

Guía de los Derechos Humanos para los Usuarios de Internet

Elaborada por el Consejo de Europa, Recomendación CM/Rec(2014)6

Antecedentes

1. Los Estados miembros del Consejo de Europa tienen la obligación de garantizar a todas las personas de su jurisdicción los derechos humanos y las libertades fundamentales consagrados en el Convenio Europeo de Derechos Humanos (STE n.º 5, el Convenio). Esta obligación es aplicable en el contexto del uso de Internet. También son aplicables otros convenios e instrumentos del Consejo de Europa que tratan de la protección del derecho a la libertad de expresión, el acceso a la información, el derecho a la libertad de reunión, la protección frente a la ciberdelincuencia, el derecho al respeto a la vida privada y la protección de los datos personales.
2. Las obligaciones de los Estados en cuanto a respetar, proteger y promover los derechos humanos incluyen la supervisión de las empresas privadas. Los derechos humanos, que son universales e indivisibles, así como las normas relacionadas, prevalecen sobre las condiciones generales impuestas a los usuarios de Internet por cualquier actor del sector privado.
3. Internet tiene características de servicio público. Personas, comunidades, autoridades públicas y entidades privadas dependen cada vez más de Internet para sus actividades y tienen una expectativa legítima de que sus servicios sean accesibles, ofrecidos sin discriminación, asequibles, seguros, fiables y continuos. Además, nadie debería estar sujeto a injerencias ilícitas, innecesarias o desproporcionadas en el ejercicio de sus derechos humanos y sus libertades fundamentales al usar Internet.
4. Los usuarios deberían recibir apoyo para comprender y ejercer de manera efectiva sus derechos humanos en Internet en el caso de que sus derechos y libertades hayan sido objeto de restricción o injerencia. Tal apoyo debería incluir orientación sobre el acceso a recursos efectivos. A la luz de las oportunidades que brinda Internet en términos de transparencia y responsabilidad en la gestión de los asuntos públicos, los usuarios deberían poder usar Internet para participar en la vida democrática.
5. A fin de garantizar que los derechos humanos y las libertades fundamentales reconocidos se apliquen por igual dentro y fuera de la red, el Consejo de Ministros recomienda, en virtud de los términos del Artículo 15.b del Estatuto del Consejo de Europa, que los Estados miembros:
 - 5.1. Promuevan activamente la Guía de los derechos humanos para los usuarios de Internet (como se presenta en el Anexo) entre los ciudadanos, las autoridades públicas y los actores del sector privado, y emprendan acciones específicas para su aplicación a fin de permitir a los usuarios ejercer plenamente sus derechos humanos y libertades fundamentales en línea;
 - 5.2. Evalúen, revisen periódicamente y, en su caso, eliminen las restricciones relativas al ejercicio de los derechos y libertades en Internet, en especial cuando no sean conformes al Convenio a la luz de la jurisprudencia relevante del Tribunal Europeo de Derechos Humanos. Toda restricción deberá estar prevista por la ley, ser necesaria en el marco de una sociedad democrática para alcanzar un objetivo legítimo y ser proporcional a ese objetivo;
 - 5.3. Garanticen que los usuarios de Internet tengan acceso a recursos efectivos cuando se hayan restringido sus derechos y libertades o cuando consideren que se han violado sus derechos. Esto exige mejorar la coordinación y la cooperación entre las instituciones, entidades y comunidades relevantes. Asimismo, requiere la participación de actores del sector privado y organizaciones de la sociedad civil y la cooperación efectiva con ambos. Dependiendo del contexto nacional, esto puede incluir mecanismos de reparación tales como los previstos por las autoridades de protección de datos, instituciones nacionales de derechos humanos (p. ej.: mediadores), procedimientos judiciales o líneas de asistencia telefónica;

5.4. Promuevan la coordinación con otros actores estatales y no estatales, dentro y más allá del Consejo de Europa, en relación con las normas y los procedimientos que tienen un impacto sobre la protección de los derechos humanos y las libertades fundamentales en Internet;

5.5. Impulsen al sector privado a participar en un diálogo abierto con las autoridades estatales relevantes y la sociedad civil en el ejercicio de su responsabilidad social corporativa, en especial en cuanto a transparencia y rendición de cuentas, de acuerdo con los Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para “proteger, respetar y remediar”. También se debería fomentar la contribución del sector privado a la divulgación de la guía;

5.6. Alienten a la sociedad civil a respaldar la divulgación y aplicación de la guía de modo que constituya una herramienta efectiva para los usuarios de Internet.

6. La Recomendación CM/Rec(2014)6 del Consejo de Ministros a los Estados miembros sobre una Guía de los derechos humanos para los usuarios de Internet fue adoptada por el Consejo de Ministros el 16 de abril de 2014, en la 1197ª reunión de Delegados de los Ministros de 47 países y cuenta con el apoyo, entre otros, de la Asociaciones de Usuarios de Internet (www.aui.es), Asociación de Internautas (www.internautas.org) y el capítulo Español de la Internet Society (www.isoc-es.org)

Introducción

1. La presente guía es una herramienta para que usted, como usuario de Internet, conozca sus derechos humanos en la red, las posibles limitaciones de estos derechos y los recursos disponibles en caso de que detecten esta limitación. Los derechos humanos y las libertades fundamentales se aplican por igual dentro y fuera de Internet. Este principio abarca el respeto por los derechos y las libertades de los demás usuarios de Internet. La guía brinda información sobre lo que significan en la práctica los derechos y las libertades en el contexto de Internet, la manera en que pueden afirmarse y ejercerse, y las vías de recurso. Este es un documento que irá evolucionando y que estará abierto a actualizaciones periódicas.

2. Esta guía se basa en el Convenio Europeo de Derechos Humanos y en otros convenios e instrumentos del Consejo de Europa que abordan distintos elementos de protección de los derechos humanos. Todos los Estados miembros del Consejo de Europa tienen el deber de respetar, proteger y cumplir con los derechos y libertades contemplados en los instrumentos que han ratificado. La constante interpretación de estos derechos y libertades por el Tribunal Europeo de Derechos Humanos, así como otros instrumentos jurídicos pertinentes del Consejo de Europa, inspiran también esta guía.

3. La guía no establece nuevos derechos humanos ni nuevas libertades fundamentales. Por el contrario, se apoya en normas ya reconocidas y en mecanismos de cumplimiento ya existentes.¹

Acceso y no discriminación

1. El acceso a Internet es un medio importante para que usted ejerza sus derechos y libertades y participe en la democracia. Por lo tanto, usted no debería quedar desconectado de Internet contra su voluntad, salvo por decisión judicial. En ciertos casos, el servicio podría descontinuarse debido a acuerdos contractuales, pero esta debería ser una medida de último recurso.

2. Su acceso debería ser asequible y no discriminatorio. Usted debería tener el mayor acceso posible al contenido, las aplicaciones y los servicios de Internet desde los dispositivos de su elección.

3. Si vive en una zona rural o alejada geográficamente, dispone de bajos ingresos, tiene alguna discapacidad o tiene necesidades especiales, debería tener la expectativa de que las autoridades públicas hagan esfuerzos razonables y tomen medidas específicas para facilitar su acceso a Internet.

4. En sus relaciones con las autoridades públicas, con los proveedores de servicios de Internet y proveedores de contenido y servicios en línea, o con otros usuarios o grupos de usuarios, usted no debe ser víctima de discriminación por razones de género, raza, color, idioma, religión o creencias, opiniones políticas o de otra índole, origen nacional o social, relación con una minoría nacional, propiedad, nacimiento, etnia, edad, orientación sexual u otros factores.

Libertad de expresión e información

Usted tiene derecho a buscar, recibir y comunicar información e ideas de su elección, sin injerencia y sin consideración de fronteras. Esto significa que:

1. usted tiene la libertad de expresarse en línea y de acceder a la información y las opiniones y expresiones de otros. Esto incluye discursos políticos, puntos de vista sobre religión y opiniones u expresiones que tengan una acogida favorable o se consideren inofensivas, así como también aquellas que puedan ofender, chocar o perturbar a otros. Usted debe tomar debidamente en consideración la reputación y los derechos de los demás, inclusive el derecho al respeto a la vida privada;

¹ Esta guía forma parte de una recomendación adoptada por el Comité de Ministros de los 47 Estados miembros del Consejo de Europa. En el anexo de Exposición de motivos que acompaña a la recomendación pueden encontrarse explicaciones más detalladas sobre la guía.

2. pueden aplicarse restricciones a las expresiones que incitan a la discriminación, el odio o la violencia. Estas restricciones deben ser lícitas, estar definidas de manera estricta y ejecutarse bajo supervisión judicial;
3. usted es libre de crear, reutilizar y distribuir contenidos que respeten el derecho a la protección de la propiedad intelectual, incluidos los derechos de autor;
4. las autoridades públicas tienen el deber de respetar y proteger su libertad de expresión y su libertad de información. Toda restricción a esta libertad debe tener un carácter no arbitrario, debe obedecer a un objetivo legítimo de acuerdo con el Convenio Europeo de Derechos Humanos (por ejemplo, la protección de la seguridad nacional, el orden público, la salud pública o la moral) y debe ser conforme a las leyes sobre derechos humanos. Además, toda restricción se le deberá dar a conocer, junto con información sobre la manera de buscar orientación y obtener reparación. El alcance o la duración de la restricción no deberán ser mayores de lo estrictamente necesario para lograr un objetivo legítimo;
5. su proveedor de servicios de Internet y su proveedor de contenido y servicios en línea tienen responsabilidades corporativas que cumplir en lo que se refiere a respetar sus derechos humanos y a brindarle mecanismos para responder a sus reclamaciones. No obstante, usted debe tener en cuenta que los proveedores de servicios en línea, como las redes sociales, pueden restringir ciertos tipos de contenido y comportamientos debido a sus políticas de contenido. Usted debería ser informado sobre las posibles restricciones de modo que pueda decidir, con conocimiento de causa, si utiliza o no el servicio. Esto incluye información específica sobre los contenidos y comportamientos que el proveedor de servicios en línea considera ilegales o inadecuados cuando se usa el servicio, y sobre la manera en que trata esos casos;
6. usted puede optar por no revelar su identidad en línea, por ejemplo mediante el uso de un seudónimo. Sin embargo, debe tener en cuenta que las autoridades nacionales pueden tomar medidas que conduzcan a revelar su identidad.

Reunión, asociación y participación

Usted tiene derecho a reunirse y asociarse pacíficamente con otras personas usando Internet. En la práctica, esto significa que:

1. usted tiene la libertad de elegir cualquier sitio web, aplicación u otro servicio para formar o movilizar grupos sociales o asociaciones, o para su ingreso o participación en estos, independientemente de que estén o no reconocidos de manera formal por las autoridades públicas. Usted también debería poder utilizar Internet para ejercer su derecho a constituir sindicatos y formar parte de los mismos;
2. usted tiene derecho a protestar pacíficamente en línea. Sin embargo, debe tener en cuenta que se expone a consecuencias jurídicas si su protesta en la red causa bloqueos, interrupción de servicios o daños a los bienes de terceros;
3. usted es libre de utilizar las herramientas disponibles en línea para participar en los debates de política pública, las iniciativas legislativas y el control público de los procesos de toma de decisiones a nivel local, nacional y mundial. Asimismo, tiene derecho a firmar peticiones y a participar en la elaboración de políticas para la regulación de Internet.

Protección de la vida privada y de los datos personales

Usted tiene derecho al respeto de su vida privada y familiar en Internet, lo cual abarca la protección de sus datos personales y el respeto de la confidencialidad de su correspondencia y sus comunicaciones. Esto significa que:

1. usted debería tener en cuenta que, al utilizar Internet, sus datos personales son objeto de un tratamiento constante. Esto ocurre cuando utiliza servicios tales como navegadores, correo electrónico, mensajes instantáneos, protocolos de transmisión de voz por Internet, redes sociales, motores de búsqueda y servicios de almacenamiento de datos en la nube;
2. las autoridades públicas y las empresas privadas tienen la obligación de respetar normas y procedimientos específicos cuando tratan sus datos personales;
3. sus datos personales solo deberían ser objeto de tratamiento cuando la ley lo prevea o cuando usted haya dado su consentimiento. A usted se le debería informar qué datos personales son objeto de tratamiento o transferencia a terceros, cuándo lo son, por quién y con qué propósito. De manera general, usted debería poder ejercer un control sobre sus datos de carácter personal (verificar que sean exactos, solicitar que se corrijan o se eliminen, o pedir que no se conserven por más tiempo de lo necesario);
4. usted no debe ser sometido a medidas generales de vigilancia o interceptación. Solo en circunstancias excepcionales definidas por la ley se podrá quebrantar su privacidad con respecto a los datos personales; por ejemplo, en el marco de la investigación de un delito. Debería ponerse a su disposición información accesible, clara y precisa sobre las leyes o políticas relevantes y sobre sus derechos a este respecto;
5. su vida privada también se debe respetar en el lugar de trabajo. Esto incluye la confidencialidad de su correspondencia y sus comunicaciones privadas en línea. Su empleador debe informarle sobre la aplicación de cualquier medida de vigilancia o control;
6. usted puede recibir asistencia de parte de las autoridades de protección de datos (existentes en la mayoría de países europeos) para garantizar el cumplimiento de los principios y las leyes de protección de datos.

Educación y conocimientos básicos

Usted tiene derecho a la educación, lo cual abarca el acceso al conocimiento. Esto significa que:

1. usted debería tener acceso en línea a la educación, así como a contenidos culturales, científicos, académicos y de otra índole en lenguas oficiales. En relación con tal acceso, podrían aplicarse condiciones a fin de remunerar a los titulares de derechos por el trabajo que realizan. Usted también debería poder acceder libremente en Internet a las investigaciones y obras culturales de dominio público que sean financiadas con fondos públicos, cuando estén disponibles;
2. como parte del conocimiento básico de Internet y de los medios de comunicación, y con el objetivo de ejercer sus derechos y libertades en Internet, usted debería tener acceso a la educación y el saber digital, que abarca las competencias para comprender una amplia gama de herramientas de Internet, así como para usarlas y trabajar con ellas. Esto debería permitirle evaluar con una mirada crítica la exactitud y la fiabilidad de los contenidos, aplicaciones y servicios a los que tiene acceso o a los que le gustaría acceder.

Niños y jóvenes

Como niño(a) o joven, tienes todos los derechos y las libertades que se describen en esta guía. En particular, debido a tu edad, tienes derecho a recibir protección y orientación especial al utilizar Internet. Esto significa que:

1. tienes derecho a expresar libremente tus puntos de vista y a participar en la sociedad, a que se te escuche y a contribuir en la toma de decisiones sobre los asuntos que te afecten. Se debe dar a tus opiniones la consideración adecuada en función de tu edad y madurez, sin discriminación;
2. puedes tener la expectativa de recibir información en un lenguaje apropiado para tu edad y de que tus profesores, educadores, padres o tutores te orienten sobre el uso seguro de Internet, incluida la manera de proteger tu vida privada;
3. debes tener en cuenta que tanto el contenido creado por ti en Internet como el contenido creado por otros usuarios en relación contigo pueden ser accesibles en todo el mundo y podrían poner en peligro tu dignidad, tu seguridad y tu vida privada, o ser de otro modo perjudiciales para ti o para tus derechos, ahora o en una etapa posterior de tu vida. Si lo solicitas, tal contenido debe ser retirado o eliminado dentro de un plazo razonable;
4. puedes tener la expectativa de contar con información clara sobre los comportamientos y contenidos que son ilegales en Internet (por ejemplo, el acoso en línea), así como con la posibilidad de denunciar contenidos presuntamente ilegales. La información debería estar adaptada a tu edad y a tus circunstancias. Además, se te debería brindar apoyo y asesoramiento, con el debido respeto por tu confidencialidad y anonimato;
5. deberías gozar de protección especial contra toda traba a tu bienestar físico, mental y moral, en particular el abuso y la explotación sexual en Internet y otras formas de ciberdelincuencia. En especial, tienes derecho a la educación para protegerte de tales amenazas.

Recursos efectivos

1. Usted tiene derecho a un recurso efectivo cuando sus derechos humanos y libertades fundamentales sean objeto de restricción o violación. Para disponer de un recurso, no debería ser necesario que inicie directamente una acción legal. Las vías de recurso deberían estar disponibles, ser conocidas, accesibles y asequibles, y ser aptas para brindar una reparación adecuada. Deben poder obtenerse recursos efectivos directamente de los proveedores de servicios de Internet, las autoridades públicas o las instituciones nacionales de derechos humanos. Dependiendo de la violación de que se trate, los recursos efectivos pueden dar lugar a: la investigación, la explicación, la respuesta, la corrección, la petición de disculpas, el restablecimiento, la reconexión y la compensación. En la práctica, esto significa que:

- 1.1. su proveedor de servicios de Internet, los proveedores de acceso a contenidos y servicios en línea, u otras compañías o autoridades públicas deberían informarle sobre sus derechos y libertades, así como sobre los recursos posibles y el modo de obtenerlos. Esto incluye información fácilmente accesible sobre la manera de denunciar injerencias en sus derechos, de presentar quejas al respecto y de buscar reparación;
- 1.2. las autoridades públicas, instituciones nacionales de derechos humanos (tales como mediadores), autoridades de protección de datos, oficinas de asesoramiento a los ciudadanos, asociaciones de derechos humanos o derechos digitales, u organizaciones de consumidores deberían poner a disposición información y orientación adicional;

1.3. las autoridades nacionales tienen la obligación de protegerle de actividades ilícitas o delitos cometidos en Internet o mediante el uso de Internet, en particular cuando están relacionados con el acceso ilícito, la interferencia, la falsificación u otros manejos fraudulentos de su identidad digital, su ordenador o los datos allí contenidos. Las autoridades de orden público competentes tienen la obligación de investigar y tomar medidas adecuadas, lo cual incluye sanciones, si usted presenta una queja por perjuicio o injerencia en relación con su identidad personal y su propiedad en línea.

2. En lo que respecta a la determinación de sus derechos y obligaciones o de cualquier acusación penal contra usted en relación con Internet:

2.1. usted tiene derecho a un proceso equitativo, dentro de un plazo razonable, por un tribunal independiente e imparcial;

2.2. usted tiene derecho a interponer un recurso individual ante el Tribunal Europeo de Derechos Humanos después de haber agotado todos los recursos nacionales disponibles.

Anexo: Exposición de motivos a la recomendación CM(2014)31

Introducción

1. Internet desempeña un papel importante en la vida diaria de las personas y en todos los aspectos de la sociedad humana. Continuamente evoluciona y brinda a los ciudadanos posibilidades de acceder a información y servicios, de conectarse y comunicarse, y de compartir ideas y conocimientos en todo el mundo. El impacto de Internet sobre las actividades sociales, económicas y culturales va creciendo igualmente.

2. El Tribunal Europeo de Derechos Humanos (“el Tribunal”) atiende un número cada vez mayor de casos relacionados con Internet.¹ Es así como ha llegado a afirmar que “Internet es en la actualidad el principal medio de la gente para ejercer su derecho a la libertad de expresión y de información: se encuentran herramientas esenciales de participación en actividades y debates relativos a cuestiones políticas o de interés público”.²

3. La Estrategia de gobernanza de Internet 2012-2015 del Consejo de Europa otorga importancia a los derechos de los usuarios de Internet. El capítulo relativo a Reforzar los derechos y las libertades de los usuarios de Internet, que apunta a promover el acceso a Internet y el mejor uso de esta herramienta, incluye como línea de acción: “elaborar un compendio de los derechos humanos reconocidos para los usuarios de Internet a fin de ayudarles en la comunicación y en la búsqueda de recursos efectivos con actores clave de Internet y agencias gubernamentales cuando consideren que sus derechos y libertades se han visto afectados negativamente: denunciar un incidente, formular una queja o ejercer un derecho de respuesta, reparación u otro tipo de recurso”.

Antecedentes y contexto

4. El Comité Director sobre Medios de Comunicación y Sociedad de la Información (CDMSI), en su primera reunión del 27 al 30 de abril de 2012, propuso al Consejo de Ministros la creación de un Comité de Expertos sobre Derechos de los Usuarios de Internet (MSI-DUI) y acordó su proyecto de mandato. En respuesta a la propuesta del CDMSI, el Consejo de Ministros aprobó el mandato en la 1147.^a reunión de Delegados de los Ministros, el 6 de julio de 2012.³ El resultado esperado del MSI-DUI, de acuerdo con su mandato, es el siguiente:

“Se elabora un compendio de los derechos humanos para los usuarios de Internet a fin de ayudarles a comprender y ejercer sus derechos cuando —considerando que sus derechos y libertades se hayan visto afectados negativamente— se comuniquen con los principales actores de Internet o con agencias gubernamentales y busquen ante ellos un recurso efectivo (2013)” (en lo sucesivo, el Compendio).

5. El MSI-DUI celebró su primera reunión los días 13 y 14 de septiembre de 2012, en Estrasburgo. Se acordó que el trabajo del MSI-DUI no debería apuntar a crear nuevos derechos humanos sino a examinar la aplicación, en el contexto de Internet, de los derechos ya existentes. El MSI-DUI decidió reunir información, por medio de un cuestionario enviado a sus redes y comunidades, sobre problemas prácticos afrontados por los usuarios y, de este modo, sobre posibles violaciones de sus derechos humanos y recursos disponibles en la materia.

6. Con ocasión del Foro de Gobernanza de Internet, del 6 al 9 de noviembre de 2012, en Bakú, se realizaron consultas con las partes interesadas, en el taller sobre empoderamiento de los usuarios de Internet (*Empowerment of Internet Users – which tools?*). Los miembros participantes del MSI-DUI aprovecharon las posibilidades de acercamiento que brindaba este evento para obtener aportaciones de las partes interesadas sobre varios temas relevantes para el Compendio. Las discusiones del taller

¹ Para una visión general de la jurisprudencia del Tribunal Europeo de Derechos Humanos en relación con Internet, véase la ficha informativa sobre nuevas tecnologías, de octubre de 2013.

² Véase *Yildirim c. Turquía*, n.º 3111/10 § 54.

³ Véase CM(2012)91.

pusieron de relieve problemas a los que se enfrentan los usuarios de Internet, como la eliminación de sus contenidos sin el debido proceso, cuestiones relativas a la protección de datos personales y la falta de recursos efectivos.

7. El MSI-DUI celebró su segunda reunión los días 13 y 14 de diciembre de 2012, en Estrasburgo. Estudió entonces las respuestas recibidas al cuestionario y examinó la información recogida a través del acercamiento a las partes interesadas. El MSI-DUI decidió completar la fase analítica preliminar de su trabajo y, sobre esta base, empezar a redactar el Compendio. Durante la reunión en cuestión se presentó un primer borrador.

8. En su tercera reunión, celebrada los días 20 y 21 de marzo de 2013, en Estrasburgo, el MSI-DUI examinó en detalle asuntos relacionados con el derecho a la libertad de expresión, el derecho al respeto a la vida privada, la libertad de reunión y de asociación, la seguridad en línea, el derecho a la educación, los derechos del niño, la no discriminación y el derecho a un recurso efectivo. Este examen estuvo basado en normas pertinentes —vinculantes y no vinculantes— del Consejo de Europa y en la jurisprudencia del Tribunal. El MSI-DUI también adelantó discusiones sobre el tipo de instrumento que podría adoptar el Consejo de Europa para respaldar el Compendio, como una declaración o una recomendación del Consejo de Ministros. El instrumento debería cumplir dos objetivos: brindar a los usuarios de Internet orientación simple y clara sobre sus derechos humanos en línea y asegurar la adopción, por parte de los Estados miembros, de un texto acorde con sus obligaciones en virtud del Convenio Europeo de Derechos Humanos (CEDH) y otras normas del Consejo de Europa.

9. En su tercera reunión, del 23 al 26 de abril de 2013, en Estrasburgo, el CDMSI consideró que el Compendio debería combinar un lenguaje formal y simplificado; no obstante, se debería prestar atención a evitar una simplificación excesiva de las normas de derechos humanos existentes y de la jurisprudencia del Tribunal. Además, los debates subrayaron que sería deseable poner al día el Compendio periódicamente a fin de reflejar las rápidas evoluciones de las políticas de Internet. El CDMSI decidió también presentar comentarios sobre el proyecto de Compendio, en su estado de avance en el momento de las consultas, anotando que se trataba de un documento “en proceso”, a fin de aportar asesoramiento y orientación general. Las respuestas recibidas respaldaron el enfoque adoptado por el MSI-DUI en cuanto a elaborar un documento de sensibilización de uso fácil para el usuario, con especial atención al derecho a la libertad de expresión, el derecho al respeto a la vida privada, el derecho a la educación, los derechos del niño y la protección frente a la ciberdelincuencia.

10. El proyecto de Compendio fue presentado a los actores interesados y discutido con ellos en el marco del Diálogo europeo sobre la gobernanza en Internet (EuroDIG, 20 al 21 de junio de 2013, en Lisboa), en particular durante el taller sobre normas, derechos y responsabilidades para el futuro en Internet (*Towards a Human Internet? Rules, Rights and Responsibilities for our Online Future*). Los miembros del MSI-DUI que asistieron al taller celebraron una reunión informal en Lisboa. Se concluyó que el proyecto de Compendio debería abreviarse con miras a ser más accesible para los usuarios de Internet. Después de estas discusiones y del trabajo del MSI-DUI entre sesiones, se llevó a cabo una reunión ad hoc con los miembros del MSI-DUI disponibles, el 10 de septiembre de 2013, en Estrasburgo. El MSI-DUI examinó un proyecto de recomendación del Consejo de Ministros sobre los derechos humanos para los usuarios de Internet, que incluía en su anexo un proyecto de Compendio de los derechos humanos y las libertades fundamentales para los usuarios de Internet. El enfoque adoptado para el proyecto de Compendio fue el de dirigirse directamente al usuario. Teniendo en cuenta esto, se decidió dar un nuevo nombre al Compendio: “Guía de los derechos humanos para los usuarios de Internet”.

11. En su última reunión, del 1 y 2 de octubre de 2013, en Estrasburgo, el MSI-DUI examinó y finalizó sus propuestas dirigidas al CDMSI para un proyecto de recomendación del Consejo de Ministros sobre una Guía de los derechos humanos para los usuarios de Internet (en lo sucesivo, la Guía). Asimismo, acordó celebrar consultas con múltiples actores interesados, incluido un Foro Abierto del Consejo de Europa sobre la Guía durante el Foro de Gobernanza de Internet (22 al 25 de octubre de 2013, Indonesia). Se pidió a un grupo de actores interesados, en representación del sector privado, la sociedad civil, la comunidad técnica y el medio académico, que presentaran comentarios y sugerencias sobre la Guía. Además, se solicitaron comentarios y aportaciones informales sobre el proyecto de recomendación a otros comités directores pertinentes del Consejo de Europa, entre ellos, el Comité Director para los Derechos Humanos (CDDH), el Comité Europeo de Cooperación Jurídica

(CDCJ) y el Comité Europeo para los Problemas Criminales (CDPC), así como a comités convencionales como el Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (T-DP), el Comité del Convenio sobre la ciberdelincuencia (T-CY), el Comité de expertos sobre terrorismo (CODEXTER) y el Comité de las Partes del Convenio para la protección de los niños contra la explotación y el abuso sexual (T-ES). El CDDH, el CDCJ y miembros de la oficina del T-PD aportaron comentarios que el CDMSI tomó en consideración e integró en el proyecto de Recomendación y el proyecto de Exposición de motivos.

12. Además, se recibieron cerca de 30 contribuciones de representantes del sector privado (empresas de telecomunicaciones, proveedores de servicio en línea), organizaciones clave de la sociedad civil, la comunidad técnica y el medio académico, de diferentes partes del mundo. De manera general, estas contribuciones mostraron una acogida favorable del trabajo del Consejo de Europa sobre el proyecto de Guía y aportaron numerosos comentarios y propuestas de cambios a dicho proyecto.

13. Durante su 4.^a reunión, celebrada del 3 al 6 de diciembre de 2013, el CDMSI examinó las propuestas del MSI-DUI para un proyecto de recomendación del Consejo de Ministros sobre una Guía de los derechos humanos para los usuarios de Internet. Tomó nota de las consultas arriba mencionadas con diversos actores, y finalizó el proyecto de recomendación sobre la base de los comentarios finales que fueron enviados por correo electrónico.

Comentarios relativos a la Recomendación CM/Rec(2014)6 del Consejo de Ministros a los Estados miembros sobre una Guía de los derechos humanos para los usuarios de Internet

14. El objetivo de esta recomendación es fomentar el ejercicio y la protección de los derechos humanos y las libertades fundamentales en Internet en todos los Estados miembros del Consejo de Europa. El acceso de las personas y comunidades a Internet, y el propósito de que utilicen de la mejor manera esta herramienta, exigen esfuerzos destinados a informarlas y habilitarlas para que ejerzan sus derechos y libertades en los entornos en línea. Así lo había afirmado el Consejo de Ministros en su Declaración sobre principios de gobernanza de Internet, de 2011, en la que puso de relieve su visión de un enfoque de Internet centrado en las personas y basado en los derechos humanos, que —como un principio de gobernanza de Internet— habilite a los usuarios para ejercer sus derechos y libertades en la red.

15. La Guía, anexa a esta recomendación, ofrece información básica sobre determinados derechos humanos consagrados en el CEDH y otras normas relevantes del Consejo de Europa. Se centra en derechos y libertades específicos y en normas relacionadas de derecho internacional, en particular con respecto al derecho a la libertad de expresión, la libertad de reunión y de asociación, el derecho al respeto a la vida privada y la protección de los datos personales, los derechos de los niños y el derecho a un recurso efectivo. Además, ha sido redactada en un lenguaje fácil de entender para los usuarios. Con el fin de lograr un texto lo más sencillo posible, el MSI-DUI decidió no hacer referencia a las formulaciones jurídicas estrictas relacionadas con las obligaciones de los Estados miembros en virtud del derecho internacional, incluida la jurisprudencia del Tribunal.

16. Diversos instrumentos del Consejo de Europa garantizan los derechos humanos y las libertades fundamentales y resultan aplicables tanto dentro como fuera de los entornos en línea. En particular, los derechos humanos y las libertades fundamentales están consagrados en el CEDH, según lo interpreta el Tribunal en su jurisprudencia. Varios convenios y otros instrumentos no vinculantes del Consejo de Europa brindan explicaciones y orientaciones complementarias para los usuarios de Internet. El MSI-DUI consideró que a fin de que los usuarios de Internet comprendiesen sus derechos y libertades, era necesario explicar con un lenguaje sencillo las normas de derecho internacional pertinentes del Consejo de Europa y las Naciones Unidas.

Preámbulo

17. El preámbulo enuncia las razones que llevaron al Consejo de Ministros a adoptar la recomendación a sus Estados miembros. La premisa para las recomendaciones es que la responsabilidad de velar por los derechos humanos y las libertades fundamentales recae en los Estados miembros del Consejo de Europa. Esta tarea se debe cumplir de conformidad con el CEDH, según su interpretación por el Tribunal. También resultan pertinentes otros instrumentos jurídicamente vinculantes del Consejo de Europa, en particular el Convenio sobre la ciberdelincuencia (en lo sucesivo, el Convenio de Budapest), el Convenio para la protección de los niños contra la explotación y el abuso sexual (STCE n.º 201; en lo sucesivo, el Convenio de Lanzarote) y el Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE n.º 108; en lo sucesivo, el Convenio 108).

18. Otras normas no vinculantes adoptadas por el Consejo de Ministros brindan orientación a los Estados miembros sobre asuntos relacionados con Internet, entre ellas: la Recomendación CM/Rec(2007)16 del Consejo de Ministros a los Estados miembros sobre medidas para promover el valor de servicio público de Internet; la Recomendación CM/Rec(2008)6 del Consejo de Ministros a los Estados miembros sobre medidas para promover el respeto de la libertad de expresión y de información con respecto a los filtros en Internet; la Recomendación CM/Rec(2010)13 del Consejo de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles; la Recomendación CM/Rec (2011)7 del Consejo de Ministros a los Estados miembros sobre un nuevo concepto de los medios de comunicación; la Recomendación CM/Rec(2012)4 del Consejo de Ministros a los Estados miembros sobre la protección de los derechos humanos con respecto a los servicios de redes sociales; y la Recomendación CM/Rec(2012)3 del Consejo de Ministros a los Estados miembros sobre la protección de los derechos humanos en el contexto de los motores de búsqueda.

19. El segundo apartado del preámbulo especifica que las obligaciones de los Estados relativas a respetar, proteger y promover los derechos humanos dan lugar a la supervisión sobre empresas privadas. Esta afirmación se deriva del Artículo 1 del CEDH, según el cual los Estados deberán garantizar a toda persona bajo su jurisdicción los derechos y libertades definidos en el Convenio. Esto incluye la protección contra violaciones de los derechos humanos por actores no estatales y exige emprender acciones adecuadas para prevenir, investigar, castigar y reparar tales violaciones mediante legislaciones y medidas efectivas. El Tribunal ha afirmado en sus sentencias que los Estados tienen obligaciones positivas en lo que se refiere a proteger los derechos y las libertades fundamentales de las personas en Internet, en particular en relación con la libertad de expresión⁴, la protección de los niños y los jóvenes⁵, la protección de la moral y los derechos de los demás⁶, la lucha contra los discursos racistas o xenófobos, y la lucha contra la discriminación y el odio racial⁷. Además, el Tribunal ha juzgado responsables a los Estados por no proteger a los ciudadanos de los efectos adversos sobre sus derechos y libertades que se desprendan de las acciones de empresas privadas.⁸ El segundo apartado subraya también el principio de la universalidad e indivisibilidad de los derechos humanos, que se basa en la Declaración de Viena, proclamada en la Cumbre de Jefes de Estado y de Gobierno de los Estados miembros del Consejo de Europa, celebrada el 9 de octubre de 1993.

20. El tercer apartado del preámbulo reafirma el valor de servicio público de Internet, como se establece en la Recomendación CM/Rec(2007)16 del Consejo de Ministros.⁹ Teniendo en cuenta el importante papel que desempeña Internet en las actividades diarias de los usuarios y la necesidad de asegurar la protección de sus derechos humanos en línea, la recomendación hace énfasis en que las

⁴ Véase *Özgür Gündem c. Turquía*, n.º 23144/93, §§ 42-46.

⁵ *K.U. c. R.U.*, n.º 2872/02.

⁶ *Pay c. R.U.*, n.º 32792/05.

⁷ *Féret c. Bélgica* n.º 15615/07.

⁸ *López Ostra c. España*, n.º 16798/90, § 44-58; *Taşkın y otros c. Turquía*; *Fadeyeva c. Federación Rusa*. En el caso *Khurshid Mustafa y Tarzibachi c. Suecia*, n.º 23883/06, el Tribunal consideró que la interpretación de una jurisdicción nacional con respecto a un acto privado (contrato) comprometía la responsabilidad del Estado demandado. De este modo, amplió el alcance de la protección contemplada en el Artículo 10 a las restricciones impuestas por personas privadas.

⁹ Recomendación CM/Rec(2007)16 del Comité de Ministros a los Estados miembros sobre medidas para promover el valor de servicio público de Internet.

personas no deberán estar sujetas a interferencias ilícitas, innecesarias o desproporcionadas en el ejercicio de sus derechos y libertades.

21. El cuarto apartado del preámbulo define el objetivo de la recomendación en lo que se refiere a favorecer la comprensión de parte de los usuarios y promover el ejercicio efectivo de los derechos humanos en línea, incluido el acceso a recursos efectivos. En este sentido, resulta importante informar a los usuarios acerca de los riesgos para sus derechos y libertades fundamentales, y acerca de las posibilidades de reparación. La afirmación relativa a las oportunidades que brinda Internet en términos de transparencia y responsabilidad en los asuntos públicos explica un elemento fundamental de la recomendación, que consiste en habilitar a las personas y las comunidades para que participen en la vida democrática.

Parte dispositiva de la recomendación

22. El apartado 5 afirma un principio clave de las normas del Consejo de Europa en relación con Internet: que los derechos y libertades fundamentales se aplican por igual a entornos dentro y fuera de la red¹⁰. Este enfoque también ha sido afirmado por el Consejo de Derechos Humanos de las Naciones Unidas en su Resolución de 2012 sobre la Promoción, protección y disfrute de los derechos humanos en Internet. Promover la aplicación de la Guía reforzará la protección de los derechos humanos y las libertades fundamentales, en cumplimiento de las normas existentes en materia de derechos humanos.

23. El apartado 5.1 recomienda a los Estados miembros que la Guía sea promovida no solo por las autoridades públicas sino también a través del sector privado. Esto podría incluir su publicación y difusión en formatos impresos o adaptaciones en formatos electrónicos. Las autoridades públicas pertinentes también podrían ponerla a disposición en sus sitios web. Se podría animar al sector privado a hacer lo mismo.

24. El apartado 5.2 reafirma que el ejercicio de los derechos humanos y las libertades fundamentales en Internet puede estar sujeto a restricciones que persigan objetivos legítimos y que sean necesarias en una sociedad democrática, como se establece en los artículos relevantes del CEDH. A fin de garantizar el cumplimiento de estas condiciones, el Consejo de Ministros recomienda a los Estados miembros que evalúen, revisen periódicamente y, en su caso, eliminen las restricciones relativas al ejercicio de los derechos humanos y las libertades fundamentales en Internet.

25. El apartado 5.3 insta a los Estados miembros a incrementar sus esfuerzos para garantizar el derecho a un recurso efectivo, por ejemplo asegurando una mejor coordinación y cooperación entre las actuales instituciones, entidades (incluidos órganos de reglamentación de las comunicaciones electrónicas) y comunidades pertinentes que ofrezcan mecanismos de reparación, como en el contexto del tratamiento de quejas formuladas por los usuarios de Internet. Asimismo, la recomendación reconoce que hay una variedad de mecanismos de reparación disponibles en los distintos Estados miembros, tales como autoridades de protección de datos, mediadores, procedimientos judiciales o líneas de asistencia telefónica. Los Estados miembros también podrían realizar un examen de los mecanismos de reparación existentes en sus jurisdicciones y compilar la información pertinente en un inventario de uso fácil para el usuario. Tal información podría difundirse junto con la Guía, por ejemplo a manera de anexo. Esta es una de las acciones de seguimiento que podrían tomarse tras la adopción de la recomendación.

26. Por su naturaleza misma, Internet funciona mediante el envío y la recepción de solicitudes de información que atraviesan las fronteras y que, por lo tanto, son independientes de estas. Esto significa que los derechos humanos y las libertades fundamentales en Internet en los Estados miembros pueden estar expuestos a acciones de parte de actores estatales y no estatales más allá de las fronteras del Consejo de Europa; por ejemplo, la libertad de expresión y el acceso a la información, así como el respeto de la privacidad con respecto a los datos personales pueden ser objeto de injerencias. Por lo tanto, el apartado 5.4 recomienda la coordinación entre Estados, que sean o no miembros del Consejo de Europa, así como con los actores no estatales.

¹⁰ Véase la Declaración del Comité de Ministros sobre Principios de gobernanza de internet, principio 1, "Derechos humanos, democracia y Estado de derecho".

27. El apartado 5.5 recomienda a los Estados miembros fomentar un diálogo auténtico entre el sector privado y las autoridades estatales pertinentes, así como la sociedad civil, con respecto al ejercicio de la responsabilidad social de las empresas. Un principio fundamental de los Principios Rectores sobre las empresas y los derechos humanos¹¹ es que las empresas deben respetar los derechos humanos. En otras palabras, deben evitar toda violación de estos y corregir todo impacto perjudicial sobre los mismos en el que resulten implicadas. Se hace énfasis en la transparencia y la rendición de cuentas por parte de los actores del sector privado como un medio importante para demostrar su responsabilidad, así como en su labor de promoción y difusión activa de la Guía. Por ejemplo, los proveedores de servicios de Internet y de acceso a contenidos podrían hacer referencia a la Guía en sus condiciones de uso de los servicios.

28. El apartado 5.6 reconoce que la sociedad civil puede contribuir de manera esencial a promover la Guía y su cumplimiento. Por lo tanto, se recomienda que los Estados miembros animen a los activistas y organizaciones de la sociedad civil a colaborar en la difusión y aplicación de la Guía, y a basarse en ella cuando aboguen por la puesta en marcha y el cumplimiento de normas de derechos humanos.

Guía de los derechos humanos para los usuarios de Internet

Introducción

29. La Guía se dirige directamente al usuario. Es una herramienta para el usuario de Internet, que puede ser cualquier persona que no cuente con un conocimiento especializado de Internet adquirido a través de la enseñanza o la formación. En particular, se centra en la capacidad de los usuarios para controlar sus actividades en Internet (p. ej.: su identidad, sus datos personales). Los usuarios deberían estar plenamente informados acerca de las diferentes opciones que eligen en Internet que pueden afectar sus derechos y libertades, y acerca de las consecuencias de dar su consentimiento para tales opciones. Asimismo, deberían comprender los límites de sus derechos y deberían conocer los mecanismos de recurso a su disposición.

30. La Guía está basada en el CEDH y en la jurisprudencia pertinente del Tribunal. También se inspira en otros instrumentos jurídicamente vinculantes del Consejo de Europa. Se apoya igualmente en otros instrumentos, como ciertas declaraciones y recomendaciones del Consejo de Ministros. La Guía no afecta a la aplicabilidad de las normas existentes de derechos humanos a partir de las cuales ha sido elaborada. Los derechos y las libertades contemplados en la Guía son aplicables en virtud de los instrumentos jurídicos en los que se basan. La Guía hace referencia a normas de derechos humanos ya existentes y a los mecanismos relevantes para su cumplimiento, y no establece nuevos derechos y libertades. La Guía no es una explicación de carácter prescriptivo ni exhaustivo con respecto a las normas de derechos humanos. Por ejemplo, a fin de ayudar a los usuarios a comprender sus derechos y a protegerse y proteger a los demás, cabría tener en cuenta mayores aclaraciones sobre las posibles restricciones e injerencias en los derechos humanos, así como orientaciones sobre la manera de lidiar con la violencia y los abusos en Internet. La Guía queda abierta a actualizaciones a fin de seguir las nuevas normas del Consejo de Europa y la jurisprudencia del Tribunal a medida que la tecnología evolucione.

Acceso y no discriminación

¹¹ Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar" (A/HRC/17/31), respaldado por el Consejo de Derechos Humanos mediante la Resolución relativa a Los derechos humanos y las empresas transnacionales y otras empresas, A/HRC/RES/17/4. En particular, los Principios Rectores prevén que los Estados deberían: aplicar leyes que tengan como objetivo o efecto obligar a las empresas a respetar los derechos humanos, así como evaluar periódicamente la idoneidad de tales leyes y corregirlas cuando sea necesario; garantizar que otras leyes y políticas relativas a la creación y el funcionamiento continuo de las empresas, como el derecho de sociedades, no limiten sino —al contrario— favorezcan el respeto por los derechos humanos desde el ámbito empresarial; brindar orientación efectiva a las empresas sobre la manera de respetar los derechos humanos en todas sus operaciones; incitar a las empresas a que comuniquen de qué modo corrigen su impacto sobre los derechos humanos y, en su caso, exigirles dicha comunicación.

31. La Guía hace énfasis en principios y consideraciones que se estiman intrínsecamente vinculados y generalmente aplicables a todos los derechos humanos y libertades fundamentales en ella contemplados, incluido el acceso a Internet y el principio de no discriminación.

32. Si bien el acceso a Internet aún no está reconocido de manera formal como un derecho humano (pudiendo notarse diferencias en los contextos nacionales, incluidas las políticas y legislaciones internas), sí se considera como una condición y un medio para facilitar la libertad de expresión y otros derechos y libertades¹². En consecuencia, la desconexión de un usuario de Internet podría afectar negativamente al ejercicio de sus derechos y libertades y podría incluso asimilarse a una restricción del derecho a la libertad de expresión, incluido el derecho a recibir y comunicar información. De acuerdo con el Tribunal, hoy en día Internet se ha convertido en uno de los medios principales para que las personas ejerzan el derecho a la libertad de expresión e información. La libertad de expresión se aplica no solo al contenido de la información sino también a los medios para difundir esta, ya que toda restricción impuesta sobre tales medios necesariamente interfiere en el derecho a recibir y comunicar información. Estas interferencias solo pueden aceptarse si cumplen las condiciones establecidas en el Artículo 10, apartado 2 del CEDH, según lo interpreta el Tribunal.¹³ Una medida que influya en el acceso de las personas a Internet compromete la responsabilidad del Estado en virtud del Artículo 10.¹⁴

33. En este contexto, la Guía establece que los usuarios de Internet no deberían quedar desconectados contra su voluntad, salvo en caso de decisión judicial. No obstante, esto no debe entenderse como un obstáculo a medidas de desconexión legítimas como aquellas que se desprendan de obligaciones contractuales. Los consumidores que no paguen el servicio pueden ser desconectados de Internet. Ahora bien, esta debería ser una medida de último recurso. Asimismo, en el marco del ejercicio del control parental sobre el uso de Internet, los niños pueden estar sujetos a que se descontinue su acceso a Internet dependiendo de su edad y madurez.

34. Los usuarios de Internet deberían disponer de recursos efectivos contra las medidas de desconexión cuando estas no respondan a una orden judicial. Esto incluye la información a los usuarios, por parte de los proveedores de servicio, sobre los motivos y fundamentos jurídicos de la medida de desconexión, así como sobre los procedimientos para oponerse a dicha medida y solicitar el restablecimiento del acceso completo a Internet. Las solicitudes de esta índole deberían ser tratadas en plazos razonables. Además, en ejercicio del derecho a un proceso equitativo, todo usuario de Internet debería poder solicitar que una autoridad judicial o administrativa competente examine la medida de desconexión aplicada. Estos aspectos relacionados con el debido proceso se presentan de manera resumida en la última sección de la Guía, bajo el título "Recursos efectivos".

35. Las medidas o acciones positivas de las autoridades del Estado para garantizar que toda persona tenga una conexión a Internet son otra faceta del tema del acceso a Internet. El Consejo de Ministros del Consejo de Europa ha recomendado a sus Estados miembros promover el valor de servicio público de Internet.¹⁵ Esto se entiende como "la significativa dependencia de las personas con respecto a Internet como una herramienta esencial para las actividades diarias (comunicación, información, conocimiento, transacciones comerciales) y la expectativa legítima consiguiente de que los servicios de Internet sean accesibles, asequibles, seguros, fiables y continuos". Esta sección informa al usuario que debería tener un acceso a Internet asequible y no discriminatorio.

¹² Según subrayó Frank La Rue, Relator Especial de las Naciones Unidas sobre la promoción y protección del derecho a la libertad de opinión y de expresión: "En vista de que Internet se ha convertido en un instrumento indispensable para ejercer diversos derechos humanos, luchar contra la desigualdad y acelerar el desarrollo y el progreso humanos, la meta del acceso universal a Internet ha de ser prioritaria para todos los Estados. En consecuencia, cada uno debe elaborar una política eficaz y concreta en consulta con personas de todos los sectores de la sociedad, entre ellos el sector privado, y con los ministerios gubernamentales competentes, a fin de que Internet resulte ampliamente disponible, accesible y asequible para todos los sectores de la población". "Así pues, al funcionar como catalizador del derecho personal a la libertad de opinión y de expresión, Internet también facilita el ejercicio de otros derechos humanos diversos". http://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/a.hrc.17.27_en.pdf.

¹³ Véase la nota 2 anterior, § 50. Véase también *Autronic AG c. Suiza* (n.º 12726/87). En el caso *Khurshid Mustafa y Tarzibachi c. Suecia*, n.º 23883/06, el Tribunal consideró que la interpretación de una jurisdicción nacional con respecto a un acto privado (contrato) comprometía la responsabilidad del Estado demandado. De este modo, amplió el alcance de la protección contemplada en el Artículo 10 a las restricciones impuestas por personas privadas.

¹⁴ Véase la nota 2 anterior, § 53.

¹⁵ Véase la nota 9 anterior, CM/Rec(2007)16, sección II.

36. El derecho de acceso a los contenidos de Internet está relacionado con el derecho a recibir y comunicar información, como se establece en el Artículo 10 del CEDH.¹⁶ El Consejo de Ministros del Consejo de Europa ha afirmado que todo usuario de Internet debería tener el mayor acceso posible a los contenidos, aplicaciones y servicios de Internet que elija, independientemente de que se ofrezcan o no de manera gratuita, a través de los dispositivos de su elección. Este es un principio general, conocido usualmente como “neutralidad de la red”, que debería aplicarse sin importar la infraestructura o la red utilizada para la conectividad de Internet.¹⁷

37. Las autoridades públicas deberían acometer esfuerzos razonables para facilitar el acceso a Internet a categorías específicas de individuos, como quienes viven en áreas alejadas o quienes tienen alguna discapacidad. Esto se basa en el principio del servicio comunitario universal, como se establece en la Recomendación Rec(99)14 del Consejo de Ministros referente a los nuevos servicios de comunicación e información.¹⁸ La Guía pone de relieve que las personas que viven en zonas rurales o alejadas geográficamente, que disponen de bajos ingresos o que tienen alguna discapacidad o necesidades especiales pueden esperar medidas específicas de parte de las autoridades públicas en relación con su acceso a Internet.

38. La idea de que las personas con discapacidades pueden esperar un acceso a Internet no discriminatorio y equivalente al de los demás usuarios se deriva de los instrumentos del Consejo de Europa que recomiendan a los Estados miembros tomar medidas destinadas a fomentar la puesta a disposición de medios adecuados para el acceso a Internet y a las TIC para los usuarios discapacitados.¹⁹ Los Estados miembros deberían promover el acceso asequible a Internet, teniendo en cuenta la importancia del diseño, la necesidad de sensibilización entre estos grupos o personas, el carácter adecuado y atractivo del acceso y los servicios, así como los aspectos de adaptabilidad y compatibilidad.²⁰

39. El principio de no discriminación debería aplicarse a las interacciones de los usuarios con las autoridades públicas, los proveedores de servicios de Internet, los proveedores de acceso a contenidos y otras empresas, otros usuarios o grupos de usuarios. El cuarto apartado retoma lo enunciado en el Artículo 14 del CEDH y el Artículo 1 del Protocolo 12 al CEDH, ambos relacionados con la prohibición de la discriminación.

Libertad de expresión e información

40. Esta sección se refiere al derecho a la libertad de expresión, consagrado en el Artículo 10 del CEDH. El Tribunal ha afirmado en su jurisprudencia que el Artículo 10 se puede aplicar plenamente a Internet.²¹ El derecho a la libertad de expresión comprende el derecho a expresar libremente opiniones, ideas y puntos de vista, y a buscar, recibir y comunicar informaciones sin consideración de fronteras. Los usuarios de Internet deberían ser libres de expresar sus convicciones políticas, así como sus opiniones religiosas o no religiosas. Este último aspecto está relacionado con el ejercicio del derecho a la libertad de pensamiento, de conciencia y de religión, consagrado en el Artículo 9 del CEDH. La libertad de expresión resulta aplicable no solo para las “informaciones” o “ideas” que son recibidas favorablemente o consideradas como inofensivas o indiferentes, sino también para aquellas que chocan, inquietan u ofenden.²²

41. Debe existir un equilibrio entre el ejercicio del derecho a la libertad de expresión por los usuarios de Internet y el derecho a la protección de la reputación. En diversos casos, el Tribunal ha sostenido que este último es un derecho protegido por el Artículo 8 del CEDH, relativo al respeto a la

¹⁶ Véase la nota 2 anterior, § 50.

¹⁷ Declaración del Comité de Ministros sobre la neutralidad de la red, adoptada por el Comité de Ministros el 29 de septiembre de 2010. Véase también la Directiva 2002/21/CE del Parlamento Europeo y del Consejo, de 7 de marzo de 2002, relativa a un marco regulador común de las redes y los servicios de comunicaciones electrónicas, Artículo 8(4) g.

¹⁸ Véase la nota 9 anterior, CM/Rec(2007)16, Anexo, sección II; Recomendación Rec(99)14 del Comité de Ministros a los Estados miembros sobre el servicio comunitario universal referente a los nuevos servicios de comunicación e información, principio 1.

¹⁹ *Ibid.*

²⁰ Véase la nota 9 anterior, CM/Rec(2007)16, Anexo, sección II.

²¹ Véase la nota 2 anterior, §50.

²² *Handyside c. Reino Unido*, sentencia del 7 de diciembre de 1976, Serie A, n.º 24, apartado 49.

vida privada.²³ Asimismo, ha considerado que, como una cuestión de principio, los derechos garantizados en virtud de los Artículos 8 y 10 merecen un respeto equivalente. En este sentido, los criterios que estima relevantes para el equilibrio entre el derecho a la libertad de expresión y el derecho al respeto a la vida privada incluyen: contribución a un debate de interés general, notoriedad de la persona afectada, tema del informe, conducta anterior de la persona interesada, método de obtención de la información y veracidad de la misma, contenido, forma y consecuencias de la publicación, y gravedad de la sanción impuesta.²⁴ Así, la Guía especifica que el usuario de Internet debería tomar debidamente en consideración la cuestión de la reputación de los demás, que abarca el derecho al respeto a la vida privada.

42. La protección del Artículo 10 del CEDH no se aplica a algunas expresiones, como los discursos de odio. El Tribunal ha afirmado que las formas de expresión que inciten al odio o que nieguen los valores fundamentales del CEDH quedan excluidas de la protección contemplada en el Artículo 10.²⁵ A este respecto, el Tribunal aplica el Artículo 17 del CEDH. Si bien no existe una definición universalmente aceptada de los discursos de odio, el Consejo de Ministros del Consejo de Europa ha afirmado que por el término “discurso de odio” se entenderán todas las formas de expresión que propaguen, inciten, promuevan o justifiquen el odio racial, la xenofobia, el antisemitismo u otras formas de odio basadas en la intolerancia, incluida la intolerancia expresada por agresivo nacionalismo y el etnocentrismo, la discriminación y la hostilidad contra las minorías, los migrantes y las personas de origen inmigrante.²⁶ El apartado 2 de la sección sobre la libertad de expresión aporta información concisa formulada en un lenguaje sencillo para el usuario en relación con la idea de que los discursos de odio no están cubiertos por el Artículo 10 del CEDH. Este apartado no apunta a explicar en términos jurídicos las distintas maneras en que el Artículo 10 y el Artículo 17 del CEDH podrían aplicarse a los discursos de odio. Teniendo en cuenta el carácter jurídico de esta distinción, se consideró más apropiado incluir la información sobre este punto en la Exposición de motivos.

43. Los usuarios tienen derecho a recibir y comunicar información en Internet. En particular, tienen derecho a crear, reutilizar y distribuir contenido usando Internet. El Tribunal ha examinado la relación entre la protección de la propiedad intelectual y la libertad de expresión en casos de condena penal por infracción a los derechos de autor. En la materia, ha considerado tales condenas como injerencias en el derecho a la libertad de expresión que solo se justifican si están previstas por la ley, obedecen al objetivo legítimo de proteger los derechos de los demás, y se consideran necesarias en una sociedad democrática.²⁷ El acto de compartir o de autorizar a otros a compartir archivos en Internet, incluso en el caso de materiales que estén protegidos por derechos de autor o que tengan fines de lucro, está cubierto por el derecho a recibir y comunicar información, como se prevé en el Artículo 10 del CEDH.²⁸ Ahora bien, este derecho no es absoluto, por lo cual es necesario sopesar, por una parte, el interés de compartir información y, por otra, el interés de proteger los derechos de autor. El Tribunal ha subrayado que la propiedad intelectual goza de la protección otorgada por el Artículo 1 del Protocolo al CEDH. Así, se trata de hallar el equilibrio entre dos intereses en conflicto, ambos protegidos por el CEDH.

44. La recomendación del Consejo de Ministros a los Estados miembros para promover el valor de servicio público de Internet incluye orientación específica sobre medidas y estrategias en relación con la libertad de comunicación y de creación en Internet sin consideración de fronteras. En particular, deberían tomarse medidas para facilitar, cuando sea apropiado, la “reutilización” de contenidos de Internet, es decir, el uso de recursos existentes de contenido digital para crear contenidos o servicios futuros de una manera que sea compatible con el respeto de los derechos de propiedad intelectual.²⁹

²³ Chauvy y otros, n.º 64915/01 § 70; Pfeifer c. Austria, n.º 12556/03, § 35; y Polanco Torres y Movilla Polanco c. España, n.º 34147/06, § 40.

²⁴ Delfi As c. Estonia, n.º 64569/09, § 78-81 (este caso ha sido remitido a la Gran Sala del Tribunal); Axel Springer AG c. Alemania n.º 39954/08 § 89-95, y Von Hannover c. Alemania (n.º 2), n.ºs 40660/08 y 60641/08 §§ 108-113.

²⁵ Féret c. Bélgica n.º 15615/07; Garaudy c. Francia n.º 65831/01, 24.06.2003, decisión de admisibilidad; Leroy c. Francia n.º 36109/03; Jersild c. Dinamarca n.º 15890/89; Vejdeland y otros c. Suecia n.º 1813/07.

²⁶ Recomendación (97) 20 del Comité de Ministros a los Estados miembros sobre “Discurso de odio”.

²⁷ Neij y Sunde Kolmisoppi c. Suecia n.º 40397/12. Véase también Ashby Donald y otros c. Francia, n.º 36769/08 § 34.

²⁸ *Ibid.*

²⁹ Véase la nota 9 anterior, CM/Rec(2007)16, Anexo, sección III, segundo guion.

45. El apartado 4 brinda una visión general de los requisitos que deberían cumplir las restricciones al derecho a la libertad de expresión. De conformidad con el artículo 10 del CEDH, los Estados miembros tienen la obligación fundamental de no interferir en la comunicación de información entre las personas, sean estas físicas o jurídicas. El Tribunal ha afirmado que el ejercicio efectivo del derecho a la libertad de expresión puede exigir también medidas positivas de protección, incluso en el contexto de las relaciones entre individuos. La responsabilidad de un Estado se puede ver comprometida por no adoptar una legislación nacional adecuada³⁰. También podrá establecerse que ha habido una violación del CEDH cuando la interpretación dada por una jurisdicción nacional a un acto jurídico —contrato privado, documento público, disposición legal o práctica administrativa— presente un carácter no razonable, arbitrario, discriminatorio o, de manera más general, no acorde con los principios subyacentes del CEDH.³¹

46. La libertad de expresión no es un derecho absoluto y puede estar sujeta a restricciones. Las injerencias con respecto a la libertad de expresión han de entenderse como toda forma de restricción proveniente de cualquier autoridad que ejerza deberes y poderes públicos o que actúe en el servicio público, como tribunales, fiscalías, policía, organismos de cumplimiento de la ley, servicios de inteligencia, consejos centrales o locales, entes gubernamentales, órganos de decisión del ejército y estructuras profesionales públicas.

47. Con arreglo a lo dispuesto en el Artículo 10, apartado 2, del CEDH, toda injerencia deberá estar prevista por la ley. Esto significa que la ley deberá ser accesible, clara y suficientemente precisa para permitir a los individuos regular su comportamiento. La ley debería prever garantías suficientes contra las medidas de restricción abusivas, incluido un control efectivo por un tribunal u otro órgano decisorio independiente.³² Una injerencia también deberá obedecer a un objetivo legítimo que tenga como interés la seguridad nacional, la integridad del territorio o la seguridad pública, la defensa del orden y la prevención del delito, la protección de la salud o la moral, la protección de la reputación o de los derechos de los demás, el propósito de impedir que se revele información recibida de manera confidencial, o la defensa de la autoridad e imparcialidad de la rama judicial. Esta lista es exhaustiva, pero su interpretación y su alcance evolucionan con la jurisprudencia del Tribunal. Asimismo, una injerencia deberá ser necesaria en una sociedad democrática, es decir, deberá probarse que responde a una necesidad social urgente, que busca un objetivo legítimo y que es el medio menos restrictivo para alcanzar tal objetivo.³³ Estos requisitos se resumen en un lenguaje claro para el usuario, a saber, que toda restricción a la libertad de expresión debe tener un carácter no arbitrario, debe obedecer a un objetivo legítimo de acuerdo con el CEDH (por ejemplo, la protección de la seguridad nacional, el orden público, la salud pública o la moral) y debe cumplir las leyes sobre derechos humanos.

48. En los apartados siguientes de la Exposición de motivos se presenta información más detallada sobre las garantías de las que deberían disfrutar los usuarios de Internet cuando existan restricciones al derecho a la libertad de expresión en línea. El bloqueo y el filtrado son ejemplos de restricciones que podrían considerarse como violaciones del derecho a la libertad de expresión. Algunos principios generales relativos al bloqueo y el filtrado se basan en la jurisprudencia del Tribunal o en otras normas relevantes adoptadas por el Consejo de Ministros³⁴.

49. A escala nacional, las autoridades estatales pueden tomar medidas de bloqueo y filtrado únicamente en la medida en que estas se apliquen a contenidos específicos claramente identificables, sobre la base de una decisión —emitida por una autoridad nacional competente— que establezca su ilegalidad y que pueda ser examinada por un tribunal o un órgano regulador independiente e imparcial, de acuerdo con lo exigido en el Artículo 6 del CEDH.³⁵ Con el propósito de evitar bloqueos injustificados de contenido, las autoridades del Estado deberían garantizar que todos los filtros sean examinados tanto antes como durante su instalación, de tal manera que sus efectos

³⁰ Vgt Verein gegen Tierfabriken c. Suiza, n.º 24699/94, § 45.

³¹ Véase Khurshid Mustafa y Tarzibachi c. Suecia n.º 23883/06 § 33; Plaand Puncernau c. Andorra, n.º 69498/01, § 59, CEDH 2004-VIII.

³² Véase la nota 2 anterior, § 64.

³³ *Ibid.* § 66-70.

³⁴ Recomendación CM/Rec(2008)6 del Comité de Ministros a los Estados miembros sobre medidas para promover el respeto de la libertad de expresión y de información con respecto a los filtros en Internet; véase el Anexo, parte III, ii. Véase también la nota 1 anterior.

³⁵ *Ibid.* CM/Rec(2008)6, véase el Anexo, parte III, iv.

sean proporcionales al objetivo de la restricción y, de este modo, necesarios en una sociedad democrática.³⁶

50. Las medidas adoptadas con miras a bloquear contenidos específicos de Internet no deberán usarse de modo arbitrario como un medio de bloqueo general de la información de Internet. Tampoco deberán tener un efecto colateral en el sentido de impedir el acceso a grandes cantidades de información de una manera que restrinja sustancialmente los derechos de los usuarios de Internet.³⁷ Asimismo, tales medidas deberán estar previstas por la ley. Debería haber una supervisión estricta del alcance del bloqueo y un control judicial efectivo a fin de evitar todo abuso de poder.³⁸ El examen judicial de las medidas en cuestión debería sopesar los intereses en conflicto, apuntar a un equilibrio entre estos y determinar si podrían aplicarse medidas de menor alcance para bloquear el acceso a los contenidos específicos de Internet.³⁹ Los requisitos y principios arriba mencionados no impiden la instalación de filtros para la protección de los menores en lugares específicos en los que estos tengan acceso a Internet, como escuelas y bibliotecas.⁴⁰

51. El filtrado y la desindexación de contenidos de Internet por motores de búsqueda conllevan el riesgo de violar la libertad de expresión de los usuarios de Internet. Los motores de búsqueda tienen la libertad de explorar e indexar la información disponible en la red. No deberían estar obligados a supervisar sus redes y servicios de manera proactiva con la finalidad de detectar contenidos potencialmente ilícitos, y no deberían realizar ninguna actividad *ex ante* de bloqueo o filtrado, salvo que así lo exija una orden judicial o una autoridad competente. La desindexación o el filtrado de sitios web específicos a solicitud de las autoridades públicas deberían ser transparentes, estar estrechamente definidos y ser examinados de manera periódica, de conformidad con las exigencias relativas al debido proceso.⁴¹

52. Esta sección también identifica algunas de las garantías de las que deberían disfrutar los usuarios de Internet cuando se apliquen restricciones. En particular, se hace énfasis en la información que debería recibir el usuario y en las posibilidades de oponerse a las restricciones. Esta cuestión se aborda en la recomendación del Consejo de Ministros del Consejo de Europa sobre medidas de filtrado y bloqueo.⁴² Los usuarios de Internet deberían recibir información sobre cuándo se ha activado un filtro y por qué se ha filtrado un tipo específico de contenido. Asimismo, deberían recibir información que les permita comprender el modo y los criterios de funcionamiento del filtro (por ejemplo, listas negras, listas blancas, bloqueo por palabras clave, clasificación de contenido, desindexación o filtrado de contenidos o sitios web específicos por los motores de búsqueda). Debería brindárseles orientación e información concisa sobre la manera de deshabilitar manualmente un filtro activo, es decir, a quién pueden contactar cuando parezca que se ha bloqueado contenido de modo injustificado y por qué medios anular un filtro para un sitio web o un contenido específico. Los usuarios deberían contar con medios de recurso y reparación efectivos y fácilmente accesibles, incluida la suspensión de los filtros, en los casos en los que aleguen que el contenido ha sido objeto de un bloqueo injustificado.

53. Puede ocurrir que empresas, tales como las redes sociales, eliminen contenidos creados y puestos en línea por los usuarios de Internet. Asimismo, estas empresas pueden desactivar la cuenta de un usuario (p. ej.: el perfil o la presencia de un usuario en las redes sociales), usando como justificación el incumplimiento de las condiciones de uso del servicio. Estos actos podrían constituir una injerencia en el derecho a la libertad de expresión y el derecho a recibir y comunicar información, salvo que se cumplan las condiciones del Artículo 10, apartado 2 del CEDH, según su interpretación por el Tribunal.⁴³

³⁶ *Ibid.*

³⁷ Véanse la nota 2 anterior, § 52, 66-68 y la Declaración sobre la libertad de comunicación en internet, del Comité de Ministros

³⁸ *Ibid.*, nota 2 anterior, § 64. Asociación Ekin c. Francia, n.º 39288/98

³⁹ *Ibid.*, nota 2 anterior, § 64-66.

⁴⁰ Véase la Declaración sobre la libertad de comunicación en internet, principio 3.

⁴¹ Véase la Recomendación CM/Rec(2012)3 del Comité de Ministros a los Estados miembros sobre la protección de los derechos humanos con respecto a los motores de búsqueda, Anexo, parte III.

⁴² Véase la nota 34 anterior, CM/Rec(2008)6, véase el Anexo, parte I; *Ibid.*, CM/Rec(2012)3, Anexo, parte III.

⁴³ Recomendación CM/Rec (2011)7 del Comité de Ministros a los Estados miembros sobre un nuevo concepto de los medios de comunicación, § 7, Anexo, § 15; 44-47; 68 -69; Recomendación CM/Rec(2012)4 del Comité de Ministros a los Estados miembros sobre la protección de los derechos humanos con respecto a los servicios de redes sociales, § 3.

54. De acuerdo con los Principios Rectores sobre las empresas y los derechos humanos de las Naciones Unidas (que no son un instrumento vinculante), las empresas tienen la responsabilidad de respetar los derechos humanos. Esto significa que han de evitar ser causantes de efectos negativos sobre los derechos humanos y evitar contribuir a ellos. Asimismo, han de prever medios de reparación o contribuir a la reparación de esos efectos. El deber de proteger y de brindar acceso a recursos efectivos incumbe en esencia a los Estados. A esto se hace referencia en el apartado 5 de la sección sobre la libertad de expresión. La responsabilidad social corporativa de los proveedores de servicios en línea incluye el compromiso de combatir los discursos de odio y otros contenidos que inciten a la violencia o la discriminación. Los proveedores de servicios en línea deberían estar atentos al uso y a las respuestas editoriales que reciben las expresiones fundadas en prejuicios racistas, xenófobos, antisemitas, misóginos, sexistas (incluso con respecto a personas lesbianas, gais, bisexuales y transexuales) o de otra índole.⁴⁴ Asimismo, deberían estar preparados para ayudar a los usuarios de Internet a denunciar los contenidos, expresiones o comportamientos que puedan considerarse ilegales.⁴⁵

55. La Guía advierte que los proveedores de servicios en línea que alojan contenidos creados por los usuarios pueden aplicar diferentes niveles de control editorial sobre el contenido publicado a través de sus servicios.⁴⁶ Sin perjuicio de su libertad editorial, deberían garantizar que se respete el derecho de los usuarios de Internet a buscar, recibir y comunicar información, de conformidad con el Artículo 10 del CEDH.⁴⁷ Esto significa que toda restricción aplicada a contenidos generados por los usuarios debería ser específica, estar justificada por la finalidad que busca y ser comunicada al usuario interesado.

56. Los usuarios de Internet deberían poder tomar decisiones informadas en cuanto a usar o no los servicios en línea. En la práctica, el usuario de Internet debería estar plenamente informado acerca de cualquier medida destinada a eliminar los contenidos que ha creado o destinada a desactivar su cuenta, antes de que se aplique la medida en cuestión.⁴⁸ Además, los usuarios de Internet deberían recibir información clara, precisa y abordable (en un lenguaje comprensible para ellos) sobre los hechos y motivos en los que se basen las medidas de eliminación de contenido o de desactivación de una cuenta. Esto abarca las disposiciones legales en las que se apoyen tales medidas y otros elementos considerados para evaluar la proporcionalidad y la legitimidad del objetivo que se pretende alcanzar. Por otra parte, los usuarios deberían poder solicitar que se examine, dentro de un plazo razonable, la decisión de eliminar el contenido o de desactivar la cuenta, y deberían tener la posibilidad de impugnar tal decisión ante una autoridad judicial o administrativa competente.

57. El sexto apartado trata la cuestión del anonimato, basándose en la jurisprudencia del Tribunal, en el Convenio de Budapest y en otros instrumentos del Consejo de Ministros. El Tribunal examinó el tema de la confidencialidad de las comunicaciones en Internet en un caso en el que un Estado miembro del Consejo de Europa no obligó a un proveedor de servicios de Internet a revelar la identidad de una persona que publicó una publicidad indecente relacionada con un menor en un sitio de encuentros por Internet. El Tribunal sostuvo que, si bien la libertad de expresión y la confidencialidad de las comunicaciones son consideraciones de primer orden y los usuarios de servicios de telecomunicaciones e Internet deben tener garantías de respeto de su vida privada y de su libertad de expresión, tales garantías no pueden ser absolutas y, en ocasiones, será necesario renunciar a ellas a favor de otros imperativos legítimos, como la defensa del orden y la prevención del delito o la protección de los derechos y libertades de otras personas. El Estado tiene la obligación positiva de asegurar un marco en el que se concilien estos intereses en conflicto.⁴⁹

58. El Convenio de Budapest no tipifica como delito el uso de la tecnología informática para comunicaciones anónimas. De acuerdo con el Informe explicativo del Convenio, “la modificación de los datos relativos al tráfico con el fin de facilitar comunicaciones anónimas (p. ej.: las actividades de

⁴⁴ *Ibid.*, CM/Rec (2011)7, § 91.

⁴⁵ *Ibid.*, CM/Rec(2012)4, II/10.

⁴⁶ *Ibid.*, CM/Rec (2011)7, § 18; 30-31.

⁴⁷ *Ibid.*, CM/Rec (2011)7, § 7, segundo guion.

⁴⁸ Véase el informe *Account Deactivation and Content Removal: Guiding Principles and Practices for Companies and Users* de Erica Newland, Caroline Nolan, Cynthia Wong y Jillian York, disponible en: http://cyber.law.harvard.edu/sites/cyber.law.harvard.edu/files/Final_Report_on_Account_Deactivation_and_Content_Removal.pdf

⁴⁹ K.U. c. Finlandia, n.º 2872/02 § 49.

los sistemas de redireccionamiento de mensajes de correo electrónico anónimos), o la modificación de datos con el fin de garantizar la seguridad de las comunicaciones (p. ej.: el cifrado) deberían en principio ser consideradas una forma de protección legítima de la vida privada y, por lo tanto, ser consideradas actividades legítimas. Sin embargo, las Partes [en el Convenio de Budapest] tal vez deseen establecer como delito ciertos abusos relacionados con las comunicaciones anónimas, por ejemplo, cuando la información contenida en el encabezamiento del paquete es alterada con el fin de ocultar la identidad del autor del delito”.⁵⁰

59. El Consejo de Ministros del Consejo de Europa afirmó el principio del anonimato en su Declaración sobre la libertad de comunicación en Internet.⁵¹ Así, a fin de garantizar la protección contra la vigilancia en línea y favorecer la libertad de expresión, los Estados miembros del Consejo de Europa deberían respetar la voluntad de los usuarios de Internet de no revelar su identidad. No obstante, el respeto del anonimato no impide que los Estados miembros tomen medidas para perseguir a los autores de delitos, de conformidad con el derecho interno, el CEDH y otros acuerdos internacionales en los ámbitos de justicia y de policía.

Reunión, asociación y participación

60. El derecho a la libertad de reunión y de asociación está consagrado en el Artículo 11 del CEDH. También está relacionado con los principios establecidos por el Tribunal en cuanto a la protección del discurso político, en particular en el sentido de que, conforme al Artículo 10, apartado 2 del CEDH, existe un margen reducido para las restricciones al discurso político o a los debates sobre cuestiones de interés público.⁵²

61. Los usuarios de Internet tienen derecho a reunirse y asociarse pacíficamente con otras personas usando Internet. En particular, tienen derecho a constituir, unirse a, movilizar y participar en grupos sociales, asociaciones o sindicatos usando las herramientas de Internet. Esto incluye, por ejemplo, firmar peticiones para participar en campañas u otras formas de acción cívica. Los usuarios deberían tener la libertad de elegir las herramientas (sitios web, aplicaciones u otros servicios) para el ejercicio de sus derechos. El ejercicio de este derecho no depende del reconocimiento formal de los grupos sociales y asociaciones por las autoridades públicas.

62. El derecho a protestar se aplica por igual dentro y fuera de Internet. Las protestas que tienen consecuencias para el público en general, como perturbaciones o bloqueos del acceso a instalaciones, entran dentro de los límites del ejercicio de la libertad de reunión, de conformidad con el Artículo 11 del CEDH. No obstante, puede haber excepciones cuando tales acciones dan lugar a alteraciones de los servicios en línea, como el acceso no autorizado a un sitio web en particular o a un espacio en línea de ingreso restringido, o el tratamiento de contenido digital sin la debida autorización. En últimas, es importante hacer saber al usuario que la libertad y las consecuencias de las protestas en línea que provoquen perturbaciones pueden no aceptarse libremente.

63. Internet se ha convertido en una herramienta que permite a los ciudadanos participar activamente en la construcción y el fortalecimiento de sociedades democráticas. El Consejo de Ministros ha recomendado a los Estados miembros desarrollar y poner en marcha estrategias para la democracia, la participación y el gobierno en línea mediante el uso de las tecnologías de la información y la comunicación (TIC) en los debates y procesos democráticos, tanto en las relaciones entre las autoridades públicas y la sociedad civil, como en la prestación de servicios públicos.⁵³

64. Esto abarca la libertad para participar en los debates de política pública, las iniciativas legislativas y la observación de los procesos de toma de decisiones a nivel local, nacional y global, incluido el derecho a firmar peticiones mediante las TIC, cuando las haya. Esto se basa en las recomendaciones del Consejo de Ministros a los Estados miembros en lo que se refiere a fomentar el uso de las TIC por los ciudadanos (incluso en foros, blogs, chats de política, mensajes instantáneos y otras formas de comunicación entre ciudadanos) para participar en el debate democrático, en

⁵⁰ Convenio de Budapest sobre la ciberdelincuencia, Artículo 2, Informe explicativo, §. 62.

⁵¹ Véase la Declaración sobre la libertad de comunicación en internet, Principio 7.

⁵² Wingrove c. Reino Unido, 25 de noviembre de 1996, § 58, Informes 1996-V.

⁵³ Véase la nota 9 anterior, CM/Rec(2007)16, Anexo, parte I.

campañas virtuales y en el activismo en línea; manifestar sus preocupaciones, ideas e iniciativas; promover el diálogo y el debate con sus representantes y gobiernos; y supervisar a los funcionarios y políticos en asuntos de interés público.

Protección de la vida privada y de los datos personales

65. El derecho al respeto a la vida privada y familiar está consagrado en el Artículo 8 del CEDH. La jurisprudencia del Tribunal aporta un marco de interpretación de este derecho, completado y reforzado por el Convenio 108 del Consejo de Europa.

66. La noción de vida privada no se presta a una definición exhaustiva. El Tribunal ha subrayado que el Artículo 8 abarca una gran variedad de intereses, a saber, la vida privada y familiar, el domicilio y la correspondencia, que incluye el correo, las comunicaciones telefónicas⁵⁴ y los correos electrónicos en el lugar de trabajo. El derecho al respeto a la vida privada está relacionado con el derecho de la persona a su imagen⁵⁵, por ejemplo, a través de fotografías y videoclips. También tiene que ver con la identidad de la persona y el desarrollo personal, y el derecho a establecer y mantener relaciones con otros seres humanos. Quedan igualmente cubiertas las actividades de índole profesional o comercial.⁵⁶

67. Muchas de las actividades de los usuarios implican algún tipo de tratamiento automático de los datos personales, por ejemplo, el uso de navegadores, buzones de correo electrónico, mensajes instantáneos, protocolos de transmisión de voz por Internet, redes sociales, motores de búsqueda y servicios de almacenamiento de datos en la nube. El Convenio 108 cubre todas las operaciones efectuadas en Internet, como la recogida, el almacenamiento, la alteración, la eliminación y la recuperación o la difusión de datos personales.⁵⁷

68. Existen principios y normas que deberían seguir las autoridades públicas y empresas privadas que participen en el tratamiento de datos personales. Es necesario que los usuarios sepan y comprendan qué datos son objeto de tratamiento y de qué manera, y si pueden hacer algo a este respecto, por ejemplo, solicitar la corrección o la eliminación de datos. De acuerdo con el Convenio 108, los datos de carácter personal se deben obtener y tratar de manera leal y legítima, y se deben registrar para finalidades determinadas y legítimas. Asimismo, deben ser adecuados, pertinentes y no excesivos en relación con las finalidades para las cuales se hayan registrado; deben ser exactos y, si fuera necesario, puestos al día; y se deben conservar en una forma que permita la identificación de las personas interesadas durante un período de tiempo que no exceda del necesario para las finalidades para las cuales se hayan registrado.⁵⁸

69. Se hace énfasis en dos principios específicos del tratamiento de los datos personales: la legitimidad del tratamiento y el consentimiento del usuario. El usuario debe ser informado de que los datos solo podrán tratarse cuando la ley así lo disponga y cuando haya dado su consentimiento para ello, por ejemplo, al aceptar las condiciones de uso de un servicio de Internet.

70. La cuestión del consentimiento libre, específico, informado y explícito (inequívoco) de una persona con respecto al tratamiento de sus datos en Internet, está en discusión actualmente con miras a integrarla en el Convenio 108.⁵⁹ También se hace referencia al consentimiento informado en la Recomendación CM/Rec(2012)4 del Consejo de Ministros a los Estados miembros sobre la protección de los derechos humanos con respecto a los servicios de redes sociales. En particular, las

⁵⁴ Klass y otros c. Alemania, n.º 5029/71, §41.

⁵⁵ Von Hannover c. Alemania (n.º 2), n.º 40660/08 y 60641/08 §§ 108-113. Sciacca c. Italia, n.º 50774/99, § 29.

⁵⁶ Rotaru c. Rumanía (n.º 28341/95); P.G. y J.H. c. Reino Unido (n.º 44787/98); Peck c. Reino Unido (n.º 44647/98); Perry c. Reino Unido (n.º 63737/00); Amann c. Suiza (n.º 27798/95).

⁵⁷ Véase el Convenio 108, Artículo 2.

⁵⁸ Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE n.º 108).

⁵⁹ El Comité Consultivo del Convenio para la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal (STE n.º 108) ha presentado una serie de propuestas para modernizar este convenio (T-PD(2012)4Rev3_en). Una de estas propuestas se centra en el consentimiento de la persona como condición previa al tratamiento de los datos personales: "Cada Parte velará por que el tratamiento de los datos solo pueda efectuarse sobre la base del consentimiento libre, específico, informado y [explícito, inequívoco] o de algún fundamento legítimo establecido por la ley".

redes sociales deberían contar con el consentimiento informado de sus usuarios antes de que los datos personales de estos sean difundidos o compartidos con otras categorías de personas o empresas, o utilizados en modos distintos de los necesarios para las finalidades para las que se hayan recogido inicialmente. A fin de garantizar el consentimiento real de los usuarios, estos deberían tener la posibilidad de decidir si aceptan un acceso más amplio a sus datos personales por terceros (p. ej.: cuando en la red social se utilicen aplicaciones de terceros). Del mismo modo, los usuarios deberían poder retirar su consentimiento.

71. Es importante destacar la Recomendación CM/Rec(2010)13 del Consejo de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles. Esta hace referencia a la "creación de perfiles", entendida como una técnica de tratamiento automatizado de datos que consiste en aplicar un "perfil" a una persona física, en particular con el fin de tomar decisiones sobre la misma o de analizar o prever sus preferencias, comportamientos y actitudes personales. En concreto, los datos personales de un usuario de Internet pueden ser recogidos y tratados en el contexto de su interacción con un sitio web o una aplicación, o en el contexto de su actividad de navegación sobre un período de tiempo o entre diferentes sitios web (p. ej.: recogida de información sobre páginas y contenidos consultados, hora de las visitas, tipo de búsquedas, clics efectuados). Uno de los medios empleados para rastrear las actividades de navegación de los usuarios son las *cookies*, que almacenan información en el equipo del usuario para recuperarla posteriormente. La Recomendación contempla el derecho de los usuarios de Internet a otorgar su consentimiento para el uso de datos personales con miras a la creación de perfiles y el derecho a retirar dicho consentimiento.⁶⁰

72. Diferentes instrumentos del Consejo de Europa mencionan los derechos de los usuarios de Internet en lo que se refiere a la información sobre el tratamiento de sus datos personales. El Convenio 108 dispone que el usuario interesado debería poder conocer la existencia de un fichero automatizado de datos de carácter personal a cargo de cualquier persona física o jurídica, sus finalidades principales, así como la identidad y la residencia habitual o el establecimiento principal de la autoridad controladora del fichero. Asimismo, debería poder obtener a intervalos razonables y sin demora o gastos excesivos la confirmación de la existencia o no en el fichero automatizado de sus datos de carácter personal, así como la comunicación de dichos datos en forma inteligible.⁶¹

73. También se hace referencia a la información destinada a los usuarios en la Recomendación CM/Rec(2012)4 del Consejo de Ministros a los Estados miembros sobre la protección de los derechos humanos con respecto a los servicios de redes sociales. Los usuarios de redes sociales deberían recibir información clara y comprensible sobre cualquier cambio a las condiciones de servicio y de uso del proveedor. Esto incluye también otros aspectos, como la instalación de aplicaciones de terceros que supongan un riesgo para la privacidad de los usuarios; la legislación aplicable a los servicios de la red social y al tratamiento relacionado de los datos personales; las consecuencias del acceso abierto (en términos de tiempo y territorio) a los perfiles y comunicaciones, explicando en particular las diferencias entre comunicaciones públicas y privadas, y las consecuencias de poner la información a disposición del público, incluido el acceso no restringido y la recogida de los datos por terceros; y la necesidad de obtener el consentimiento previo de otras personas antes de publicar los datos personales de estas, incluidos contenidos de audio y vídeo, en los casos en los que hayan ampliado el acceso más allá de los contactos personalmente seleccionados. Además, los usuarios de Internet deberían recibir información específica sobre la lógica subyacente al tratamiento de los datos personales que se aplica para asignarles un perfil, así como sobre las finalidades de la creación de perfiles.

74. Los usuarios de Internet deberían poder ejercer el control sobre sus datos personales, como se indica en el Convenio 108, y, en particular, el derecho a obtener la rectificación o la eliminación de los datos que hayan sido tratados contrariamente a la ley, así como el derecho a interponer un recurso en caso de incumplimiento de una solicitud de confirmación o, en su caso, de comunicación, rectificación o eliminación, según lo anteriormente mencionado.⁶²

⁶⁰ Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, sección 5.

⁶¹ Convenio 108, Artículo 8.

⁶² Véase la nota 60 anterior, Artículo 8.

75. La Recomendación CM/Rec(2012)3 del Consejo de Ministros a los Estados miembros sobre la protección de los derechos humanos con respecto a los motores de búsqueda hace referencia a una serie de medidas que pueden tomar los proveedores con el objetivo de proteger la privacidad de sus usuarios. Esto incluye la protección de los datos personales contra el acceso ilícito por terceros y esquemas de notificación en los casos de violaciones relativas a los datos. Entre las medidas debería incluirse también el cifrado “de punta a punta” de las comunicaciones entre el usuario y el proveedor del motor de búsqueda. La correlación cruzada de datos obtenidos desde diferentes servicios o plataformas del proveedor de un motor de búsqueda únicamente debe realizarse si el usuario ha dado su consentimiento inequívoco para ese servicio específico. Los usuarios deberían poder consultar, corregir y eliminar los datos recogidos durante el uso de tales servicios, así como cualquier perfil creado, por ejemplo con fines de marketing directo.⁶³

76. Las redes sociales deberían prestar asistencia a los usuarios en la gestión y protección de sus datos, en particular a través de:

- *configuraciones por defecto que protejan la privacidad*, a fin de limitar el acceso a los datos a aquellos contactos que hayan sido identificados y seleccionados por el usuario. Esto incluye ajustes a las configuraciones de privacidad y a la selección del nivel de acceso público a los datos;
- *una protección avanzada para los datos sensibles*, como el acceso a los datos biométricos o al reconocimiento facial, que no debería activarse por defecto;
- *la seguridad de los datos personales contra todo acceso ilícito* por terceros, incluido el cifrado de punta a punta de las comunicaciones entre el usuario y las redes sociales. Los usuarios deberían ser informados acerca de las violaciones que afecten a la seguridad de sus datos personales a fin de poder tomar medidas preventivas como cambiar sus contraseñas y ser vigilantes con sus transacciones financieras (por ejemplo, cuando las redes sociales posean datos bancarios o datos de la tarjeta de crédito).
- *la protección de la privacidad desde el diseño*, lo cual significa tomar en cuenta las necesidades de protección de los datos en la etapa de concepción de los servicios o productos, y evaluar continuamente el impacto sobre la privacidad que puedan tener los cambios a los servicios existentes;
- *la protección a favor de quienes no utilicen las redes sociales*, absteniéndose de recoger y tratar sus datos personales, por ejemplo, direcciones de correo electrónico y datos biométricos. Los usuarios deberían tener conocimiento de sus obligaciones con respecto a otras personas y, en particular, del hecho de que la publicación de datos personales relacionados con otros individuos debería respetar los derechos de estos.⁶⁴

77. Antes del cierre de la cuenta de un usuario en una red social, este debería poder transferir sus datos a otro servicio o dispositivo, de manera libre y sencilla, en un formato que pueda utilizar. Después del cierre, todos los datos obtenidos del usuario y relacionados con este deberían suprimirse de modo permanente de los medios de almacenamiento del servicio de la red social. Además, los usuarios de Internet deberían poder tomar decisiones informadas sobre su identidad en línea, incluido el uso de un seudónimo. En el caso de que un servicio de red social requiera el registro de la identidad real, la publicación de esta identidad en Internet debería ser opcional para los usuarios. Esto no impide que las autoridades encargadas del cumplimiento de la ley puedan tener acceso a la identidad real de un usuario cuando ello resulte necesario, teniendo en cuenta las garantías jurídicas pertinentes relativas al respeto de los derechos y las libertades fundamentales.

78. El usuario debería poder oponerse al uso de sus datos personales para los fines de creación de perfiles y a toda decisión tomada únicamente sobre la base de la creación de perfiles que repercuta en efectos jurídicos para él o que lo afecte significativamente, salvo que la ley así lo prevea con medidas para salvaguardar los intereses legítimos del usuario, en particular permitiéndole

⁶³ Véase la Recomendación CM/Rec(2012)3, en particular el Anexo, parte II.

⁶⁴ *Ibid.*

expresar su punto de vista, y a menos que la decisión se haya tomado durante la ejecución de un contrato y estén en aplicación las medidas de salvaguardia de los intereses legítimos del usuario.⁶⁵

79. Los derechos de los usuarios de Internet no son absolutos; de ahí la expresión “de manera general” en el apartado 3. Puede haber excepciones a estos derechos cuando así lo prevea la legislación y cuando resulte necesario en una sociedad democrática para los fines de: (a) proteger la seguridad del Estado, la seguridad pública, los intereses monetarios del Estado, o reprimir los delitos; y (b) proteger a las personas interesadas o velar por los derechos y las libertades de los demás. La legislación puede prever restricciones al ejercicio de los derechos con respecto a los archivos automatizados de datos personales que se utilicen con fines estadísticos o de investigación científica cuando no exista ningún riesgo manifiesto de violación de la privacidad de la persona interesada.⁶⁶

80. La interceptación está relacionada con la escucha, la vigilancia o el control del contenido de las comunicaciones con miras a la obtención del contenido de los datos, bien mediante el acceso y uso del sistema informático, o bien, indirectamente, mediante el uso de dispositivos de intervención y escucha. La interceptación puede abarcar también la grabación de comunicaciones.⁶⁷ El derecho al respeto de la confidencialidad de la correspondencia y las comunicaciones está consagrado en el Artículo 8 del CEDH, según su interpretación por el Tribunal. El concepto de correspondencia incluye el correo electrónico y las telecomunicaciones⁶⁸, así como los correos electrónicos enviados en un contexto laboral⁶⁹. Se espera que la interpretación de este concepto evolucione al ritmo de los desarrollos tecnológicos, que pueden traer nuevas formas de comunicaciones en Internet, como los mensajes de correo electrónico (en un contexto más amplio), los mensajes instantáneos u otros dentro del ámbito de la protección prevista por el Artículo 8.

81. Abajo se presentan algunos de los principios generales afirmados por la jurisprudencia del Tribunal con respecto a la interceptación y vigilancia de las comunicaciones en casos no relacionados con Internet y casos relativos a injerencias por autoridades del Estado. Estos principios brindan un marco de orientación y referencia general que podría aplicarse en el futuro a las comunicaciones en Internet.

82. La interceptación de la correspondencia y las telecomunicaciones constituye una injerencia con respecto al derecho al respeto a la vida privada, y está sujeta a las condiciones establecidas en el Artículo 8, apartado 2, del CEDH. La existencia misma de normas que permitan la vigilancia de las telecomunicaciones puede considerarse como una injerencia en el derecho al respeto a la vida privada. Una norma que instituya un sistema de vigilancia mediante el cual puedan llegar a vigilarse los correos y telecomunicaciones de todas las personas de un país afecta directamente a todos los usuarios o usuarios potenciales de los servicios postales y de telecomunicaciones de dicho país. Por lo tanto, el Tribunal ha aceptado que, en ciertas circunstancias, una persona puede alegar ser víctima de una violación ocasionada por la sola existencia de medidas secretas o de normas que permitan, sin tener que alegar que tales medidas hayan sido efectivamente aplicadas en su caso particular.⁷⁰

83. La interceptación debe estar prevista por la ley y ser necesaria en una sociedad democrática para la seguridad nacional, la seguridad pública o el bienestar económico del país, la defensa del orden y la prevención del delito, la protección de la salud o de la moral, o la protección de los derechos y las libertades de los demás, a tenor de lo dispuesto en el Artículo 8 del CEDH. El Tribunal ha desarrollado los siguientes principios generales, en especial en referencia a las exigencias que deben cumplir las normas que prevean medidas encubiertas de vigilancia de la correspondencia y las comunicaciones por las autoridades públicas.

⁶⁵ Recomendación CM/Rec(2010)13 del Comité de Ministros a los Estados miembros sobre la protección de las personas con respecto al tratamiento automatizado de datos de carácter personal en el contexto de la creación de perfiles, sección 5.

⁶⁶ Convenio 108, Artículo 9.

⁶⁷ Véase el Informe explicativo del Convenio de Budapest, apartado 53.

⁶⁸ Asociación para la Integración Europea y los Derechos Humanos y Ekmidzhiev c. Bulgaria n.º 62540/00 § 58; Klass y otros c. Alemania n.º 5029/71, Malone c. Reino Unido, n.º 8691/79 y Weber y Saravia c. Alemania, n.º 54934/00.

⁶⁹ Véase Copland c. Reino Unido, n.º 62617/00.

⁷⁰ Klass y otros, n.º 5029/71 §§ 30-38; Malone c. Reino Unido n.º 8691/79§ 64; y Weber y Saravia c. Alemania n.º 54934/00, §§ 78 y 79, Asociación para la Integración Europea y los Derechos Humanos y Ekmidzhiev c. Bulgaria n.º 62540/00 § 58, § 69-70.

- *Previsibilidad* – la legislación debe ser accesible para la persona interesada, quien debe poder prever las consecuencias de la aplicación de la misma en su caso particular. La legislación debe ser formulada con suficiente claridad y precisión para dar a los ciudadanos una indicación adecuada de las condiciones y circunstancias en las que las autoridades estarán habilitadas a recurrir a esta injerencia secreta y potencialmente peligrosa con respecto al derecho al respeto a la vida privada y a la privacidad de la correspondencia.⁷¹
- *Garantías mínimas para el ejercicio del poder discrecional por las autoridades públicas* – la legislación debe tener reglas detalladas con respecto a (i) la naturaleza de las infracciones que pueden dar lugar a una orden de interceptación; (ii) la definición de las categorías de personas cuyas comunicaciones pueden ser objeto de vigilancia; (iii) la duración límite de la vigilancia; (iv) el procedimiento que deberá seguirse para examinar, utilizar y almacenar los datos obtenidos; y (v) las precauciones que deberán tomarse cuando se comuniquen los datos a terceros; así como las circunstancias en las cuales pueden o deben eliminarse los datos obtenidos o destruirse los registros existentes.⁷²
- *Supervisión y examen por las autoridades competentes* – el Tribunal exige la existencia de garantías adecuadas y efectivas contra los abusos.⁷³

84. La jurisprudencia del Tribunal en relación con la privacidad en el lugar de trabajo ha determinado que las nociones de vida privada y correspondencia son aplicables a las llamadas telefónicas efectuadas por un empleado dentro de las instalaciones de su empresa. Los correos electrónicos enviados desde el lugar de trabajo, así como la información obtenida a través de la vigilancia del uso personal de Internet, deberían estar protegidos en virtud del Artículo 8 del CEDH. A falta de una advertencia sobre la posibilidad de vigilancia, el empleado puede tener una expectativa razonable de que se respete su privacidad en las llamadas telefónicas, los correos electrónicos y el uso de Internet en el sitio de trabajo.⁷⁴ El usuario puede recibir ayuda de las autoridades de protección de datos o de otras autoridades competentes en los Estados miembros.

85. Las autoridades de protección de datos, presentes en la mayoría de los Estados miembros, desempeñan un papel importante en las actividades de investigación, intervención, sensibilización o recurso en los casos de injerencia en el tratamiento de datos personales. Esto no obsta al papel primordial del Estado en lo que atañe a garantizar la protección de los datos personales dentro del marco general de su obligación de velar por el derecho al respeto a la vida privada y familiar.

Educación y conocimientos básicos

86. El derecho a la educación está consagrado en el Artículo 2 del Protocolo 1 al CEDH. La Recomendación CM/Rec(2007)16 del Consejo de Ministros a los Estados miembros sobre medidas para promover el valor de servicio público de Internet fomenta la creación, el tratamiento y el acceso a contenidos educativos, culturales y científicos en formato digital, a fin de velar por que todas las culturas puedan expresarse y tener acceso a Internet en todos los idiomas, incluidos los propios.⁷⁵ Los usuarios de Internet deberían poder acceder libremente a las obras culturales y de investigación presentes en Internet que hayan sido financiadas con fondos públicos,⁷⁶ así como —dentro de los límites razonables— a los materiales del patrimonio digital que sean de dominio público. En casos específicos, puede haber condiciones para el acceso al conocimiento a fin de remunerar por su trabajo a los titulares de derechos, dentro de los límites de las excepciones permisibles a la protección de la propiedad intelectual.

⁷¹ Malone c. Reino Unido, n.º 8691/79 § 67; Valenzuela Contreras c. España, sentencia del 30 de julio de 1998, Informes 1998-V, p. 1925, § 46 (iii); y Khan c. Reino Unido, n.º 35394/97, § 26, Asociación para la Integración Europea y los Derechos Humanos y Ekmidzhiev c. Bulgaria, n.º 62540/00, § 71.

⁷² Véase Kruslin c. Francia, n.º 11801/85 § 33; Huvig c. Francia, n.º 11105/84 § 32; Amann c. Suiza, n.º 27798/95 § 56; Weber y Saravia c. Alemania, n.º 54934/00 § 93; Asociación para la Integración Europea y los Derechos Humanos y Ekmidzhiev c. Bulgaria, n.º 62540/00 § 76.

⁷³ *Ibíd.*, n.º 62540/00 § 77.

⁷⁴ Copland c. Reino Unido, n.º 62617/00, § 41, 42.

⁷⁵ Véase también la nota 8 anterior, CM/Rec(2007)16 Sección IV.

⁷⁶ *Ibíd.*

87. Los usuarios de Internet deberían poder adquirir la información, la educación, el conocimiento y las competencias de base para ejercer sus derechos humanos y sus libertades fundamentales en Internet. Esto concuerda con las normas del Consejo de Ministros del Consejo de Europa que promueven los conocimientos básicos en informática como condición previa fundamental para el acceso a la información y el ejercicio de los derechos culturales y el derecho a la educación a través de las TIC.⁷⁷

88. Los programas e iniciativas sobre conocimientos básicos de Internet brindan a los usuarios la capacidad para analizar de manera crítica la exactitud y fiabilidad de los contenidos de Internet. El Consejo de Ministros ha recomendado a los Estados miembros del Consejo de Europa facilitar el acceso a los dispositivos de las TIC y promover una educación que permita a todas las personas, en particular los niños, adquirir las competencias necesarias para trabajar con una amplia gama de TIC y evaluar de modo crítico la calidad de la información, sobre todo aquella que podría causarles algún perjuicio.⁷⁸

Niños y jóvenes

89. Los niños y los jóvenes tienen derecho a expresar sus puntos de vista y a participar en la sociedad y en las decisiones que los afecten, a través de Internet y de otras TIC. Esto se basa en las normas del Consejo de Ministros que establecen que todos los niños y jóvenes menores de 18 años deberían disfrutar del derecho, los medios, el espacio, la posibilidad y, cuando sea necesario, el apoyo para expresar libremente sus opiniones, para ser escuchados y para contribuir a la toma de decisiones sobre temas que los afecten, dándose el debido peso a sus opiniones en función de su edad y su nivel de madurez y comprensión. El derecho de los niños y los jóvenes a participar se aplica plenamente a los entornos de Internet, sin discriminación por razones de raza, etnia, color, sexo, idioma, religión, opiniones políticas o de otra índole, origen nacional o social, propiedad, discapacidad, nacimiento, orientación sexual u otros factores.⁷⁹

90. Los niños y los jóvenes deberían recibir, incluso a través de las redes sociales y otros medios, información apropiada para su edad y circunstancias sobre las oportunidades para ejercer sus derechos. Se les debería informar plenamente acerca del alcance de su participación —lo cual incluye los límites, los resultados esperados y los resultados reales de dicha participación— y de la manera en que se tomaron en consideración sus puntos de vista.⁸⁰ Cuando consideren que se ha violado su derecho a participar, se les deberían brindar medios de recurso y reparación efectivos, por ejemplo, medios para la presentación de quejas que sean adaptados para su edad, y procedimientos administrativos y judiciales, junto con el apoyo y la asistencia para utilizarlos.⁸¹

91. Los niños y los jóvenes deberían poder usar Internet de una manera segura, con el debido respeto a su vida privada. Deberían recibir formación e información de parte de sus maestros, sus educadores y sus padres. Los conocimientos básicos de los niños y los jóvenes en materia de información significan el uso competente de las herramientas que permiten el acceso a la información, el desarrollo del análisis crítico del contenido y la apropiación de las habilidades de comunicación para fomentar la ciudadanía y la creatividad, así como iniciativas de formación para los niños y sus educadores, que les permitan usar las TIC e Internet de una manera positiva y responsable.⁸²

92. El derecho al respeto a la vida privada de los niños ha sido objeto de examen en casos presentados ante el Tribunal. El bienestar físico y moral de los niños es un componente esencial de su derecho a la vida privada. Los Estados miembros tienen obligaciones positivas en lo que se refiere

⁷⁷ Declaración del Comité de Ministros sobre los derechos humanos y el Estado de derecho en la sociedad de la información, CM(2005)56 final, del 13 de mayo de 2005.

⁷⁸ *Ibid.*

⁷⁹ Recomendación CM/Rec(2012)2 del Comité de Ministros a los Estados miembros sobre la participación de niños y jóvenes menores de 18 años.

⁸⁰ *Ibid.*

⁸¹ Véase la Recomendación CM Rec(2011)12 del Comité de Ministros a los Estados miembros sobre los derechos de los niños y servicios sociales adaptados y accesibles para los niños y sus familias, Directrices del Consejo de Europa sobre una justicia favorable a los niños.

⁸² Recomendación Rec(2006)12 del Comité de Ministros sobre capacitar a los niños en el nuevo entorno de la información y de la comunicación.

a garantizar el respeto efectivo de este derecho.⁸³ El Tribunal estima que la disuasión efectiva contra actos graves que amenacen valores fundamentales y aspectos esenciales de la vida privada exige disposiciones e investigaciones penales efectivas.⁸⁴

93. Es importante comprender que los contenidos que crean los niños y los jóvenes en Internet o por este medio, así como los contenidos que crean otras personas en relación con ellos (p. ej.: fotos, vídeos, texto u otros) o los rastros de dichos contenidos (registros, archivos y tratamiento) pueden perdurar o ser accesibles de modo permanente. Esto puede poner en entredicho su dignidad, seguridad y privacidad, o hacerlos de otro modo vulnerables ahora o en una etapa futura de sus vidas. Los niños y los jóvenes, al igual que sus padres, tutores, profesores y otras personas encargadas, deberían estar capacitados para comprender y afrontar esta realidad, y para velar por su vida privada en línea. Para este fin, es importante que se ofrezca asesoramiento práctico sobre la manera de borrar la información personal. El Consejo de Ministros del Consejo de Europa ha brindado orientación a los Estados miembros al afirmar que, salvo en el marco del cumplimiento de la ley, los contenidos creados por los niños en Internet que atenten contra su dignidad, seguridad y vida privada, o que los hagan de otro modo vulnerables ahora o en una etapa futura de sus vidas, no deberían ser accesibles de forma duradera o permanente.⁸⁵ Por lo tanto, los Estados miembros fueron invitados a explorar, junto con otros actores pertinentes, cuando corresponda, la viabilidad de retirar o eliminar tales contenidos, incluida toda huella de los mismos (registros, archivos y tratamiento) dentro de un plazo razonablemente breve.⁸⁶ No obstante, el apartado 3 no se aplica al contenido relacionado con niños o jóvenes que sea creado por la prensa o por editores. La primera frase de esta disposición de la Guía aclara que las situaciones contempladas son aquellas en las que se trata o bien de contenidos creados por los niños o los jóvenes, o bien de contenidos relacionados con ellos y creados por otros usuarios de Internet.

94. En lo referente al contenido y el comportamiento perjudiciales en línea, los niños tienen derecho a asistencia y cuidado especial, en función de su edad y circunstancias, en particular en lo que atañe al riesgo que suponen la pornografía, la representación degradante y estereotipada de la mujer, la representación y la glorificación de la violencia y el daño autoinfligido —en especial el suicidio—, las expresiones humillantes, discriminatorias o racistas o la apología de tales conductas, las solicitudes con fines de abuso sexual, el reclutamiento de niños víctimas de trata de seres humanos, la intimidación y las diferentes formas de acoso, que pueden afectar negativamente el bienestar físico, emocional y psicológico de los niños.⁸⁷ Así, los niños y los jóvenes deberían ser informados, de una manera adaptada a su edad y a otras circunstancias particulares, acerca de los tipos de contenidos y comportamientos que son ilegales.

95. Los niños y los jóvenes también deberían poder denunciar los contenidos y comportamientos potencialmente perjudiciales, y recibir asesoramiento y apoyo, con la debida atención a su confidencialidad y a su anonimato. Esto es particularmente relevante en el contexto de las redes sociales. El Consejo de Ministros ha recomendado a los Estados miembros tomar medidas en la materia⁸⁸, en especial para proteger a los niños y los jóvenes del contenido perjudicial, a saber:

- brindar información clara sobre los tipos de contenido, intercambios de contenido o conductas que pueden ir en contra de las disposiciones legales aplicables;
- desarrollar políticas editoriales de modo que los contenidos o comportamientos pertinentes puedan definirse como “inadecuados” en las condiciones de uso del servicio de red social, al mismo tiempo que se garantiza que este enfoque no restrinja el derecho a la libertad de expresión y a la información;

⁸³ K.U. c. Finlandia - 2872/02 § 40, 41.

⁸⁴ X e Y c. Países Bajos, §§ 23-24 y 27; August c. Reino Unido n.º 36505/02; y M.C. c. Bulgaria, n.º 39272/98, § 150. K.U. c. Finlandia, n.º 2872/02 § 46.

⁸⁵ Declaración del Comité de Ministros sobre la protección de la dignidad, la seguridad y la privacidad de los niños en internet.

⁸⁶ *Ibid.*

⁸⁷ Recomendación CM/Rec(2009)5 del Comité de Ministros a los Estados miembros sobre las medidas para proteger a los niños contra el contenido y comportamiento perjudiciales y para promover su participación activa en el nuevo entorno de la información y las comunicaciones.

⁸⁸ Véase CM/Rec(2012)4, Anexo, II, §10.

- establecer mecanismos de fácil acceso para denunciar los contenidos o comportamientos inadecuados o aparentemente ilícitos en las redes sociales;
- brindar respuesta, con la debida diligencia, a las quejas por acoso y manipulación de menores a través de Internet.⁸⁹

96. Los niños y los jóvenes deberían ser informados acerca de los riesgos para su bienestar físico y moral en los entornos en línea, como pueden ser el abuso y la explotación sexual, que demandan una protección especial. A esto se hace referencia en el Convenio de Lanzarote del Consejo de Europa y en la jurisprudencia del Tribunal, que reconoce que los Estados tienen obligaciones positivas en lo que respecta a garantizar la protección de los niños en Internet.⁹⁰

97. En virtud del Convenio de Lanzarote, debería protegerse a los niños de manera que no sean reclutados, incitados u obligados a participar en espectáculos pornográficos accesibles o disponibles a través de Internet (p. ej.: mediante cámaras web, salas de chat o juegos en línea).⁹¹ Asimismo, se les debe proteger de toda solicitud realizada mediante el uso de Internet o de otras TIC que tenga como finalidad hacerlos participar en actividades sexuales con un menor que, de acuerdo con las disposiciones pertinentes del derecho nacional, no haya alcanzado la edad legal para actividades sexuales, o hacerlos participar en la producción de pornografía infantil.⁹²

98. Debería fomentarse la participación de los niños en la elaboración y aplicación de políticas, programas u otras iniciativas estatales en relación con la lucha contra la explotación sexual y el abuso sexual de menores en los entornos de Internet.⁹³ Deberían brindarse a los niños medios accesibles y adaptados a su edad para denunciar los presuntos casos de abuso o explotación sexual en Internet y para presentar quejas a través de los servicios de información, tales como líneas de asistencia telefónica o por Internet. Asimismo, se les debería brindar asesoramiento y apoyo en el uso de estos servicios, con el debido respeto a su confidencialidad y anonimato.⁹⁴

Recursos efectivos

99. El derecho a un recurso efectivo está consagrado en el Artículo 13 del CEDH. Toda persona cuyos derechos y libertades hayan sido restringidos o violados en Internet tiene derecho a un recurso efectivo.

100. El Artículo 13 del CEDH garantiza la existencia, a nivel nacional, de un recurso por el que se pueda obtener el cumplimiento sustancial de los derechos y las libertades reconocidos en el Convenio, como quiera que estén consagrados en el ordenamiento jurídico interno. Exige la concesión de un recurso interno que permita tratar la parte sustantiva de una demanda en virtud del CEDH y aportar una reparación adecuada.⁹⁵ Los Estados tienen la obligación positiva de investigar de manera diligente, exhaustiva y eficaz las alegaciones por violación de los derechos humanos. Los procedimientos seguidos deberán permitir al órgano competente pronunciarse sobre el fondo de la demanda de violación del Convenio y sancionar toda violación efectiva, pero también garantizar la ejecución de las decisiones adoptadas.⁹⁶

101. Debería haber una autoridad nacional encargada de pronunciarse sobre las supuestas violaciones de los derechos consagrados en el CEDH.⁹⁷ Debe haber una vía jurídica específica mediante la cual las personas puedan presentar sus quejas cuando el plazo de los procedimientos

⁸⁹ Ibid.

⁹⁰ K.U. c. Finlandia n.º 2872/02.

⁹¹ Convenio del Consejo de Europa para la protección de los niños contra la explotación y el abuso sexual, STCE n.º: 201, Artículo 2, Artículo 21; véase también el Informe explicativo sobre estos artículos.

⁹² Ibid. Artículo 23.

⁹³ Ibid. Artículo 9/1.

⁹⁴ Ibid. Artículo 13. Véase también la Recomendación CM/Rec(2011)12 del Comité de Ministros a los Estados miembros sobre los derechos de los niños y servicios sociales adaptados y accesibles para los niños y sus familias, Directrices del Consejo de Europa sobre una justicia favorable a los niños.

⁹⁵ Kaya c. Turquía, n.º 22729/93, §106.

⁹⁶ Smith y Grady c. Reino Unido, n.º 33985/96 33986/96.

⁹⁷ Silver y otros c. Reino Unido, n.º 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 §113; Kaya c. Turquía, n.º 22729/93, §106.

para determinar sus derechos sea más largo de lo razonable.⁹⁸ La autoridad no necesariamente tendrá que ser judicial si presenta garantías de independencia e imparcialidad. No obstante, sus poderes y las garantías procesales ofrecidas deberían permitir determinar si el recurso pertinente es efectivo.⁹⁹

102. El procedimiento adoptado por la autoridad nacional competente debería permitir la investigación efectiva de toda violación. Asimismo, debería permitir a tal autoridad pronunciarse sobre el fondo de la demanda por violación de los derechos consagrados en el CEDH,¹⁰⁰ sancionar toda violación y garantizar a la víctima la ejecución de la decisión tomada.¹⁰¹ La efectividad del recurso deberá ser de hecho y de derecho, y no podrá depender de la certeza de un resultado favorable para el demandante.¹⁰² Los requisitos del Artículo 13 se pueden cumplir mediante un conjunto de recursos previstos en la legislación, pese a que cada uno de estos recursos no satisfaga por sí solo dichos requisitos.¹⁰³

103. Las vías de recurso efectivo deberían estar disponibles, ser conocidas, accesibles y asequibles, y ser aptas para brindar una reparación adecuada. El recurso efectivo se puede obtener directamente de los proveedores de servicios de Internet (aunque estos pueden no tener la suficiente independencia para cumplir con el Artículo 13 del CEDH), de las autoridades públicas o de otras instituciones nacionales de derechos humanos. Los medios de reparación pueden ser: una investigación, una explicación por parte del proveedor del servicio o el proveedor en línea, la posibilidad de contestar a una declaración que se considere —por ejemplo— difamatoria u ofensiva, el restablecimiento de contenido creado por el usuario que haya sido retirado por un proveedor de servicio en línea, o la reconexión a Internet cuando el usuario haya sido desconectado, y la compensación correspondiente.

104. Como parte de sus obligaciones positivas en lo que se refiere a proteger a las personas contra las violaciones de los derechos humanos por empresas privadas, los Estados deberían tomar medidas adecuadas a fin de garantizar que, en los casos en que ocurran dichas violaciones, las personas afectadas tengan acceso a mecanismos judiciales y extrajudiciales.¹⁰⁴ Los Principios Rectores sobre las empresas y los derechos humanos de las Naciones Unidas especifican que las empresas deberían establecer mecanismos de reclamación que sean accesibles, predecibles (disponer de un procedimiento claro y conocido, con un calendario indicativo de cada etapa, y aclarar los posibles procesos y resultados disponibles, así como los medios para supervisar la implementación), equitativos (acceso a las fuentes de información, asesoramiento y conocimientos especializados), transparentes y capaces de ofrecer a las personas reparaciones que sean plenamente conformes a los derechos humanos internacionalmente reconocidos.¹⁰⁵

105. Debería brindarse a los usuarios de Internet información clara y transparente sobre los medios de reparación con los que pueden contar. Esta información podría incluirse en las condiciones de uso o servicio o en otras pautas y políticas de los proveedores en línea o proveedores de servicios de Internet. Deberían brindarse a los usuarios de Internet herramientas prácticas y accesibles para comunicar sus inquietudes a los proveedores en línea o proveedores de servicios de Internet. Los usuarios deberían poder solicitar información y buscar reparación. Algunos ejemplos de recursos para los usuarios de Internet son las líneas de asistencia telefónica o líneas directas administradas por los proveedores de servicios de Internet o por asociaciones de protección del consumidor a las que pueden llamar en caso de violación de sus derechos o de los derechos de otras personas. Debería haber posibilidades de orientación de parte de las autoridades públicas y de las instituciones

⁹⁸ Kudla c. Polonia, n.º 30210/96, §157.

⁹⁹ Silver y otros c. Reino Unido, n.º 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 §113; Kaya c. Turquía, n.º 22729/93, §106.

¹⁰⁰ Smith y Grady c. Reino Unido, n.º 33985/96 33986/96, § 138.

¹⁰¹ Iatridis c. Grecia, n.º 31107/96, § 60.

¹⁰² Kudla c. Polonia, n.º 30210/96, §158.

¹⁰³ Silver y otros c. Reino Unido, n.º 5947/72; 6205/73; 7052/75; 7061/75; 7107/75; 7113/75; 7136/75 §113; Kudla c. Polonia, n.º 30210/96 §157.

¹⁰⁴ Las cuestiones de la responsabilidad social corporativa y de las obligaciones positivas de los Estados en cuanto a proteger los derechos humanos se explican en los apartados 19 y 28 de la Exposición de motivos.

¹⁰⁵ Véanse los Principios Rectores sobre las empresas y los derechos humanos: puesta en práctica del marco de las Naciones Unidas para “proteger, respetar y remediar” (A/HRC/17/31) aprobados por el Consejo de Derechos Humanos mediante la Resolución Los derechos humanos y las empresas transnacionales y otras empresas A/HRC/RES/17/4, capítulo III, principios 28-31.

nacionales de derechos humanos (mediadores), autoridades de protección de datos, órganos de reglamentación de las comunicaciones electrónicas, oficinas de asesoramiento a los ciudadanos, asociaciones de derechos humanos o derechos digitales, u organizaciones de consumidores.

106. Se debería proteger a los usuarios de Internet contra la ciberdelincuencia. Los Estados parte en el Convenio de Budapest han adquirido obligaciones por las cuales les corresponde proteger a los ciudadanos contra actividades ilícitas o delitos en Internet. Los usuarios de Internet tienen una expectativa razonable de protección contra las actividades ilícitas o los delitos cometidos en Internet o por ese medio.

107. Se hace énfasis en los delitos que atentan contra la confidencialidad y la integridad de los sistemas y datos informáticos y en los delitos cometidos mediante sistemas informáticos. No se cubren aquí los delitos relacionados con el contenido (pornografía infantil, infracción a los derechos de autor). En efecto, se considera que las Partes de la Guía relativas a los derechos de los niños abordan tales delitos. Se estima también que la protección de los titulares de derechos es un asunto que afecta a los intereses de este grupo en particular más que a los de los usuarios de Internet. Además, las cuestiones de la interceptación y la vigilancia de las comunicaciones se tratan en la sección sobre privacidad y protección de los datos.

108. Los usuarios de Internet tienen un interés legítimo en gestionar, operar y controlar sus sistemas informáticos sin perturbaciones ni represiones. Deberían recibir protección contra el acceso ilícito a la totalidad o a partes de los sistemas informáticos que utilizan, lo cual incluye el hardware, los componentes, los datos almacenados del sistema instalado, los directorios y los datos de tráfico y contenido. Esta protección se extiende también a las intrusiones no autorizadas en los datos y sistemas informáticos (piratería [*hacking*], quebrantamiento de seguridad [*cracking*] u otras formas de intrusión) que pongan trabas a los usuarios de Internet, como el acceso a datos confidenciales (contraseñas, información, secretos, etc.).¹⁰⁶

109. Los usuarios de Internet deberían recibir protección contra las injerencias que afecten a los datos informáticos, como el uso de códigos malintencionados (p. ej.: virus y troyanos).¹⁰⁷ También deberían recibir protección contra las injerencias que afecten al funcionamiento de los sistemas informáticos o de telecomunicaciones, al ingresar, transmitir, dañar, borrar, alterar o suprimir datos informáticos¹⁰⁸, por ejemplo: programas que generen ataques por denegación de servicio; códigos malintencionados, tales como virus, que impidan o desaceleren sustancialmente la operación del sistema; o programas que envíen grandes cantidades de correo electrónico a un receptor con la intención de bloquear las funciones de comunicación del sistema (*spamming*). En función del derecho interno, puede tratarse de una infracción administrativa o penal.

110. Los usuarios de Internet deberían recibir protección contra la falsificación informática, que implica la creación no autorizada o la alteración de datos de manera que adquieran un valor de prueba diferente en el curso de transacciones legales que dependen de la autenticidad de la información contenida en los datos.¹⁰⁹

111. Los usuarios de Internet tienen un interés legítimo en la protección de los bienes representados o administrados en sistemas informáticos (fondos electrónicos, depósitos). Deberían gozar de protección contra las manipulaciones por fraude informático que les ocasionen una pérdida material o económica directa (dinero, bienes materiales o inmateriales con un valor económico), como el fraude de tarjetas de crédito.¹¹⁰

112. Toda medida de seguridad destinada a garantizar la protección de los usuarios de Internet frente a la ciberdelincuencia debe cumplir plenamente las normas del CEDH, en particular el derecho al respeto a la vida privada y familiar y el derecho a la libertad de expresión.¹¹¹

¹⁰⁶ Convenio de Budapest sobre la ciberdelincuencia, Artículo 2, Informe explicativo, §.44-50.

¹⁰⁷ *Ibid.* Artículo 4, Informe explicativo, § 60-61.

¹⁰⁸ *Ibid.* Artículo 5, Informe explicativo, § 65-69.

¹⁰⁹ *Ibid.* Artículo 7, Informe explicativo, § 81.

¹¹⁰ *Ibid.* Artículo 8, Informe explicativo § 86-88.

¹¹¹ *Ibid.* Artículo 15.

113. Los usuarios de Internet tienen derecho a un proceso equitativo, como lo establece el Artículo 6 del CEDH. Esto se refiere a la determinación de los derechos y obligaciones de carácter civil o de cualquier acusación en materia penal en relación con las actividades de los usuarios de Internet. En particular, tiene que ver con principios clave pronunciados por el Tribunal, como el derecho a ser oído equitativa y públicamente, dentro de un plazo razonable, por un Tribunal independiente e imparcial; el derecho a iniciar una acción ante los tribunales, a una decisión final sobre el caso, a un juicio razonado y a la ejecución de la decisión; el derecho a un procedimiento contradictorio y a la igualdad de armas, entre otros.

114. El Tribunal ha establecido —si bien no en casos relacionados con Internet— principios generales con respeto a la calidad de la administración de justicia (independencia, imparcialidad, competencia del tribunal), la protección del derecho de las partes (audiencia pública y equitativa, igualdad de armas) y la eficiencia de la administración de justicia (plazo razonable).

115. El usuario de Internet tiene derecho a interponer un recurso individual ante el Tribunal después de haber agotado todos los recursos nacionales disponibles y efectivos, dentro de un plazo de seis meses¹¹² a partir de la fecha en que se haya tomado una decisión final.

¹¹² Este plazo será de cuatro meses una vez entrado en vigor el Protocolo n° 15 al CEDH.