Derecho, Universidad Estatal de Río de Janeiro, Brasil.

Justine Limpitlaw, abogada especializada en comunicaciones electrónicas, Sudáfrica.

Henry Omusundi Maina, Director, ARTICLE 19 Este y Cuerno de África, Kenya.

Susan E. McGregor, Profesora Asistente y Directora Asistente, Centro Tow para el Periodismo Digital, Escuela de Periodismo de Columbia, Universidad de Columbia, Estados Unidos de América.

Toby Mendel, Director, Centro para la Ley y la Democracia, Canadá.

Gavin Millar QC, abogado, Matrix International, Reino Unido de Gran Bretaña e Irlanda del Norte.

Peter Noorlander, abogado especializado en medios de comunicación, Media Legal Defence Initiative, Reino Unido de Gran Bretaña e Irlanda del Norte.

Gunnar Nygren, Profesor, Escuela de Ciencias Sociales, Universidad de Estocolmo, Suecia.

Leanne O'Donnell, abogado principal, Política de Asuntos Jurídicos, Instituto de Derecho de Victoria, Australia.

Toyosi Ogunseye, Editor, *The Sunday Punch*, Nigeria.

Julie Owono, Directora de la Oficina para África, Internet Sans Frontières, Francia.

Courtney Radsch, Directora de Promoción de Causas, Comité para la Protección de los Periodistas, Estados Unidos de América.

Marcelo Rech, Director Ejecutivo de Periodismo, Grupo RBS, Brasil.

Alan Rusbridger, Redactor Jefe, *The Guardian*, Reino Unido de Gran Bretaña e Irlanda del Norte.

Gerard Ryle, Director, International Consortium of Investigative Journalists, Estados Unidos de América.

Rana Sabbagh, Directora Ejecutiva, Reporteros Árabes por el Periodismo de Investigación, Jordania.

Josh Stearns, Director de Periodismo y Sostenibilidad, Geraldine R. Dodge Foundation, Estados Unidos de América.

Atanas Tchobanov, Editor, Bivol.bg, y periodista, BalkanLeaks, Bulgaria.

Charles D. Tobin, socio, Holland & Knight, Estados Unidos de América.

Pär Trehörning, defensor del afiliado, Unión de Periodistas de Suecia, Suecia.

Pedro Vaca Villarreal, Director Ejecutivo, Fundación para la Libertad de Prensa (FLIP), Colombia.

Anita Vahlberg, Asesora Principal, Unión de Periodistas de Suecia, Suecia.

Dirk Voorhoof, Profesor, Facultad de Ciencias Políticas y Sociales, y Facultad de Derecho, Universidad de Gante, Bélgica.

Wei Yongzheng, profesor, Universidad de la Comunicación de China, Pekín, China.

George Williams, Profesor, profesor Anthony Mason, profesor de ciencias (Scientia), Director de Fundación, Centro Gilbert + Tobin de Derecho Público, Facultad de Derechos, Universidad de Nueva Gales del Sur, Australia.

Jillian York, Director de Libertad de Expresión Internacional, Electronic Frontier Foundation, Alemania.

Yuan Zhen (seudónimo), Redactor Jefe, (periódico sin denominar), China.

ANEXO 3: ESTADOS MIEMBROS DE LA UNESCO EXAMINADOS EN PROTECCIÓN DE LAS FUENTES PERIODÍSTICAS EN LA ERA DIGITAL[30]

África	Asia y el Pacífico	Estados Árabes	Europa y América del Norte	América Latina y el Caribe
Angola	Australia	Argelia	Andorra	Argentina
Benín	Bangladesh	Egipto	Armenia	Bolivia (Estado Plurinacional de)
Botswana	Camboya	Mauritania	Austria	Brasil
Burkina Faso	Bhután	Marruecos	Belarrús	Chile
Burundi	China	Djibouti	Bélgica	Colombia
Camerún	Timor Oriental	Sudán	Bosnia y Herzegovina	Costa Rica
Cabo Verde	Fiji	Siria	Bulgaria	República Dominicana
Chad	India		Canadá	Ecuador
Costa de Marfil	Indonesia		República Checa	El Salvador
República Democrática del Congo	Japón		Dinamarca	Guatemala
Etiopía	República de Corea		Estonia	Guyana
Zambia	Kiribati		Finlandia	Haití
Gambia	Kirguistán		Francia	Honduras
Ghana	Malasia		Georgia	México
Kenya	Nueva Zelanda		Alemania	Paraguay
Lesotho	Pakistán		Grecia	Panamá
Liberia	Palau		Hungría	Perú
Malawi	Singapur		Islandia	Uruguay
Malí	Sri Lanka		Irlanda	Venezuela, República Bolivariana de
Mauricio	Filipinas		Israel	Nicaragua
Mozambique	Uzbekistán		Italia	
Uganda	Tayikistán		Letonia	
Níger	Turkmenistán		Lituania	
Nigeria	Vanuatu		Luxemburgo	
Rwanda			Antigua República Yugoslava de Macedonia	
Senegal			Mónaco	
Zimbabwe			Países Bajos	
Sudáfrica			Noruega	
Swazilandia			Polonia	
Somalia			Portugal	
Tanzania			Federación Rusa	
Togo			Eslovaquia	
			España	
			Suecia	
			Suiza	
			Turquía	
			Reino Unido de Gran Bretaña e Irlanda del Norte	
			Estados Unidos de América	

30 Estados miembros seleccionados con arreglo a un estudio de 2007 a cargo de David Banisar, titulado *Silencing Sources: An International Survey of Protections and Threats to Journalists"Sources*. (Silenciamiento de las fuentes: Un estudio internacional de las protecciones y las amenazas que atañen a las fuentes periodísticas).

ANEXO 4: PROTECCIÓN DE LAS FUENTES PERIODÍSTICAS EN LA ERA DIGITAL – PREGUNTAS DE LA ENCUESTA

1. ¿Cuáles son los retos a) actuales y b) emergentes que atañen a la libertad de expresión en un entorno digital, en cuanto a su relación con la práctica del periodismo de investigación que se sirve de fuentes confidenciales?

2. ¿Qué leyes o instrumentos jurídicos existen actualmente en su país o región de actividad diseñados para proteger las fuentes periodísticas?

3. ¿Qué leyes o precedentes y políticas jurídicas se han derogado, sustituido o añadido desde 2007 en su país o región de actividad?

4. ¿En qué medida protegen estas leyes vigentes al periodismo de interfaz digital y a las fuentes periodísticas?

5. ¿Cómo podría o debería actualizarse la legislación que repercute en la protección de las fuentes periodísticas en la era digital?

    i) ¿Qué cambios en estas leyes son necesarios para proteger mejor a los periodistas y a sus fuentes en el intercambio de información y la publicación en un entorno digital?

    ii) ¿Qué cambios son necesarios en su país o región en concreto?

    iii) ¿Qué cambios podrían promulgarse mejor a través de instrumentos de política de escala mundial (como los de las Naciones Unidas)?

6. Sírvase identificar de uno a tres casos de su país o su región de actividad que pongan de relieve las cuestiones relativas a la protección de las fuentes periodísticas que, en su opinión, justifican un estudio más detenido. (Nota: nos interesan especialmente los estudios de caso que pongan de relieve la complejidad del intercambio de información y la publicación en un entorno digital, la emergencia de los periodistas ciudadanos, la repercusión de la legislación nacional sobre seguridad, y el conflicto entre la protección legislativa de las fuentes periodísticas y otros medios de protección como el derecho a la privacidad.)

7. ¿Es necesaria una protección específica de la libertad de expresión en Internet en lo que respecta a la práctica del periodismo de investigación? ¿Por qué/por qué no?

8. ¿Se han elaborado leyes, o se han visto o resuelto causas judiciales en su país (o región de actividad) que hayan definido o puesto a prueba la elegibilidad de los blogueros y periodistas ciudadanos para reclamar protección frente a la revelación de fuentes con arreglo a las leyes de secreto profesional? Sírvase consignar ejemplos al respecto.

9. ¿Tiene conocimiento de leyes, políticas formales o causas judiciales en las que se haya puesto en cuestión el asunto y el papel de los intermediarios terceros de Internet (como Google, Facebook o Twitter) en la protección de fuentes periodísticas (p. ej., casos en los que un sitio tercero puede tener acceso a datos que, si se revelan, podrían identificar a una fuente y en los que un tribunal exige a dicho sitio tercero que presente tales datos, eludiendo así el derecho legal o la obligación ética del periodista de proteger su fuente)? En caso afirmativo, sírvase explicar el caso.

10. ¿Ha puesto en marcha políticas, procedimientos o campañas diseñados para que periodistas e informantes tomen conciencia de los cambios en el entorno digital en lo que se refiere a la protección de las fuentes, en caso de que tales actividades le atañan a su organización? En caso afirmativo, sírvase explicar dichas actividades.

ANEXO 5: PROTECCIÓN DE LAS FUENTES PERIODÍSTICAS EN LA ERA DIGITAL – PREGUNTAS CUALITATIVAS DE LA ENCUESTA

a) Preguntas dirigidas a abogados, activistas de los derechos humanos y ONG

1. ¿Cuál es el grado de seguridad existente en lo que atañe a la protección jurídica de las fuentes periodísticas en la era digital?

2. Según su experiencia, ¿cuáles son las principales amenazas y retos emergentes en lo que se refiere a la protección de las fuentes?

3. ¿En qué medida es significativa la amenaza de la vigilancia masiva (del Estado y de las empresas) para la efectividad de las leyes sobre protección de las fuentes en su región/trabajo? (Sírvase consignar ejemplos al respecto.)

4. ¿Cuál es el papel de la legislación nacional en materia de seguridad y lucha contra el terrorismo (que ejerce un efecto limitador en las leyes de protección de las fuentes) en el menoscabo de estas leyes? ¿Cómo se manifiesta este problema en su región? (Sírvase consignar ejemplos al respecto.)

5. ¿Qué nuevas presiones cree que se ejercen respecto a la protección de las fuentes periodísticas y la actuación de intermediarios terceros como Facebook, Twitter, Google, las empresas de telefonía móvil y los PSI en lo que atañe a la conservación y la entrega de datos (a tribunales, gobiernos, etc.)? (Sírvase consignar ejemplos al respecto.)

6. ¿A quiénes deberían aplicarse las leyes de protección de las fuentes en la era digital? ¿A periodistas profesionales (en tal caso, ¿cómo los definimos?)? ¿A todos los agentes de los medios de comunicación? ¿O deberíamos vincular más bien la protección a los “actos de periodismo” (y de nuevo en este caso, ¿cómo definiríamos tales actos?)?

7. ¿Es posible en la práctica que los periodistas sigan prometiendo confidencialidad a las fuentes si consideramos los efectos de la vigilancia masiva, la conservación de datos y el efecto fundamental de la legislación sobre seguridad nacional y lucha contra el terrorismo, ya que estos factores socavan las protecciones jurídicas aplicadas tradicionalmente para que los periodistas puedan evitar que sus fuentes sean reveladas?

8. ¿Cómo puede reforzarse la protección jurídica de las fuentes en la era digital? ¿Es posible, por ejemplo, considerar la adopción de exclusiones legales para proteger a los periodistas (o a sus datos) de su exposición derivada de la vigilancia masiva?

9. ¿Qué piensa de este marco propuesto para evaluar las leyes de protección de las fuentes en la era digital? Sírvase comentar cada uno de los puntos a discreción. ¿Qué excluiría o añadiría a la lista para que pudiese funcionar como herramienta de medición de la efectividad de las leyes de protección de las fuentes?

En condiciones ideales, una ley modelo de protección de las fuentes podría:

1. Reconocer el principio y el valor éticos de la protección de las fuentes para la sociedad.

2. Reconocer que la protección se extienda a todos los actos de periodismo, definidos en términos inclusivos.

3. Reconocer que la protección de las fuentes no conlleva ni el registro de los profesionales del periodismo, ni la concesión de licencias a los mismos.

4. Afirmar que la confidencialidad se aplica al uso de todo datos personal digital recabado por cualquier agente.

5. Definir las excepciones a todas las condiciones anteriores de manera muy restringida en lo que se refiere a los fines que permiten la limitación del principio.

6. Definir excepciones que requieran la conformidad con la provisión de necesidad; en otras palabras, que sean aplicables cuando no exista alternativa.

7. Definir un proceso judicial independiente, con posibilidad de recurso, para las excepciones autorizadas.

8. Tipificar como delito las infracciones arbitrarias y no autorizadas de la confidencialidad de las fuentes cometidas por terceros.

9. ¿Qué medida, en su caso, le gustaría ver adoptada en su región, o a escala internacional, respecto a la consolidación de la protección jurídica de las fuentes periodísticas?

b) Conjunto alternativo de preguntas para periodistas entrevistados

1. ¿En qué medida confía en la protección jurídica de las fuentes que se ofrece en su país o región en 2014?

2. ¿Cómo ha afectado a su confianza en la protección jurídica de las fuentes las nuevas cuestiones planteadas en la era digital? (sírvase desarrollar su respuesta)

   a) Vigilancia masiva - ¿tienen algún sentido las leyes que defienden el derecho de los periodistas a no divulgar las fuentes confidenciales (p. ej., las de secreto profesional) si la vigilancia masiva puede dar lugar a su desenmascaramiento en cualquier caso?

b) Leyes de conservación de datos (y los requerimientos asociados para que se entreguen determinados datos que se aplican a intermediarios terceros como Facebook, Twitter, Google y PSI).

c) Legislación en materia de seguridad nacional y lucha contra el terrorismo (en la medida en que limita el alcance de las leyes de protección de las fuentes).

3. ¿Qué efecto han tenido estos cambios en sus fuentes confidenciales? ¿Observa un efecto inhibidor en este sentido? ¿Están menos dispuestas a ofrecer información que anteriormente? (Sírvase consignar ejemplos al respecto.)

4. ¿Sigue creyendo que es posible prometer a las fuentes que mantendrán su confidencialidad y se beneficiarán de las medidas de protección jurídica existentes (en caso de que sean aplicables en su región)? Y ¿le produce alguna desazón desde el punto de vista ético seguir manteniendo tales promesas? En caso afirmativo, ¿por qué? En caso negativo, ¿por qué no?

5. ¿A quiénes deberían aplicarse las leyes de protección de las fuentes en la era digital? ¿a periodistas profesionales (en tal caso, ¿cómo los definimos?)? ¿A todos los agentes de los medios de comunicación? ¿O deberíamos vincular más bien la protección a los "actos de periodismo" (y de nuevo en este caso, ¿cómo definiríamos tales actos?)?

6. En la práctica ¿cómo está cambiando la inseguridad en torno a la protección de las fuentes el modo en que afronta el periodismo de investigación (p. ej., ¿está menos dispuesto a trabajar en determinadas historias que dependen de fuentes confidenciales?)? ¿Adapta sus prácticas periodísticas de otro modo? En tal caso, ¿cómo?

7. ¿Ha participado en iniciativas internacionales de colaboración en el ejercicio del periodismo de investigación? En caso afirmativo, ¿qué repercusión han tenido las cuestiones antes referidas en las investigaciones transfronterizas? ¿Cómo aborda las diferencias en las normas y las prácticas jurídicas internacionales en tales investigaciones? ¿Qué idea se ha hecho de la efectividad de las leyes de protección de las fuentes a escala global en este contexto?

8. ¿Cómo puede reforzarse la protección jurídica de las fuentes en la era digital? Por ejemplo, ¿deberían considerar los Estados la adopción de exclusiones legales para proteger a los periodistas (o a sus datos) de su exposición derivada de la vigilancia masiva o de la conservación o la entrega de datos? (¿Por qué/por qué no?) Asimismo, ¿debería controlarse con mayor rigor el efecto limitador de la legislación de seguridad nacional y lucha contra el terrorismo en las leyes de protección de las fuentes? (¿Por qué/por qué no?)

9. ¿Qué piensa de este marco propuesto para evaluar las leyes de protección de las fuentes en la era digital? Sírvase comentar cada uno de los puntos a discreción. ¿Qué excluiría o añadiría a la lista para que pudiese funcionar como herramienta de medición de la efectividad de las leyes de protección de las fuentes?

En condiciones ideales, una ley modelo de protección de las fuentes podría:

1. Reconocer el principio y el valor éticos de la protección de las fuentes para la sociedad.

2. Reconocer que la protección se extienda a todos los actos de periodismo, definidos en términos inclusivos.

3. Reconocer que la protección de las fuentes no conlleva ni el registro de los profesionales del periodismo, ni la concesión de licencias a los mismos.

4. Afirmar que la confidencialidad se aplica al uso de todo datos personal digital recabado por cualquier agente.

5. Definir las excepciones a todas las condiciones anteriores de manera muy restringida en lo que se refiere a los fines que permiten la limitación del principio.

6. Definir excepciones que requieran la conformidad con la provisión de necesidad; en otras palabras, que sean aplicables cuando no exista alternativa.

7. Definir un proceso judicial independiente, con posibilidad de recurso, para las excepciones autorizadas.

8. Tipificar como delito las infracciones arbitrarias y no autorizadas de la confidencialidad de las fuentes cometidas por terceros.

9. ¿Qué otra medida, en su caso, le gustaría ver adoptada en su región, o a escala internacional, respecto a la consolidación de la protección jurídica de las fuentes periodísticas?

SELECCIÓN BIBLIOGRÁFICA

Organización de las Naciones Unidas:

Comité para la Eliminación de la Discriminación Racial. 2002. Recomendación general 29, Discriminación basada en la ascendencia (61ª sesión, 2002), U.N. Doc. A/57/18 en 111 (2002), reimpreso en la Recopilación de las observaciones generales y recomendaciones generales adoptadas por órganos creados en virtud de Tratados de Derechos Humanos, U.N. Doc. HRI\GEN\1\Rev.6 en 223 (2003)

Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. 5 de octubre de 2012. Plan de Acción de Rabat sobre la prohibición de la apología del odio nacional, racial o religioso que constituye incitación a la discriminación, la hostilidad o la violencia. http://www.ohchr.org/Documents/Issues/Opinion/SeminarRabat/Rabat_draft_outcome.pdf

—. 2011. *Principios Rectores de la ONU sobre las Empresas y los Derechos Humanos*. Nueva York y Ginebra: Organización de las Naciones Unidas.

—. 16 de diciembre de 1966. *Pacto Internacional de Derechos Civiles y Políticos*. www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

Asamblea General de las Naciones Unidas. 11 de febrero de 2015. *Resolución adoptada por la Asamblea General el 18 de diciembre de 2014, 69/185. La seguridad de los periodistas y la cuestión de la impunidad*. A/RES/69/185. http://www.un.org/en/ga/search/view_doc.asp? symbol=A/RES/69/185

—. 23 de septiembre de 2014. *Informe del Relator Especial sobre la promoción y protección de los derechos humanos y las libertades fundamentales en la lucha contra el terrorismo.* A/69/397. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/N14/545/19/PDF/N1454519. pdf?OpenElement

—. 21 de febrero de 2014. *La seguridad de los periodistas y la cuestión de la impunidad: Resolución adoptada por la Asamblea General el 18 de diciembre de 2013*. A/RES/68/163. http://www.refworld.org/docid/53a7fab74.html

—. 20 de noviembre de 2013. *El derecho a la privacidad en la era digital. (A/C.3/68/167)* http://www.un.org/ga/search/view_doc.asp?symbol=A/RES/68/167

—. 1979. *Convención sobre la eliminación de todas las formas de discriminación contra la mujer*. http://www.un.org/womenwatch/daw/cedaw/

—. 16 de diciembre de 1966. *Pacto Internacional de Derechos Civiles y Políticos*. http://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

—. 10 de diciembre de 1948. *Declaración Universal de Derechos Humanos*. http://www.un.org/en/documents/udhr/

Asamblea General de las Naciones Unidas, Comité de Derechos Humanos. 5 de enero de 2015. *Informe de la Relatora Especial sobre cuestiones de las minorías, Rita Izsák*. A/HRC/28/64

—. 11-29 de julio de 2011. *Observación general 34.* http://www2.ohchr.org/english/bodies/ hrc/docs/gc34.pdf

—. 14 de julio de 2011. *Resolución 17/19, Derechos humanos, orientación sexual e identidad de género*. A/HRC/RES/17/19

—. 2000. *Observación general 28, La igualdad de derechos entre hombres y mujeres*, U.N. Doc. CCPR/C/21/Rev.1/Add.10

—. 1993. *Observación general 22, artículo 18* (48ª sesión). Recopilación de las observaciones generales y recomendaciones generales adoptadas por órganos de derechos humanos creados en virtud de tratados, U.N. Doc. HRI\GEN\1\ Rev.1 en 35 (1994)

Consejo de Derechos Humanos de la ONU. 22 de mayo de 2015. *Informe del Relator Especial para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión, David Kaye* A/HRC/29/32. http://www.ohchr.org/EN/Issues/FreedomOpinion/Pages/ CallForSubmission.aspx

—. 2 de octubre de 2014. *Resolución adoptada por el Consejo de Derechos Humanos, 27/5: La seguridad de los periodistas.* A/HRC/RES/27/5 http://daccess-dds-ny.un.org/doc/UNDOC/ GEN/G14/177/81/ PDF/G1417781.pdf?OpenElement

—. 23 de julio de 2014. *Mesa redonda sobre la seguridad de los periodistas: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.* A/HRC/27/35. http://www.refworld.org/docid/53eb46d34.html

—. 30 de junio de 2014. *El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.* A/HRC/27/37. www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session27/Documents/A.HRC.27.37_en.pdf

—. 1 de julio de 2013. *La seguridad de los periodistas: Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos.* A/HRC/24/23. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G13/153/19/PDF/G1315319.pdf?OpenElement

—. 17 de abril de 2013. *Informe del Relator Especial para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión*. A/HRC/23/40. http://www.refworld.org/docid/51a5ca5f4.html

—. 9 de octubre de 2012. *La seguridad de los periodistas: resolución adoptada por el Consejo de Derechos Humanos.* A/HRC/RES/21/12 http://www.refworld.org/docid/50adf4812.html

—. 16 de julio de 2012. *Promoción, protección y disfrute de los derechos humanos en Internet.* A/HRC/RES/20/8 http://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/RES/20/8

—. 4 de junio de 2012. *Informe del Relator Especial para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión, Frank La Rue. A*/HRC/20/17. http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session20/A-HRC-20-17_en.pdf

—. 16 de mayo de 2011. *Informe del Relator Especial para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión, Frank La Rue.* A/HRC/17/27. http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf

—. 20 de abril de 2010. *Informe del Relator Especial para la Promoción y la Protección del Derecho a la Libertad de Opinión y de Expresión, Frank La Rue.* A/HRC/14/23. http://www2.ohchr.org/english/bodies/hrcouncil/docs/14session/A.HRC.14.23.pdf

—. 16 de enero de 2009. *Informe del Alto Comisionado para los Derechos Humanos Adición Seminario de expertos sobre la relación entre los artículos 19 y 20 del Pacto Internacional de Derechos Civiles y Políticos, A/HRC/10/31/Add.3.* http://www2.ohchr.org/ english/issues/opinion/articles1920_iccpr/docs/A-HRC-10-31-Add3.pdf

—. 10 de septiembre de 2006. *Incitación al odio racial y religioso y promoción de la tolerancia: informe de la Alta Comisionada de las Naciones Unidas para los Derechos Humanos*. A/HRC/2/6. http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G06/139/97/PDF/G0613997.pdf? OpenElement

Oficina de Naciones Unidas contra la Droga y el Delito. 2013. *Estudio mundial sobre el homicidio.* http://www.unodc.org/gsh/

—. 2003. *Convención de las Naciones Unidas contra la corrupción* https://www.unodc.org/documents/treaties/UNCAC/Publications/Convention/08-50026_E.pdf

Radio ONU. 12 de julio de 2013. 'Human Rights chief urges respect for right to privacy and protection of individuals revealing human rights violations'. http://www.unmultimedia. org/radio/english/2013/07/human-rights-chief-urges-respect-for-right-to-privacy-and-protection-of-individuals-revealing-human-rights-violations/

Consejo de Seguridad de la ONU. 27 de mayo de 2015. *Resolución 2222 (2015):* adoptada por el Consejo de Seguridad en su 7.450ª sesión, el 27 de mayo de 2015. S/RES/2222 (2015). http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_res_2222.pdf

—. 22 de noviembre de 2013. *Informe del Secretario General sobre la protección de los civiles en los conflictos armados.* S/2013/689. http://www.securitycouncilreport.org/atf/cf/%7B65BFCF9B-6D27-4E9C-8CD3-CF6E4FF96FF9%7D/s_2013_689.pdf

UNESCO

Daudin Clavaud, P. y T. Mendel. 2015. *Freedom of Expression and Public Order: Training manual*. París: UNESCO. http://unesdoc.unesco.org/images/0023/002313/231305e.pdf

Dutton, W. H. y cols. 2011. *Freedom of Connection – Freedom of Expression: The Changing Legal and Regulatory Ecology Shaping the Internet*. UNESCO Series on Internet Freedom. París: UNESCO. http://unesdoc.unesco.org/images/0019/001915/191594e.pdf

Gagliardone, I. y cols. 2015. *Countering Online Hate Speech* (Contrarrestar la incitación al odio en Internet) UNESCO Series on Internet Freedom. París: UNESCO. http://unesdoc.unesco.org/images/0023/002332/233231e.pdf

Henrichsen, J. R., M. Betz y J. M. Lisosky 2015. *Building Digital Safety for Journalism: A Survey of Selected Issues*. París: UNESCO. http://unesdoc.unesco.org/images/0023/ 002323/232358e.pdf

MacKinnon, R. y cols. 2014. *Fostering Freedom Online: The Role of Internet Intermediaries*. UNESCO Series on Internet Freedom. París: UNESCO / Internet Society. http://unesdoc.unesco.org/images/0023/002311/231162e.pdf

Mendel, T. y cols. 2012. *Global Survey on Internet Privacy and Freedom of Expression*. UNESCO Series on Internet Freedom. París: UNESCO. http://unesdoc.unesco.org/ images/0021/002182/218273e.pdf

UNESCO. Educación para la ciudadanía mundial. http://www.unesco.org/new/en/global-citizenship-education

—. 2015. *Keystones to foster inclusive Knowledge Societies: Access to information and knowledge, Freedom of Expression, Privacy, and Ethics on a Global Internet*. París: UNESCO. http://unesdoc.unesco.org/images/0023/002325/232563E.pdf

—. 17 de marzo de 2015. *Decisión 196 EX/31 sobre la Seguridad de los Periodistas y la Cuestión de la Impunidad*. Adoptada en la 196ª Sesión del Consejo Ejecutivo de la UNESCO. http://unesdoc.unesco.org/images/0023/002323/232337e.pdf

—. 2014. *Tendencias Mundiales en Libertad de Expresión y Desarrollo de los Medios.* París: UNESCO. www.unesco.org/new/en/communication-and-information/resources/publications-and-communication-materials/publications/full-list/world-trends-in-freedom-of-expression-and-media-development

—. Julio de 2014. *Internet Universality: A Means towards Building Knowledge Societies and the Post-2015 Sustainable Development Agenda*. Proyecto elaborado por la Secretaría. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/Internet_universality_summary_240314_en.pdf

—. Mayo de 2014. *Declaración de París sobre la alfabetización mediática e informacional en la era digital*. http://www.unesco.org/new/en/communication-and-information/resources/news-and-in-focus-articles/in-focus-articles/2014/paris-declaration-on-media-and-information-literacy-adopted/

—. 2013. *Proyecto de Estrategia a Plazo Medio: 2014–2021 (37 C/4)*. París: UNESCO. http://unesdoc.unesco.org/images/0022/002200/220031e.pdf

—. Noviembre de 2013. *Resolución sobre cuestiones relacionadas con Internet, con inclusión del acceso a la información y el conocimiento, la libertad de expresión, la privacidad y las dimensiones éticas de la sociedad de la información.* 37ª Sesión de la Conferencia General. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/news/37gc_resolution_Internet.pdf

—. 25 de octubre - 10 de noviembre de 2011. *Actas de la Conferencia General, 36ª sesión.* Volumen 1: Resoluciones. http://unesdoc.unesco.org/images/0021/002150/215084e.pdf

UNESCO, Consejo Intergubernamental del Programa Internacional para el Desarrollo de la Comunicación (PIDC). 20-21 de noviembre de 2014. *Decisiones adoptadas por el 29ª sesión del Consejo del PIDC.* Sala X, Sede de la UNESCO, París. http://www.unesco.org/new/fileadmin/MULTIMEDIA/HQ/CI/CI/pdf/IPDC/ipdc29EN_IPDC29_FULL_DECISIONS_FINAL.pdf

—. 22-23 de marzo de 2012. *Informe final (28ª sesión).* UNESCO: París: http://unesdoc.unesco.org/images/0021/002199/219910E.pdf

—. 24-26 de marzo de 2010. *Informe final (27ª sesión).* UNESCO: París: http://unesdoc.unesco.org/images/0018/001896/189697m.pdf

—. 26-28 de marzo de 2008. *Informe final (26ª sesión).* UNESCO: París: http://unesdoc.unesco.org/images/0016/001634/163437m.pdf

UNESCO, Programa Internacional para el Desarrollo de la Comunicación (PIDC). 2014. *La seguridad de los periodistas y el peligro de la impunidad - Informe del Director General al Consejo Intergubernamental del PIDC (29ª Sesión).* CI-14/CONF.202/4 Rev2. París: http://unesdoc.unesco.org/images/0023/002301/230101E.pdf

Otras organizaciones intergubernamentales:

Comisión Africana de Derechos Humanos y de los Pueblos. 17-23 de octubre de 2002. Declaración de principios sobre la libertad de expresión en África, 32ª Sesión, Banjul.

APEC Cross-Border Privacy Rules System. http://www.cbprs.org/

Asociación de Naciones del Asia Sudoriental (ASEAN) 19 de noviembre de 2012. *Declaración de Derechos Humanos de la ASEAN.* http://www.asean.org/news/asean-statement-communiques/item/asean-human-rights-declaration

Benedek, W. y M. C. Kettemann. Diciembre de 2013. *Freedom of Expression and the Internet*. Estrasburgo: Consejo de Europa. https://book.coe.int/eur/en/human-rights-and-democracy/5810-freedom-of-expression-and-the-Internet.html

Bigo y cols. 2013. *National Programmes for Mass Surveillance of Personal Data in EU Member States and their compatibility with EU Law.* Parlamento Europeo. http://www.europarl.europa.eu/RegData/etudes/etudes/join/2013/493032/IPOL-LIBE_ET%282013%29493032_EN.pdf

Botero Marino, C. 2014, 22 de abril. *Informe anual de la Comisión Interamericana de Derechos Humanos, 2013: Informe anual de la Oficina del relator especial para la libertad de expresión, volumen ii.* Washington, D.C.: Organización de Estados Americanos. http://www.oas.org/en/iachr/expression/docs/reports/2014_04_22_%20IA_2013_ENG%20_FINALweb.pdf

—. 31 de diciembre de 2013. *Violencia contra periodistas y trabajadores de medios: Estándares interamericanos y prácticas nacionales sobre prevención, protección y procuración de la justicia. Oficina de la Relatoría Especial para la Libertad de Expresión, Comisión Interamericana de Derechos Humanos.* http://www.oas.org/en/iachr/expression/ docs/reports/2014_04_22_Violence_WEB.pdf

—. 2012. *Informe anual de la Comisión Interamericana de Derechos Humanos, volumen II, Informe de la Oficina de la Relatoría Especial para la Libertad de Expresión*

Broadband Commission Working Group on Broadband and Gender. Septiembre de 2013. *Doubling Digital Opportunities: Enhancing the Inclusion of Women & Girls in the Information Society*. Ginebra: Unión Internacional de Telecomunicaciones. www.broadbandcommission.org/Documents/working-groups/bb-doubling-digital-2013.pdf

Consejo de Europa. 16 de abril de 2014. *Recomendación del Consejo de Ministros a los Estados miembros sobre una Guía de los derechos humanos para los usuarios de Internet*. (CM/Rec(2014)6.) https://wcd.coe.int/ViewDoc.jsp?id=2184807

—. 15 de abril de 2012. *Mapping study on projects against hate speech online*. Estrasburgo. https://www.coe.int/t/dg4/youth/Source/Training/Training_courses/2012_Mapping_projects_against_Hate_Speech.pdf

—. 26 de septiembre de 2007. *Directrices del Comité de Ministros del Consejo de Europa sobre la protección de la libertad de expresión e información en épocas de crisis*, 1.005ª sesión. https://wcd.coe.int/ViewDoc.jsp?id=1188493

—. 28 de enero de 2003. *Protocolo adicional al Convenio sobre la Ciberdelincuencia relativo a la penalización de actos de índole racista y xenófoba cometidos por medio de sistemas informáticos*

—. 23 de noviembre de 2001. *Convenio sobre la Ciberdelincuencia*

Consejo de Europa, Comité de Ministros. 28 de mayo de 2003. *Declaración sobre la libertad de comunicación en Internet.* (Decl-28.05.2003E.) https://wcd.coe.int/ViewDoc.jsp?id=37031

—. 2000. *Recomendación sobre el "derecho de los periodistas a no revelar sus fuentes de información"*. http://www.coe.int/t/dghl/standardsetting/media/doc/cm/rec%282000%29007& expmem_EN.asp

Consejo de Europa, Comisario para los Derechos Humanos. 4 de octubre de 2011. 'Protection of journalists from violence: Issue discussion paper'. https://wcd.coe.int/ ViewDoc.jsp?id=1899957https://wcd.coe.int/ViewDoc.jsp?id=1899957

Consejo de Europa, Comisión Europea contra el Racismo y la Intolerancia (ECRI). 15 de diciembre de 2000. *Recomendación nº 6 de política general de la ECRI: Combating the dissemination of racist, xenophobic and antisemitic materiel via the Internet.* http://www.coe.int/t/dghl/monitoring/ecri/activities/gpr/en/recommendation_n6/Recommendation_6_en.asp

Consejo de Europa, Asamblea Parlamentaria. 25 de enero de 2011. Recomendación 1950: La protección de las fuentes periodísticas. http://assembly.coe.int/ Mainf.asp?link=/ Documents/AdoptedText/ta11/EREC1950.htm

Tribunal de Justicia de la Unión Europea. 8 de abril de 2014. El Tribunal de Justicia declara inválida la Directiva sobre la conservación de datos. Comunicado de prensa nº. 54/14. http://curia.europa.eu/jcms/upload/docs/application/pdf/2014-04/cp140054en.pdf

Edwards, L. 2011, 22 de junio. *Role and Responsibility of Internet Intermediaries in the Field of Copyright and Related Rights*. Ginebra: Organización Mundial de la Propiedad Intelectual. (WIPO-ISOC/GE/11/REF/01/EDWARDS). www.wipo.int/export/sites/www/copyright/en/doc/role_and_responsibility_of_the_Internet_intermediaries_final.pdf

Comisión Europea. 16 de julio de 2013. *Overview on Binding Corporate Rules. Data Protection*. http://ec.europa.eu/justice/data-protection/document/international-transfers/binding-corporate-rules/index_en.htm

—. 28 de noviembre de 2008. *Decisión marco relativa al racismo y la xenofobia.* http://ec.europa.eu/justice/fundamental-rights/racism-xenophobia/framework-decision/ index_en.htm

—. 4 de mayo de 2000. *Directiva sobre comercio electrónico.* (2000/31/EC). http://ec.europa.eu/ internal_market/e-commerce/directive/index_en.htm

Tribunal Europeo de Derechos Humanos. 1996. *Goodwin v. Reino Unido*. http://hudoc.echr.coe.int/ sites/eng/pages/search.aspx?i=001-57974

Parlamento Europeo y Consejo de la Unión Europea. 22 de mayo de 2011. *Directiva 2001/29/CE del Parlamento Europeo y del Consejo, de 22 de mayo de 2001, relativa a la armonización de determinados aspectos de los derechos de autor y derechos afines a los derechos de autor en la sociedad de la información.* http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32001L0029

Unión Europea. 2000. *Carta de los Derechos Fundamentales de la Unión Europea.* http://ec.europa.eu/justice/fundamental-rights/charter/

Horsley, W. 2012. *OSCE Safety of journalists guidebook*. Oficina del Representante para la libertad de los medios de comunicación de la OSCE. https://www.osce.org/fom/85777?download=true

Hulin, A. (Ed.). 2013. *Joint Declarations of the representatives of intergovernmental bodies to protect free media and expression.* Viena: Organización para la Seguridad y la Cooperación en Europa. www.osce.org/fom/99558?download=true

Comisión Interamericana de Derechos Humanos. 20 de octubre de 2000. *Declaración Interamericana de Principios sobre Libertad de Expresión*

—. 13 de noviembre de 1985. *Opinión consultiva OC-5/85*

Corte Interamericana de Derechos Humanos. 2009. 28 de enero. Asunto de *Ríos y otros. v. Venezuela*. http://corteidh.or.cr/docs/casos/articulos/seriec_194_ing.pdf

ISO/IEC. Marzo de 2004. FDIS 11179-1. 'Information technology - Metadata registries - Part 1: Framework'. http://stats.oecd.org/glossary/detail.asp?ID=4575

Liga de los Estados Árabes. 22 de mayo de 2004. Carta Árabe de Derechos Humanos. Entró en vigor el 15 de marzo de 2008.

Ministers of the Freedom Online Coalition. *Recommendations for Freedom Online*. Adoptadas en Tallin, Estonia, el 28 de abril de 2014. https://www.freedomonlinecoalition.com/wp-content/uploads/2014/04/FOC-recommendations-consensus.pdf

Organización de Cooperación y Desarrollo Económicos. 13 de diciembre de 2011. *Recomendación del Consejo de la OCDE sobre Principios para la Elaboración de Políticas de Internet*. www.oecd.org/Internet/ieconomy/49258588.pdf

—. Septiembre de 2011. *The Role of Internet Intermediaries in Advancing Public Policy Objectives*. París: OECD http://browse.oecdbookshop.org/oecd/pdfs/product/9311031e.pdf

Organización de Estados Americanos. *Convención Americana sobre Derechos Humanos "Pacto de San José, Costa Rica" (B-32).* http://www.oas.org/dil/treaties_B-32_American_Convention_on_Human_Rights.htm

—. 2011. *Colegiación obligatoria para el ejercicio del periodismo profesional* http://www.oas.org/en/iachr/expression/showarticle.asp?artID=154&lID=1

Organización de la Conferencia Islámica. 5 de agosto de 1990. *Declaración de El Cairo sobre Derechos Humanos en el Islam*, preámbulo

Organización de Cooperación Islámica. Diciembre de 2013. *Sixth OIC Observatory Report on Islamophobia*. Presentado ante el 40º Consejo de Ministros de Asuntos Exteriores, Conakry, República de Guinea.

Organización para la Seguridad y la Cooperación en Europa. *Despenalización de la difamación.* www.osce.org/fom/106287

—. 8 de junio de 2011. *Recomendaciones de Vilnius para la seguridad de los periodistas.* http://www.osce.org/cio/78522

Perset, K. / OCDE. Marzo de 2010. *The Economic and Social Role of Internet Intermediaries*. (DSTI/ICCP(2009)9/FINAL). París: OCDE. www.oecd.org/Internet/ieconomy/44949023.pdf

Otros documentos y recursos

Access Now. *Telco Remedy Plan*. https://www.accessnow.org/telco-remedy-plan

ARTICLE 19. Abril de 2009. *Los Principios de Camden Sobre La Libertad de Expresión y la Igualdad.* https://www.article19.org/data/files/pdfs/standards/the-camden-principles-on-freedom-of-expression-and-equality.pdf

Broadband Stakeholder Group (Reino Unido). *Voluntary industry code of practice on traffic management transparency for broadband services.* http://www.broadbanduk.org/wp-content/uploads/2013/08/Voluntary-industry-code-of-practice-on-traffic-management-transparency-on-broadband-services-updated-version-May-2013.pdf

The Center for Internet and Society. Julio de 2014. *World Intermediary Liability Map (WILMap)*. Stanford, Calif.: Stanford Law School. http://cyberlaw.stanford.edu/our-work/projects/world-intermediary-liability-map-wilmap

Chilling Effects. http://www.chillingeffects.org

Comité para la Protección de los Periodistas. 1 de diciembre de 2014. *2014 prison census: 221 journalists jailed worldwide*. https://cpj.org/imprisoned/2014.php

—. 1 de diciembre de 2013. *2013 prison census: 211 journalists jailed worldwide*. https://cpj.org/imprisoned/2013.php

Electronic Frontier Foundation. *Takedown Hall of Shame.* https://www.eff.org/takedowns

—. 2014. *Who Has Your Back? Protecting Your Data From Government Requests.* https://www.eff.org/who-has-your-back-2014

Instituto Universitario Europeo, Centre for Media Pluralism and Media Freedom. 2014. *Status of European Journalists*. http://journalism.cmpf.eui.eu/maps/journalists-status/

Facebook. *Normas comunitarias*. https://www.facebook.com/communitystandards

Global Network Initiative. *Directrices de ejecución.* https://globalnetworkinitiative.org/implementationguidelines/index.php

—. *Principios.* http://www.globalnetworkinitiative.org/principles/

Google. *Informe de transparencia.* http://www.google.com/transparencyreport/

Hatebase. *Most Common Hate Speech*. http://www.hatebase.org/popular

In Other Words Project. 2013. *Toolbox*. http://www.inotherwords-project.eu/sites/default/files/Toolbox.pdf

Internet Live Stats. 2014. *Internet Users by Country*. www.Internetlivestats.com/Internet-users-by-country

MediaSmarts *Facing online hate*. http://mediasmarts.ca/tutorial/facing-online-hate-tutorial

Microsoft, Centro de Desarrollo de Windows. "11.0 Políticas de contenidos". *Aplicaciones de Windows*. https://msdn.microsoft.com/en-us/library/windows/apps/Dn764940.aspx

Microsoft, Xbox. Enero de 2014. *Código de conducta de Xbox Live.* http://www.xbox.com/en-GB/legal/codeofconduct

Necessary and Proportionate. 10 de julio de 2013. *Principios Internacionales sobre la Aplicación de los Derechos Humanos a la Vigilancia de las Comunicaciones.* https://en.necessaryandproportionate.org/text

No Hate Speech Movement. 2013. *Herramientas y materiales de las campañas.* http://nohate.ext.coe.int/Campaign-Tools-and-Materials

—. 2013. *No Hate Ninja Project - A Story About Cats, Unicorns and Hate Speech.* https://www.youtube.com/watch?v=kp7ww3KvccE

Ofcom. 22 de julio de 2014. *Report on Internet safety measures - Internet Service Providers: Network level filtering measures*. http://stakeholders.ofcom.org.uk/Internet/Internet-safety-2?utm_source=updates&utm_medium=email&utm_campaign=filtering-report

Online Hate Prevention Institute. *Fight Against Hate*. http://fightagainsthate.com/

Open Rights Group. Julio de 2014. *Blocked! The personal cost of filters*. https://www.blocked.org.uk/personal-stories

OpenNet Initiative. About Filtering. https://opennet.net/about-filtering

Organización de Cooperación y Desarrollo Económicos. Marzo de 2014. *The CleanGovBiz Toolkit for Integrity*. http://www.oecd.org/cleangovbiz/CGB-Toolkit-2014.pdf

Reporteros sin Fronteras. *2014: Journalists Imprisoned*. https://en.rsf.org/press-freedom-barometer-journalists-imprisoned.html?annee=2014

—. *2013: Journalists Imprisoned*. https://en.rsf.org/press-freedom-barometer-journalists-imprisoned.html?annee=2013

Diálogo de la industria de las telecomunicaciones: Principios sobre libertad de expresión y privacidad. 16 de marzo de 2013. *Principios rectores*. http://www.vodafone.com/ content/dam/sustainability/pdfs/telecom_industry_dialogue_principles.pdf

Tell MAMA (Measuring Anti-Muslim Attacks). 2014. http://tellmamauk.org

Terms of Service; Didn't Read. https://tosdr.org/

Twitter. *Reglas de Twitter*. https://support.twitter.com/articles/18311

—. 18 de mayo de 2015. *Condiciones de servicio de Twitter.* https://twitter.com/tos?lang=en

UC Berkeley Library. *Invisible or Deep Web: What it is, How to find it, and Its inherent ambiguity*. http://www.lib.berkeley.edu/TeachingLib/Guides/Internet/InvisibleWeb.html

UNESCO. *La UNESCO condena los asesinatos de periodistas*. http://www.unesco.org/new/en/condemnation

WAM! *WAM Twitter harassment reporting tool*. https://womenactionmedia.wufoo.com/forms/ztaetji1jrhv10/

YouTube. *Normas de la comunidad.* http://www.youtube.com/yt/policyandsafety/communityguidelines.html

Libros, artículos e informes

African Gender Institute. 2013, December. *Feminist Africa*, Vol. 18, 'e-spaces: e-politics'. http://agi.ac.za/sites/agi.ac.za/files/fa18_web-1.pdf

Albanian Media Institute. 2014. *Hate speech in online media in South East Europe.* http://www.institutemedia.org/Documents/PDF/Hate%20speech%20in%20online%20media%20in%20SEE.pdf

Alston, P. (Ed.). 2005. *Non-State Actors and Human Rights*. Oxford: Oxford University Press.

Alves, R. 2014. 'Trends in global collaborative journalism', *Trends in Newsrooms 2014,* Darmstadt, Germany: WAN-IFRA, pp. 83-87

Andrejevic, M. 2014. Wikileaks, Surveillance, and Transparency. *International Journal of Communication*, 8, pp. 2619–2630

Athique, A. 2013. *Digital Media and Society: An Introduction*. Polity.

Banisar, D. 2008, November. *Speaking of terror: A survey of the effects of counter-terrorism legislation on freedom of the media in Europe*. Council of Europe, Media and Information Society Division Directorate General of Human Rights and Legal Affairs. http://www.coe.int/t/dghl/standardsetting/media/Doc/SpeakingOfTerror_en.pdf

—. 2007. *Silencing Sources: An international survey of protections and threats to journalists' sources*. Privacy International. http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1706688 accessed 25/6/2014

Bankston, K., D. Sohn and A. McDiarmid. 2012, December. *Shielding the Messengers: Protecting Platforms for Expression and Innovation*. Washington DC: Center for Democracy and Technology. www.cdt.org/files/pdfs/CDT-Intermediary-Liability-2012.pdf

Barton, A. and H. Storm. 2014. *Violence and Harassment against Women in the News Media: A Global Picture*. International Women's Media Foundation and International News Safety Institute. http://www.iwmf.org/wp-content/uploads/2014/03/Violence-and-Harassment-against-Women-in-the-News-Media.pdf

Bauman, Z. et al. 2014. After Snowden: Rethinking the Impact of Surveillance. *International Political Sociology*, 8:2, 121-140

Bayley, E. 2009, 16 November. *The Clicks that Bind: Ways Users 'Agree' to Online Terms of Service.* Electronic Frontier Foundation. https://www.eff.org/wp/clicks-bind-ways-users-agree-online-terms-service

Benesch, S. 2012. Words as Weapons. *World Policy Journal*, vol. 29, no. 1, pp. 7-12

—. 2012, 12 January. 'Dangerous Speech: A Proposal to Prevent Group Violence'. New York: World Policy Institute. http://www.worldpolicy.org/sites/default/files/Dangerous%20Speech%20Guidelines%20Benesch%20January%202012.pdf

Bently, L. and B. Sherman. 2009. *Intellectual Property Law*, 3rd ed. Oxford: Oxford University Press.

Bergman, M. K. 2001, August. White Paper: The Deep Web: Surfacing Hidden Value. *Taking License*. Vol. 7, Issue 1. http://quod.lib.umich.edu/j/jep/3336451.0007.104

Beschastna, T. 2014. Freedom of Expression in Russia as it Relates to Criticism of the Government. *Emory International Law Review*, Vol. 27, No. 2. http://law.emory.edu/eilr/ content/volume-27/issue-2/comments/freedom-expression-russia.html

Black, J. 1996, January. Constitutionalising Self-Regulation. *The Modern Law Review*, Vol. 59, No. 1, pp. 24-55. http://dx.doi.org/10.1111/j.1468-2230.1996.tb02064.x

BSR, with CDT. 2014, September. *Legitimate and Meaningful Stakeholder Engagement in Human Rights Due Diligence: Challenges and Solutions for ICT Companies*. http://www.bsr.org/reports/BSR_Rights_Holder_Engagement.pdf

Budish, R. 2013, 19 December. 'What Transparency Reports Don't Tell Us'. *The Atlantic*. www.theatlantic.com/technology/archive/2013/12/what-transparency-reports-dont-tell-us/282529

Business and Human Rights Resource Centre. 2010, September. *The UN 'Protect, Respect and Remedy' Framework for Business and Human Rights*. www.reports-and-materials.org/ sites/default/files/reports-and-materials/Ruggie-protect-respect-remedy-framework.pdf

Buyse, A. 2014. Words of Violence: 'Fear Speech,' or How Violent Conflict Escalation Relates to the Freedom of Expression. *Human Rights Quarterly*, vol. 36, no. 4, pp. 779–97

Castells, M. 2012. *Networks of Outrage and Hope: Social Movements in the Internet Age*. Cambridge: Polity

Chin, Y. C. 2013, August. Regulating social media. Regulating life (and lives). *RJR 33 Online*, http://journalism.hkbu.edu.hk/doc/Regulating_social-Media.pdf

Citron, K. D. and H. Norton. 2011. Intermediaries and hate speech: Fostering digital citizenship for our information age. *Boston University Law Review,* vol. 91, pp. 1435-84

Comninos, A. 2012, October. *The Liability of Internet Intermediaries in Nigeria, Kenya, South Africa, and Uganda: An Uncertain Terrain*. South Africa: Association for Progressive Communications. www.apc.org/en/system/files/READY%20-%20Intermediary%20Liability%20in%20Africa_FINAL.pdf

—. 2012, October. *Intermediary liability in South Africa*. Intermediary Liability in Africa Research Papers, No. 3. South Africa: Association for Progressive Communications. www.apc.org/en/system/files/Intermediary_Liability_in_South_Africa-Comninos_06.12.12.pdf

Cotter, T. F. 2005. Some Observations on the Law and Economics of Intermediaries. *Michigan State Law Review*, Vol. 1, pp. 1-16. Washington & Lee Legal Studies Paper No. 2005-14. http://ssrn.com/abstract=822987

Das, S. and A. Kramer. 2013. Self-Censorship on Facebook. *Proceedings of the Seventh International Association for the Advancement of Artificial Intelligence (AAAI) Conference on Weblogs and Social Media*, pp. 120-27. www.aaai.org/ocs/index.php/ICWSM/ICWSM13/paper/viewFile/6093/6350

Davies, S. (Ed.). 2014, June. A Crisis of Accountability: A global analysis of the impact of the Snowden revelations. *Privacy Surgeon*. www.privacysurgeon.org/blog/wp-content/uploads/2014/06/Snowden-final-report-for-publication.pdf

Defeis, E.F., 1992. Freedom of speech and international norms: A response to hate speech. *Stan. Journal of International Law*, vol. 29, pp. 57-74

Deibert, R. et al. (Eds). 2010, April. *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*. Cambridge, Mass.: MIT Press. http://mitpress.mit.edu/books/access-controlled

—. 2008. January. *Access Denied: The Practice and Policy of Global Internet Filtering.* Cambridge, Mass.: MIT Press. https://mitpress.mit.edu/books/access-denied

DeNardis, L. 2013, August. Internet Points of Control as Global Governance. Internet Governance Papers. No.2. Centre for International Governance Innovation. http://www.cigionline.org/sites/default/files/no2_3.pdf

Diamond, L. 2010, July. Liberation technology. *Journal of Democracy*, Vol. 21, No. 3, pp. 69-83. www.journalofdemocracy.org/articles/gratis/Diamond-21-3.pdf

Electronic Frontier Foundation. 2011, January. *Freedom of Expression, Privacy and Anonymity on the Internet*. https://www.eff.org/Frank-La-Rue-United-Nations-Rapporteur

Epstein, G. 3 March 2011. Sina Weibo. *Forbes Asia*. www.forbes.com/global/2011/0314/features-charles-chao-twitter-fanfou-china-sina-weibo.html

Foxman, A.H. and C. Wolf. 2013. Viral hate: Containing its spread on the Internet. Macmillan

Ghanea, N. 2013. Intersectionality and the Spectrum of Racist Hate Speech: Proposals to the UN Committee on the Elimination of Racial Discrimination. *Human Rights Quarterly*, vol. 35, no. 4, pp. 935-54. http://dx.doi.org/10.1353/hrq.2013.0053

Gillespie, T. 2010. The Politics of 'Platforms'. *New Media & Society*, vol. 12, no. 3, pp. 347-64. http://dx.doi.org/10.1177/1461444809342738

Giroux, H. 2015. Totalitarian Paranoia in the Post-Orwellian Surveillance State. *Cultural Studies*, vol. 29, no. 2, pp. 108-140

Global Network Initiative. 2014, January. *Public Report on the Independent Assessment Process for Google, Microsoft, and Yahoo*. http://globalnetworkinitiative.org/sites/default/files/ GNI%20Assessments%20Public%20Report.pdf

Goldsmith, J.L. and T. Wu. 2006. *Who controls the Internet? Illusions of a borderless world*. Oxford: Oxford University Press. http://jost.syr.edu/wp-content/uploads/who-controls-the-Internet_illusions-of-a-borderless-world.pdf

Goodman, E. and F. Cherubini. 2013. *Online comment moderation: emerging best practices. A guide to promoting robust and civil online conversation*. World Association of Newspapers and News Publishers (WAN-IFRA). http://www.wan-ifra.org/reports/2013/10/04/online-comment-moderation-emerging-best-practices

Grabowicz, P. A. et al. 2012. Social Features of Online Networks: The Strength of Intermediary Ties in Online Social Media. *PLoS ONE*, Vol. 7, No. 1. http://dx.doi.org/10.1371/journal.pone.0029358

Hannak, A. et al. Measuring Personalization of Web Search. *WWW '13 Proceedings of the 22nd international conference on World Wide Web*, pp. 527-538. http://www.ccs.neu.edu/home/cbw/pdf/fp039-hannak.pdf

Harvey, D., VP, Trust & Safety, Twitter. 2013, 29 July. *We hear you.* https://blog.twitter.com/en-gb/2013/we-hear-you

Herpai, G. 2013, 7 January. Unsocial network: the rise and fall of iWiW. *Budapest Business Journal*. www.bbj.hu/business/unsocial-network-the-rise-and-fall-of-iwiw_64418

Hoechsmann, M. and S. R. Poyntz. 2012. *Media Literacies. A Critical Introduction.* Oxford: Wiley-Blackwell

Hope, D. A. 2011, February. *Protecting Human Rights in the Digital Age.* BSR. https://globalnetworkinitiative.org/sites/default/files/files/BSR_ICT_Human_Rights_Report.pdf

Howard, P. N. 2010. *The Digital Origins of Dictatorship and Democracy: Information Technology and Political Islam*. Oxford: Oxford University Press

Human Rights Watch. 2014. *Liberty to Monitor All*. https://www.hrw.org/report/2014/07/28/liberty-monitor-all/how-large-scale-us-surveillance-harming-journalism-law-and

iHub Research. 2013. *Umati Final Report*. http://www.research.ihub.co.ke/uploads/2013/june/1372415606__936.pdf

Imre, A. 2009, May. National intimacy and post-socialist networking. *European Journal of Cultural Studies*, Vol. 12, No. 2, pp. 219-33

The Institute for Human Rights and Business and Shift. 2013, June. *ICT Sector Guide on Implementing the UN Guiding Principles on Business and Human Rights*. European Commission. www.shiftproject.org/publication/european-commission-ict-sector-guide

Intel Corporation and Dalberg Global Development Advisors. 2012. *Women and the Web: Bridging the Internet Gap and Creating New Global Opportunities in Low and Middle-Income Countries*. www.intel.com/content/dam/www/public/us/en/documents/pdf/women-and-the-web.pdf

Internet Watch Foundation. 2013. *Internet Watch Foundation Annual & Charity Report 2013*. Cambridge: IWF, www.iwf.org.uk/assets/media/annual-reports/annual_report_2013.pdf.pdf

Jellema, A. and K. Alexander. 2013, 22 November. *2013 Web Index Report*. Geneva: World Wide Web Foundation. http://thewebindex.org/wp-content/uploads/2013/11/Web-Index-Annual-Report-2013-FINAL.pdf

Johnson, E. J., S. Bellman and G. L. Lohse. 2002. Defaults, Framing, and Privacy: Why Opting In-Opting Out. *Marketing Letters*, Vol. 13, No. 1. https://www0.gsb.columbia.edu/mygsb/faculty/research/pubfiles/1173/defaults_framing_and_privacy.pdf

Kamdar, A. 2012, 6 December. EFF's Guide to CDA 230: The Most Important Law Protecting Online Speech. *EFF Deeplinks* Blog. https://www.eff.org/deeplinks/2012/12/effs-guide-cda-230-most-important-law-protecting-online-speech

Kohl, U. 2002. Eggs, Jurisdiction, and the Internet. *International and comparative law quarterly*, vol. 51, no. 3, pp. 556-582

KVG Research. 2013, December. *TV Market and Video on Demand in the Russian Federation*. Strasbourg: European Audiovisual Observatory. www.obs.coe.int/documents/205595/552774/RU+TV+and+VoD+2013+KVG+Research+EN.pdf/5fbb076c-868e-423a-bfed-dca8b66cac43

Laclau, E. and Mouffe, C. 1985. *Hegemony and Socialist Strategy. Towards a Radical Democratic Politics.* London: Verso

Learner, J. and R. Bar-Nissim. 2014. Law Enforcement Investigations Involving Journalists. *Legal Studies Research Paper Series*, no. 2014-71. School of Law, University of California, Irving

Leo, L. A., F. D. Gaer and E. K. Cassidy. 2011. Protecting Religions from Defamation: A Threat to Universal Human Rights Standards. *Harv. JL & Pub. Pol'y*, vol. 34, pp. 769-95

Limpitlaw, J. 2013. *Media Law Handbook for Southern Africa*, vol. 2. Johannesburg: Konrad-Adenauer-Stiftung Regional Media Programme. http://www.kas.de/wf/doc/kas_35248-1522-2-30.pdf?130825185204

Marquis-Boire, M. et al. 2013, March. 'You only click twice: FinFisher's Global Proliferation'. Citizen Lab. https://citizenlab.org/2013/03/you-only-click-twice-finfishers-global-proliferation-2/

Meddaugh, P. M. and Kay, J. 2009. Hate Speech or 'Reasonable Racism?' The Other in Stormfront, *Journal of Mass Media Ethics, Vol. 24*, no. 4, pp. 251-68. MediaSmarts.NDa

Lengyel, B. et al. 2013, 26 January. Distance dead or alive Online Social Networks from a geography perspective. SSRN. http://dx.doi.org/10.2139/ssrn.2207352

Levine, M., VP of Global Public Policy, Facebook. 2013, 28 May. 'Controversial, Harmful and Hateful Speech on Facebook'. https://www.facebook.com/notes/facebook-safety/controversial-harmful-and-hateful-speech-on-facebook/574430655911054

MacKinnon, R. 2012. *Consent of the Networked: The Worldwide Struggle for Internet Freedom.* New York: Basic Books.

Maireder, A. and S. Schlögl. 2014, December. 24 Hours of an #outcry: The Networked Publics of a Socio-Political Debate. *European Journal of Communication*, Vol. 29, No. 6

Marsden, C. T. 2011. *Internet Co-Regulation: European Law, Regulatory Governance, and Legitimacy in Cyberspace*. Cambridge: Cambridge University Press

Marthews, A. and C. Tucker. 2014, 24 March. Government Surveillance and Search Behavior. SSRN. http://ssrn.com/abstract=2412564

McNamee, J. 2011, January. *The Slide from Self-Regulation to Corporate Censorship*. Brussels: European Digital Rights Initiative. www.edri.org/files/EDRI_selfreg_final_20110124.pdf

Moore, M. 2007, June. Public interest, media neglect. *British Journalism Review*, vol. 18, no.2

Morsink, J. 1999. *The universal declaration of human rights: Origins, drafting, and intent*. University of Pennsylvania Press

Mossberger, K., C. J. Tolbert and R. S. McNeal. 2008. *Digital Citizenship. The Internet, Society and Participation*. London: The MIT Press

Nash, V. 2013. Analyzing Freedom of Expression Online: Theoretical, empirical, and normative contributions. In Dutton, W.H. (Ed.). *The Oxford Handbook of Internet Studies*. Oxford: Oxford University Press

Natour, F. and J. D. Pluess. 2013, March. *Conducting an Effective Human Rights Impact Assessment*. BSR. http://www.bsr.org/reports/BSR_Human_Rights_Impact_Assessments.pdf

Noorlander, P. 2014, 5 December. 'Finding Justice for Whistleblowers'. *Journalism in Europe discussion series*, Centre for Media Pluralism and Media Freedom, European University Institute

Nowak, M. 1993. *UN covenant on civil and political rights: CCPR commentary*. NP Engel Kehl

Nyst, C. 2014, July. *End violence: Women's rights and safety online project – Internet intermediaries and violence against women online. Executive summary and findings*. Association for Progressive Communications. http://www.genderit.org/sites/default/upload/flow-cnyst-summary-formatted.pdf

Omanovic, E. 2014, 20 November. *Private Interests: Monitoring Central Asia*. Privacy International. https://www.privacyinternational.org/?q=node/59

Osler, A. and H. Starkey. 2005. *Changing Citizenship*. Berkshire: Open University Press

Palfrey, J. G. Jr. Local Nets on a Global Network: Filtering and the Internet Governance Problem. *The Global Flow of Information.* In Balkin, J. (Ed.). Harvard Public Law Working Paper No. 10-41, p.8. http://ssrn.com/abstract=1655006

Parti, K. and L. Marin. 2013. Ensuring Freedoms and Protecting Rights in the Governance of the Internet: A Comparative Analysis on Blocking Measures and Internet Providers' Removal of Illegal Internet Content. *Journal of Contemporary European Research*, vol. 9, no. 1, pp. 138-59. www.jcer.net/index.php/jcer/article/view/455/392

Pasquale, F. A. 2010. Beyond Innovation and Competition: The Need for Qualified Transparency in Internet Intermediaries. *Northwestern University Law Review*, vol. 104, no. 1, pp. 105-74. www.law.northwestern.edu/lawreview/v104/n1/105/LR104n1Pasquale.pdf

Petrova, D. 2011, 9-10 February. 'Incitement to National, Racial or Religious Hatred: Role of Civil Society and National Human Rights Institutions'. 2011 Expert Workshops on the Prohibition of Incitement to National, Racial or Religious Hatred, Vienna

Pew Research Center in association with Columbia University's Tow Center for Digital Journalism. 2015, 5 February. *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior*. http://www.journalism.org/files/2015/02/PJ_InvestigativeJournalists_0205152.pdf

Phillips, G. 2014, 10 October. *On protection of journalistic sources*. Centre for Media Pluralism and Media Freedom, European University Institute. http://journalism.cmpf.eui.eu/discussions/on-protection-of-journalistic-sources/

Podkowik, J. 2014. 'Secret surveillance, national security and journalistic privilege – in search of the balance between conflicting values in the age of new telecommunication technologies'. University of Oslo. http://www.jus.uio.no/english/research/news-and-events/events/conferences/2014/wccl-cmdc/wccl/papers/ws8/w8-podkowik.pdf

Post, R., I. Hare and J. Weinstein. 2009. Hate speech. In *Extreme speech and democracy*. Oxford: Oxford University Press, pp. 123-38

Ramzy, A. 17 February 2011. Wired Up. *Time*. http://content.time.com/time/printout/0,8816,2048171,00.html

Rosenberg, R. S. 2011. Controlling access to the Internet: The role of filtering. *Ethics and Information Technology*, vol. 3, no. 1, pp. 35-54. www.copacommission.org/papers/rosenberg.pdf

Rotenberg, M. and D. Jacobs. 2013. Updating the Law of Information Privacy: The New Framework of the European Union. *Harvard Journal of Law & Public Policy*, vol. 36, no. 2, pp. 605-52. www.harvard-jlpp.com/wp-content/uploads/2013/04/36_2_605_ Rotenberg_Jacobs.pdf

Rowbottom, J., 2012. To Rant, Vent and Converse: Protecting Low Level Digital Speech. *The Cambridge Law Journal*, vol. 71, no. 2, pp. 355-383

Russell, L. 2014. Shielding the Media: In an Age of Bloggers, Tweeters, and Leakers, Will Congress Succeed in Defining the Term 'Journalist' and in Passing a Long-Sought Federal Shield Act? *Oregon Law Review*, 93, pp. 193-227

Rustad, M. L. and D. D'Angelo. 2012. The Path of Internet Law: An Annotated Guide to Legal Landmarks. *Duke Law & Technology Review*, vol. 2011, no. 012. Suffolk University Law School Research Paper No. 11-18. http://ssrn.com/abstract=1799578

Ryngaert, C. 2008. *Jurisdiction in international law*. Oxford: Oxford University Press

Samway, M. A. 2014, October. Business, Human Rights and the Internet: A Framework for Implementation. In Lagon, M. P. and A. C. Arend (Eds.). *Human Dignity and the Future of Global Institutions*. Georgetown University Press

Savin, A. and J. Trzaskowski (eds). 2014. *Research Handbook on EU Internet Law*. Edward Elgar Publishing

Seng, D. and I. Garrote Fernandez-Diez. 2012. *Comparative Analysis of National Approaches of the Liability of the Internet Intermediaries*. Geneva: World Intellectual Property Organization. www.wipo.int/export/sites/www/copyright/en/doc/liability_of_Internet_intermediaries.pdf

Sieminski, P. 2013, 21 November. Striking Back Against Censorship. WordPress *Hot Off the Press* Blog. http://en.blog.wordpress.com/2013/11/21/striking-back-against-censorship

Sparas, D. 2013, 18 June. EU regulatory framework for e-commerce. *World Trade Organization Workshop on E-Commerce*. Geneva: World Trade Organization. www.wto.org/english/tratop_e/serv_e/wkshop_june13_e/sparas_e.pdf

Stearns, J. 2013. *Acts of journalism: Defining Press Freedom in the Digital Age*. Washington, DC: Free Press. http://www.freepress.net/resource/105079/acts-journalism-defining-press-freedom-digital-age

Sunstein, C. 2013, December. Deciding by Default. *University of Pennsylvania Law Review*, Vol. 162, No. 1. http://scholarship.law.upenn.edu/cgi/viewcontent.cgi?article=1000&context=penn_law_review

Tuppen, C. 2012. *Opening the Lines: A Call for Transparency from Governments and Telecommunications Companies*. Global Network Initiative. https://globalnetworkinitiative.org/sites/default/files/GNI_OpeningtheLines.pdf

Van Hoboken, J. 2012. *Search Engine Freedom: On the implications of the right to freedom of expression for the legal governance of Web search engines*. PhD thesis, University of Amsterdam Faculty of Law. http://dare.uva.nl/document/357527

Viljoen, F., 2012. *International human rights law in Africa*. Oxford: Oxford University Press

Villeneuve, N. 2006, January. The Filtering Matrix: Integrated mechanisms of information control and the demarcation of borders in cyberspace. *First Monday*, vol. 11. No. 1-2

Waldron, J., 2012. *The Harm in Hate Speech.* Cambridge, MA: Harvard University Press

York, J. C. 2010, September. 'Policing Content in the Quasi-Public Sphere'. OpenNet Initiative. https://opennet.net/policing-content-quasi-public-sphere

Zingales, N. 2013, November. *Internet intermediary liability: Identifying best practices for Africa*. South Africa: Association for Progressive Communications. www.apc.org/en/system/files/APCInternetIntermediaryLiability_BestPracticesAfrica_20131125.pdf

Zittrain, J. 2006, spring. A History of Online Gatekeeping. *Harvard Journal of Law & Technology*, Vol. 19, No. 2, pp. 253-98. http://jolt.law.harvard.edu/articles/pdf/v19/19HarvJLTech253.pdf

En el informe titulado *Tendencias mundiales en libertad de expresión y desarrollo de los medios: consideración prioritaria del ámbito digital 2015* se estudian los nuevos desafíos y las nuevas oportunidades que surgen en materia de libertad de prensa en la era digital. En él se subraya la importancia que revisten los nuevos agentes en la promoción y protección de la libertad de expresión, en línea y fuera de línea, prestando particular atención a las cuestiones relacionadas con el discurso del odio, la protección de las fuentes periodísticas, la función de los intermediarios de Internet en el fomento de la libertad de expresión y la seguridad de los periodistas. Esta publicación especial de la colección *Tendencias mundiales* constituye una referencia esencial para los gobiernos, los periodistas, los profesionales de los medios de comunicación, la sociedad civil, el sector privado y los círculos universitarios, en un contexto mediático que se ha visto transformado por las tecnologías digitales.

UNESCO
Organización de las Naciones Unidas para la Educación, la Ciencia y la Cultura

Sector de la Comunicación e Información

9 789233 000537