La primacía del derecho en internet y en el resto del mundo digital

Resumen ejecutivo y recomendaciones del Comisario para los derechos humanos del Consejo de Europa

Documento temático

COMMISSIONER FOR HUMAN RIGHTS
COMMISSAIRE AUX DROITS DE L'HOMME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

La primacía del derecho en internet y en el resto del mundo digital

Documento temático publicado por el Comisario para los derechos humanos del Consejo de Europa

Resumen ejecutivo y recomendaciones del Comisario

Consejo de Europa

El Comisario para los Derechos Humanos publica estos documentos temáticos para contribuir al debate y la reflexión sobre cuestiones de derechos humanos que revistan importancia en la actualidad. Muchas de ellas comprenden Recomendaciones formuladas por el Comisario como respuesta a preocupaciones concretas. Las opiniones expresadas en estos documentos especializados no reflejan necesariamente la posición del Comisario.

El documento temático en versión inglesa está disponible en: commissioner@coe.int. La versión electrónica está disponible igualmente en http://www.coe.int/web/commissioner/publications

Foto de la cubierta: © Shutterstock

Cubierta y diseño: Departamento de Documentación y Publicaciones del Consejo de Europa (SPDP).

Impreso en el Consejo de Europa

Agradecimientos:

El presente documento temático fue preparado por el profesor Douwe Korff, profesor visitante de la Universidad de Yale (Information Society Project) y de la Oxford Martin Associate, Oxford Martin School, Universidad de Oxford, Reino Unido. El profesor Korff y el Comisario quisieran agradecer igualmente las aportaciones y comentarios tan útiles que Joe McNamee, del European Digital Rights (EDRi), realizó a la versión preliminar, en concreto los relativos a las medidas privatizadas de ejecución.

Tabla de contenido

Resumen Ejecutivo

Este documento temático urge a tratar la siguiente cuestión: ¿como podemos asegurarnos de que tanto en la red como en el resto del mundo digital se instaure y perdure además la primacía del derecho? La sección nº 1 describe las diferentes actividades en línea y las amenazas que existen en este entorno. La sección nº 2 hace referencia a los principios emergentes sobre "gobernanza de internet" y advierte del control excesivo que ejercen los EE.UU. sobre el mundo digital (y el Reino Unido respecto a Europa), lo que podría provocar la fragmentación de la red. La sección nº 3 esboza las normas internacionales que rigen el estado de derecho y algunos problemas que plantea la aplicación de la ley en este nuevo entorno. Por último, la sección nº 4 examina en detalle las principales temáticas que surgen de las secciones previas (libertad de expresión, aplicación del derecho privado, protección de datos, ciberdelincuencia y seguridad nacional) y analiza los delicados equilibrios que dichas temáticas requieren.

El Comisario para los Derechos Humanos del Consejo de Europa ha formulado una serie de recomendaciones basadas precisamente en las cuestiones planteadas en este documento temático y que son descritas tras este resumen ejecutivo.

Un nuevo entorno para las actividades humanas

Vivimos en un entorno digital global que ha abierto nuevas posibilidades tanto en actividades locales, como regionales y mundiales, que incluyen nuevas formas de activismo político, intercambios culturales y el ejercicio de los derechos humanos. Dichas actividades no son virtuales en el sentido de "totalmente irreales" sino que, por el contrario, constituyen una parte esencial de la vida de los ciudadanos. Las restricciones de acceso a internet o a los entornos digitales así como los intentos de controlar nuestras actividades o nuestras comunicaciones electrónicas en línea, perjudican nuestros derechos fundamentales a la libertad de expresión y de información, a la libertad de asociación, a la intimidad y a la vida privada (y, posiblemente, otros derechos como la libertad religiosa y de creencias, o el derecho a un juicio justo).

El nuevo entorno digital mundial constituye además un nuevo espacio para la comisión de conductas ilícitas, tales como la incitación al odio, la difusión de la pornografía infantil, la incitación a la violencia, la vulneración de los derechos de autor (piratería), el fraude, el robo de identidad, el blanqueo de dinero y los ataques a la propia infraestructura de las comunicaciones electrónicas mediante software malicioso (troyanos y gusanos, entre otros) o "denegación de servicio". La ciberdelincuencia y la ciberseguridad constituyen hoy en día una de las grandes preocupaciones.

Cada vez más estas amenazas tienen un carácter transnacional y existe un amplio consenso internacional en cuanto a la necesidad de tratar la ciberdelincuencia, la ciberseguridad y el terrorismo, aunque existe un menor acuerdo en cuanto a los detalles - incluso a la hora de concretar qué, en concreto, constituye una amenaza.

Destacan cuatro temas. En primer lugar, las acciones del Estado encaminadas a contrarrestar tanto la ciberdelincuencia como las amenazas a la ciberseguridad y la seguridad nacional están cada vez más entrelazadas. Los límites que separan unas y otras son difusos, y las instituciones y organismos que se ocupan de ellas colaboran de manera cada vez más estrecha. En segundo lugar, los Estados están actualmente coordinando sus acciones en todos estos aspectos. En tercer lugar, la labor de los organismos de seguridad nacional y de inteligencia depende cada vez más de la observación de individuos y grupos en el ámbito digital. En cuarto lugar, priman hoy en día los métodos de inteligencia y prevención, en sustitución de los métodos retroactivos (*ex post facto*) de mantenimiento del orden público, permitiéndose a los organismos policiales utilizar técnicas - y tecnologías - previamente reservadas a los servicios secretos.

Naturaleza del entorno digital

Datos peligrosos

Nos encontramos en una época de "datos masivos" (los datos sobre nuestras acciones son compartidos y / o explotados de forma colectiva) y del "internet de las cosas" (cada vez más objetos físicos - cosas - se comunican a través de internet), en la que cada vez es más difícil garantizar el verdadero anonimato: cuantos más datos haya disponibles, más fácil se vuelve identificar a una persona. Por otra parte, la extracción cada vez más sofisticada de datos masivos conlleva a la creación de perfiles. Aunque estos perfiles se utilizan para detectar fenómenos poco frecuentes (por ejemplo, para encontrar a un terrorista entre una gran cantidad de información, como puede ser el registro de pasajeros de las compañías aéreas), son poco fidedignos y pueden conducir de forma inconsciente a una discriminación por motivos de raza, sexo, religión o nacionalidad. Estos perfiles tienen una complejidad tal que las decisiones basadas en ellos pueden convertirse efectivamente en incontestables y que ni siquiera aquellos que las aplican comprenden completamente lo que conllevan.

El entorno digital puede, por su propia naturaleza, minar la privacidad y otros derechos fundamentales y socavar la toma de decisiones responsables. Así mismo, abre enormes posibilidades para que se pueda socavar la primacía del derecho - mediante el debilitamiento o destrucción de los derechos a la intimidad, restringiendo la libertad de comunicación o la libertad de asociación - y la interferencia arbitraria.

Global y privado, aunque no en las nubes

Debido a la naturaleza abierta de internet (lo que es a su vez su mayor fuerza), cualquier extremo de la red puede comunicarse con prácticamente cualquier otro, siguiendo la ruta que es considerada como la más eficaz, permitiendo que los datos fluyan a través de todo tipo de conmutadores, routers y cables: la infraestructura física de internet. El sistema de comunicaciones electrónicas es transnacional, global de hecho, por su propia naturaleza; y su infraestructura es física, está situada en lugares reales, a pesar que se hable de una "nube". Por el momento muchos de estos componentes físicos se encuentran en EE.UU. y la mayoría son gestionados y controlados por entidades privadas, no por agencias gubernamentales.

La principal infraestructura de internet consta de cables de fibra óptica de alta capacidad que atraviesan los océanos y mares del planeta, así como de cables y routers terrestres asociados a aquellos. Los cables más importantes en Europa son los que van desde el continente europeo hacia el Reino Unido y de allí, bajo el Atlántico, hasta EE.UU. Dado el dominio que ejercen las empresas estadounidenses sobre internet y sobre la nube, estos cables transportan gran parte de todo el tráfico de internet y de los datos comunicados con base a internet, incluidos casi todos los datos hacia y desde Europa.

Quien tiene el control?

Gobernanza de internet

Tanto el Consejo de Europa como otras instituciones han propuesto importantes principios de gobernanza de internet que hacen hincapié en la necesidad de aplicar el derecho internacional público y el derecho internacional en materia de derechos humanos por igual, tanto en la red como fuera de ella, y de respetar el estado de derecho y la democracia en internet. Estos principios reconocen y apoyan a las múltiples partes interesadas en la gobernanza de internet e instan a todos los actores públicos y privados a que defiendan los derechos humanos en todas sus operaciones y actividades, incluso en el diseño de nuevas tecnologías, servicios y aplicaciones. Hacen además un llamamiento a los Estados para que respeten la soberanía de otras naciones, y se abstengan de actos que puedan perjudicar a las personas o entidades fuera de su jurisdicción territorial.

Sin embargo, estos principios siguen siendo declarativos en su mayor parte, meras intenciones: las disposiciones de gobernanza de internet en las que se puede confiar para garantizar la aplicación práctica de estos principios son aún deficientes.

Asimismo, la gobernanza de internet debe tener en cuenta que EE.UU. – en parte por su dominio corporativo y en parte por sus acuerdos históricos – tienen mayor control de internet que cualquier otro Estado (o incluso que todos los demás Estados juntos). Junto a su socio más cercano, el Reino Unido, tiene acceso a la mayor parte de la infraestructura de internet.

El ex-empleado de la Agencia Nacional de Seguridad de EE.UU., Edward Snowden, ha revelado que EE.UU. y el Reino Unido están utilizando este control y este acceso para vigilar de forma masiva tanto internet como los sistemas de comunicaciones electrónicas globales y las redes sociales. Se teme que la respuesta de los Estados a las revelaciones de Snowden sea la fragmentación de internet, con países o regiones empeñados en que sus datos se transmitan únicamente a través de routers y cables locales, y se almacenen en nubes locales. Hay pues un riesgo de que se destruya internet tal y como lo conocemos hoy en día, con la instauración de barreras nacionales a la red global. Salvo que EE.UU. mejore el respeto de las normas internacionales en materia de derechos humanos en sus actividades, tanto en internet como en los sistemas de comunicación global, será difícil impedir una evolución truncada de internet.

Control del sector privado

Gran parte de la infraestructura de internet y del entorno digital en general está en manos de entidades privadas, muchas de ellas corporaciones de EE.UU. Esta situación plantea problemas, al no estar las empresas directamente obligadas por el derecho internacional en materia de derechos humanos - que se aplica de forma directa únicamente a Estados y gobiernos – con lo que es más complicado obtener reparación de este tipo de empresas. Además, las entidades privadas están sujetas al derecho interno de los países en los que están implantadas o activas - y dichas normas no siempre se ajustan al derecho internacional o a las normas internacionales de derechos humanos: pueden imponer restricciones a las actividades en internet (por lo general, afectando a la libertad de expresión) que violan la legislación internacional de derechos humanos, o pueden imponer o permitir interferencias, tales como vigilar las actividades en internet o las comunicaciones electrónicas, lo que vulnera la normativa internacional de derechos humanos; además tales acciones pueden aplicarse extraterritorialmente, lo que constituye una violación de la soberanía de otros Estados.

La aplicación del derecho nacional a las actividades de entidades privadas que controlan (partes significativas de) el mundo digital es algo extremadamente complejo y delicado. Por supuesto los Estados tienen el derecho, e incluso el deber, de contrarrestar la actividad criminal que se sirve de los sistemas de internet o de comunicación electrónica. Para ello recurren, naturalmente, a la ayuda de las principales entidades privadas. Las propias empresas responsables son las primeras en querer evitar que sus productos y servicios sean utilizados con fines delictivos. No obstante, en tales circunstancias, la actuación de los Estados debería cumplir exhaustivamente con sus compromisos internacionales en materia de derechos humanos y respetar plenamente la soberanía de otros Estados. En particular, los Estados no deberían eludir sus obligaciones de derecho constitucional o internacional, alentando restricciones a los derechos humanos a través de las acciones "voluntarias" de los intermediarios; las empresas, por su parte, deberían igualmente respetar los derechos humanos de las personas.

El estado de derecho en el nuevo entorno digital

El estado de derecho

El estado de derecho es un principio de gobernanza por el cual todas las personas, instituciones y entidades, públicas y privadas, incluido el propio Estado, están sometidas a unas leyes promulgadas públicamente, aplicadas de manera igualitaria e independiente, y respetuosas con las normas y estándares internacionales de derechos humanos. Tal principio implica la adhesión a los principios de la supremacía del derecho, la igualdad ante la ley, la rendición de cuentas ante la ley, la imparcialidad en la aplicación del derecho, la separación de poderes, la participación en la toma de decisiones, la seguridad jurídica, evitar la arbitrariedad y la transparencia procesal y legal.

Los tests básicos sobre la "primacía del derecho" desarrollados por el Tribunal Europeo de Derechos Humanos

El Tribunal Europeo de Derechos Humanos ha desarrollado en su jurisprudencia unos elaborados tests sobre la "primacía del derecho" que han sido adoptados por otros

órganos internacionales de derechos humanos. Para superar estos tests, todas las restricciones a los derechos fundamentales deben basarse en normas jurídicas claras, precisas, accesibles y previsibles, y deben obedecer a objetivos claramente legítimos; deben ser "necesarios" y "proporcionales" a la finalidad legítima correspondiente (dentro de un cierto "margen de apreciación"); y debe existir un "recurso efectivo [preferentemente judicial]" contra las presuntas violaciones de dichos requisitos.

"Todos", sin distinción

Este es uno de los distintivos del derecho internacional en materia de derechos humanos desde 1945, y uno de sus mayores logros, el que los derechos humanos deban ser reconocidos a "todos", a todos los seres humanos: son derechos humanos, no únicamente derechos de los ciudadanos.

Por lo tanto, salvo muy contadas excepciones, todas las normas, de todos los Estados, que afecten o interfieran con los derechos humanos deben aplicarse a "todos", sin discriminación de ningún tipo, incluida la discriminación por motivos de residencia o nacionalidad.

Dado el lugar preeminente que ocupan los EE.UU. y las empresas estadounidenses en el funcionamiento de internet, el marco jurídico constitucional y corporativo de los EE.UU. es de particular importancia. Sin embargo, en contraste con el principio del derecho internacional en materia de derechos humanos antes mencionado, muchas de las garantías de los derechos humanos existentes en la Constitución de Estados Unidos y en diversas leyes estadounidenses relacionadas con el entorno digital sólo se aplican a los ciudadanos estadounidenses y a los ciudadanos no estadounidenses que residen en los EE.UU. ("personas estadounidenses"). Así, sólo las "personas estadounidenses" se benefician de la Primera Enmienda, que abarca la libertad de expresión y la libertad de asociación; de la Cuarta Enmienda, que protege a los ciudadanos estadounidenses de "búsquedas irrazonables"; y de la mayoría de las (limitadas) protecciones contra la excesiva vigilancia derivada de las principales normas en materia de seguridad nacional e inteligencia (Enmienda a la FISA -Ley de Vigilancia de la Inteligencia Extranjera- y los Patriot Acts).

"Bajo la jurisdicción [y en el territorio] de un Estado contratante"

> El deber de los Estados es cumplir con sus responsabilidades en virtud del derecho internacional en materia de derechos humanos aún cuando actúen extraterritorialmente.

Los principales tratados internacionales de derechos humanos, como el Pacto Internacional de Derechos Civiles y Políticos (PIDCP) y la Convención Europea de Derechos Humanos (CEDH), exigen a los Estados que "garanticen" o "aseguren" los derechos humanos establecidos en dichos tratados a "todos aquellos bajo su jurisdicción"(o "dentro de su jurisdicción"). A este requisito se le va otorgando cada vez más un carácter funcional, más que territorial - como han reafirmado recientemente el Comité de Derechos Humanos y el Tribunal Europeo de Derechos Humanos. En otras palabras, cada Estado debe asegurar o garantizar estos derechos a cualquier persona bajo su control físico o cuyos derechos se vean afectados por sus acciones (o las de sus agencias).

Por tanto, los Estados deben cumplir con sus obligaciones internacionales en materia de derechos humanos cuando adopten medidas que puedan afectar los derechos humanos de los individuos - incluso cuando actúen fuera de su territorio o tomen medidas con efecto extraterritorial.

Esta obligación tiene consecuencias concretas en el caso de los datos – que son los que constituyen el mundo digital- y en especial de los datos personales, como se reconoce en la ley de protección de datos europea, que protege a todo individuo cuyos datos sean tratados por los responsables de tratamiento europeos, independientemente de su lugar de residencia, nacionalidad o cualquier otra condición social. Sin embargo, los EE.UU. rechazan formalmente esta interpretación del derecho internacional en materia de derechos humanos, lo que supone una grave amenaza para la primacía del derecho en el entorno digital, dado el predominio que los EE.UU. (así como las corporaciones estadounidenses sujetas a su jurisdicción) tienen en este nuevo entorno.

Inconvenientes derivados de leyes concurrentes y contradictorias aplicadas simultáneamente a las actividades en línea, especialmente en lo que concierne a la libertad de expresión

El problema derivado de la aplicación concurrente y contradictoria de diferentes legislaciones nacionales al material y a las actividades de internet es un tema que requiere ser abordado con urgencia, con el fin de garantizar la primacía del derecho en internet.

Lo que se pone en cuestión no es el derecho de los gobiernos a adoptar medidas que se ajusten al derecho internacional y que sean necesarias y proporcionadas en una sociedad democrática. Los gobiernos deben, por supuesto, tener libertad para tomar decisiones reglamentarias dentro de su jurisdicción. Lo que está aquí en entredicho es la capacidad y el derecho de gobiernos o tribunales nacionales para tomar medidas que conlleven restricciones en terceros países en los que las personas actúen de acuerdo con las leyes de su país de residencia y que, a diferencia de las leyes extranjeras, deben de ser conocidas (o "conocibles") para aquellas y de aplicación previsible.

En principio, los individuos y empresas que faciliten información proveniente de su país de residencia o establecimiento deberían estar vinculados únicamente por la legislación de dicho país; y aquellas personas que accedan o descarguen materiales de sitios web extranjeros cuando pueden y deben saber que dichos materiales son ilegales en su país de residencia deberán regirse por las leyes de este último país. Los Estados únicamente deberían ejercer jurisdicción sobre los materiales extranjeros que no sean ilegales según el derecho internacional en circunstancias muy concretas, es decir, cuando haya un nexo claro y cercano entre los materiales o el difusor y el Estado que tome las medidas.

Derechos humanos y entidades privadas

La legislación sobre derechos humanos y los Principios de Ruggie, el Consejo de Europa y otras disposiciones

El derecho internacional en materia de derechos humanos se aplica fundamentalmente sólo a los Estados y a las acciones (u omisiones) de las autoridades públicas. Sin embargo, están emergiendo nuevas normas internacionales que están pensadas para que las empresas las cumplan. Las más importantes son los *Principios Rectores* de la ONU *sobre las empresas y los derechos humanos* (Principios de Ruggie), elaborados por el Representante Especial del Secretario General de Naciones Unidas sobre empresas y derechos humanos, el profesor John Ruggie. Sin embargo, los Principios de Ruggie se centran fundamentalmente en el deber de los Estados de acogida de actuar en contra de las violaciones de los derechos humanos cometidas por las empresas; no se ocupan en detalle de la situación inversa, es decir, cuando los Estados realizan demandas a empresas que les llevan a cometer violaciones del derecho internacional en materia de derechos humanos.

Parece importante la necesidad de una mayor orientación, tanto por parte del Consejo de Europa como por parte de otros organismos, sobre la responsabilidad de las empresas que hacen frente (o que se colocan en situaciones en las que muy posiblemente hagan frente) a exigencias de los gobiernos o entidades privadas para que lleven a cabo medidas que puedan violar el derecho internacional en materia de derechos humanos (como se detalla más adelante en la sección sobre medidas privatizadas de ejecución).

Filtro y bloqueo por parte de empresas de internet y de comunicaciones electrónicas, siguiendo las instrucciones de - o basándose en el "estímulo" de – los Estados

Aparte de penalizar material de internet – más aún cuando los materiales son producidos en otro país, *a posteriori*, una vez que han sido publicados y visitados – los Estados son cada vez más proclives a prevenir (bloquear) el acceso a ciertos materiales e información en línea. Este bloqueo o filtrado se realiza mediante software o hardware que revisa las comunicaciones y decide, sobre la base de criterios preestablecidos, si se impide o no el reenvío de los materiales a un determinado destinatario, a menudo alguien que navega por internet.

Tal vez no nos sorprenda el hecho de que los Estados represivos intenten bloquear el acceso a sitios web de la oposición y que los regímenes teocráticos hagan lo mismo con los sitios web que consideran blasfemos. Pero existen cada vez más Estados, supuestamente respetuosos con la primacía del derecho – incluidos Estados miembros del Consejo de Europa –, que también están tratando de bloquear el acceso a materiales que ellos consideran inaceptables. O, en un marco más insidioso y menos responsable aún, que "alientan" a los guardianes de internet (los ISP -Proveedores de Servicios de Internet- y los MNO -Operadores de Telefonía Movil-) para que lo hagan "de forma voluntaria", fuera de un marco jurídico claro de derecho público.

Por lo general, en los países democráticos, el bloqueo o las medidas de filtrado se han dirigido principalmente, al menos oficialmente y en un primer momento, contra objetivos perfectamente legítimos: "incitación al odio" racista o religioso o la

pornografía infantil. El problema, sin embargo, es que estos sistemas adolecen de fallos importantes en su funcionamiento:

- el bloqueo es fácil que provoque (de manera no intencionada) falsos positivos (es decir, el bloqueo de sitios web que carecen de material prohibido) y falsos negativos (cuando los sitios web con materiales prohibidos logran atravesar un filtro);
- los criterios para bloquear unos sitios web y no otros, y las listas de sitios web bloqueados, son a menudo opacos en el mejor de los casos, secretos en el peor;
- los procedimientos para recurrir pueden ser costosos, poco conocidos o inexistentes, sobre todo si la decisión sobre lo que se debe bloquear o no se deja - deliberadamente - a las entidades privadas;
- las medidas de bloqueo son fáciles de burlar, incluso para aquellas personas técnicamente no muy cualificadas;
- lo realmente crucial, en particular en lo que concierne la pornografía infantil, es que el bloqueo no aborda en absoluto el verdadero problema: el abuso de los menores en cuestión.

Los problemas anteriores se ven agravados por el hecho de que, una vez que los Estados han introducido el bloqueo para frenar los problemas más graves, como la pornografía infantil y la incitación al odio, tienden a extenderlo a otro tipo de asuntos que también desaprueban. A nivel mundial, incluso en Europa, ha habido intentos por parte de los Estados para bloquear no solo aquellos sitios web que incitan al odio y hacen apología del terrorismo, sino también aquellos otros que, por ejemplo, contienen debates políticos o información sobre los derechos sexuales o de las minorías.

Resulta útil distinguir entre dos situaciones diferentes: el bloqueo del contenido con base legal, de aquel otro que no la tiene. Hay, sin lugar a dudas, ciertos contenidos para los que están legítimamente justificas la aplicación de medidas de bloqueo (bloqueo, con base legal, de contenido ilegal). Sin embargo, el propósito de la medida de bloqueo y los medios técnicos reales utilizados para llevarla a cabo siguen siendo cruciales para determinar si la medida es proporcional y, por lo tanto, lícita – así, por ejemplo, cuando hay evidencia de niveles significativos de acceso accidental al contenido en cuestión y cuando el acceso deliberado sigue siendo fácil tras la medida de bloqueo, la proporcionalidad del bloqueo resulta más discutible.

El asunto se complica si la decisión relativa a los sitios web que se bloquean se deja al arbitrio de las entidades privadas "alentadas" por Estados que, sin embargo, reclaman no tener ninguna responsabilidad en dicho bloqueo (bloqueo de contenido sin base legal). Algunos países, como el Reino Unido y Suecia, han introducido sistemas de bloqueo basados en acuerdos voluntarios con los ISP. Mientras todas las consideraciones relativas a la eficacia y la proporcionalidad de la medida siguen siendo pertinentes para este tipo de bloqueo, sigue planteándose una cuestión más general y fundamental que requiere ser abordada: ¿hasta que punto estas medidas de bloqueo son realmente voluntarias y / o entrañan la responsabilidad del Estado? El hecho de que el artículo 10 del CEDH sólo se refiera a las injerencias sobre este derecho por parte "de las autoridades públicas" no significa que el Estado pueda, sin más, lavarse las manos respecto a las medidas llevadas a cabo por entidades privadas que tengan tal efecto – especialmente si el Estado, *de facto*, ha alentado

insistentemente dichas medidas. En tales circunstancias, el Estado es responsable por no establecer un sistema con una base jurídica: sin esa base, las restricciones no tienen legitimación "legal".

En su jurisprudencia reciente, el Tribunal Europeo de Derechos Humanos ha señalado claramente los peligros del bloqueo indiscriminado. En su sentencia del caso *Yildirim c. Turquía*, el Tribunal observó que la medida en cuestión - el bloqueo del acceso a todos los sitios web de Google Turquía con el fin de bloquear un sitio web de Google al que se consideró irrespetuoso con Kemal Atatürk - había provocado efectos arbitrarios y no se podía decir que su intención fuera exclusivamente bloquear el acceso al sitio web infractor, dado que consistió en un bloqueo masivo de todos los sitios web alojados por Google. Por otra parte, se consideró que los procedimientos de revisión judicial relativos al bloqueo de sitios de internet eran insuficientes para cumplir los criterios que evitaran el abuso, dado que el derecho interno no preveía ninguna salvaguardia para garantizar que una orden de bloqueo con respecto a un sitio específico no se utilizara para bloquear el acceso en general. Por consiguiente, el Tribunal consideró que existía una violación del artículo 10 del CEDH.

Inspección a fondo de paquetes (DPI) realizada indiscriminadamente por empresas mediante órdenes judiciales emitidas a petición de otras empresas, con el fin de hacer respetar los derechos de autor.

Los titulares de los derechos de propiedad intelectual piden cada vez más la imposición de filtros o bloqueos, similares a los descritos anteriormente, a aquellos sitios web que supuestamente faciliten el reparto de contenidos pirateados; y exigen cada vez más el acceso a los datos de los usuarios de internet que tengan relación con el supuesto reparto, incluso mediante el uso obligatorio de la DPI por los ISP, con el fin de detectar los probables (o posibles) infractores de dichos derechos.

La DPI requiere que el "inspector" examine no sólo una amplia variedad de metadatos relacionados con el origen o el destino del "paquete", sino también el contenido de dichas comunicaciones. Los paquetes son elegidos en base a un patrón o algoritmo vinculado al contenido específico. Para los titulares de los derechos de propiedad intelectual constituirán los indicadores específicos de un vídeo o una fotografía en especial protegida con un copyright. Pero esa misma tecnología permite realizar búsquedas prácticamente de cualquier cosa: un determinado discurso político, una determinada canción revolucionaria, un emblema sindical. Estas medidas son fuertemente intrusivas dado que requieren la vigilancia de todos los usuarios de un ISP (o de la red de telefonía móvil), cuando únicamente se trata de identificar a los pocos que son probablemente (o posiblemente) los infractores de los derechos de autor, planteando de ese modo serios interrogantes en cuanto a su necesidad y proporcionalidad.

Tanto el Tribunal Europeo de Derechos Humanos como el Tribunal de Justicia de la Unión Europea han dictado importantes sentencias en las que se indica claramente que el filtrado indiscriminado de todas las comunicaciones realizadas por un ISP (o un MNO) – es decir, el seguimiento o vigilancia en general – con el propósito de identificar posibles infractores de dichos derechos entre la masa de usuarios inocentes, es contrario a la normativa de los derechos humanos.

El ejercicio de la jurisdicción extraterritorial por los Estados

Un Estado que utiliza sus poderes legislativos y ejecutivos para capturar o ejercer de otra manera el control sobre los datos que no se encuentran físicamente en su territorio, sino en el territorio de otro Estado – por lo general mediante el uso de la infraestructura física de internet y de los sistemas de comunicaciones globales con el fin de extraer dichos datos de los servidores situados en el otro Estado o exigiendo a aquellas entidades privadas que tienen acceso a dichos datos en el extranjero que extraigan esos datos de los servidores o dispositivos en otro país y los entreguen al Estado – esta ejerciendo su jurisdicción extraterritorialmente en la jurisdicción del otro Estado.

Según el derecho internacional público en general, en ausencia de tratados que otorguen poderes de jurisdicción ejecutiva extraterritorial a las agencias extranjeras, no es lícito que el primer Estado ejerza tal jurisdicción sin el consentimiento del segundo Estado.

Las diferentes temáticas y el equilibrio entre ellas

Las diferentes temáticas

Establecer la primacía del derecho en internet y en general, en el mundo digital, requerirá la aclaración de aquellas reglas que afectan a la libertad de expresión, las entidades privadas (en particular las empresas) y los derechos humanos, la protección de datos y la ciberdelincuencia. Pero entonces surge la siguiente cuestión: ¿cómo se mantiene el equilibrio entre todas esas reglas en este nuevo entorno?

Libertad de expresión

La legislaciones nacionales relativas a las actividades en internet y en general, en el entorno digital, especialmente las legislaciones relativas a la libertad de expresión, son con frecuencia concurrentes y contradictorias. En virtud de lo dispuesto por legislaciones de numerosos Estados, las personas que realizan declaraciones en línea o utilizando comunicaciones electrónicas en o desde un país, pueden ser consideradas responsables en virtud de la legislación de otro país si dichas declaraciones implican una violación de dicha legislación, incluso si son acordes a derecho en el lugar en que se hicieron. Esto plantea una amenaza fundamental para la primacía del derecho en internet y en el ámbito informático en general. Sin embargo, este aspecto no ha sido aún abordado plenamente por la jurisprudencia del Tribunal Europeo de Derechos Humanos.

Como se sugirió anteriormente, la única manera de evitarlo sería si los Estados y los tribunales nacionales dieran muestras de clara moderación, absteniéndose de aplicar su derecho interno a expresiones e informaciones difundidas desde el extranjero a través de internet, a menos que éstas sean ilegales según el derecho internacional o que presenten claros vínculos que justifiquen el ejercicio de la jurisdicción estatal.

Otra cuestión importante es la responsabilidad de aquellas personas o empresas que gestionan un sitio web, o incluso de los ISP, respecto a los contenidos publicados en un sitio web. Aquí también, la jurisprudencia a nivel europeo sigue siendo limitada. Por ahora, las empresas privadas parecen estar atrapadas entre obligaciones claras (eliminar el contenido o afrontar la pena) y obligaciones poco claras (que garanticen a los usuarios el acceso a los contenidos legales). Ello puede provocar que las empresas

privadas tiendan a adoptar una actitud de excesivo cumplimiento evitando que todos los usuarios tengan acceso a materiales perfectamente legales, protegiéndose al mismo tiempo de posibles reclamaciones procedentes de los usuarios afectados, aplicándoles términos y condiciones imprecisas. Todas estas cuestiones constituyen temas clave que necesitan respuestas.

Medidas privatizadas de ejecución

El hecho de que internet y el entorno digital mundial esté controlado en gran parte por entidades privadas (especialmente, aunque no sólo, compañías estadounidenses) también representa una amenaza para la primacía del derecho. Tales entidades privadas pueden imponer (y ser "alentadas" para hacerlo) restricciones de acceso a la información sin estar sujetas a las restricciones de derecho constitucional o internacional aplicables a las limitaciones estatales a la libertad de expresión. Los tribunales nacionales, actuando a instancia de otras entidades privadas, pueden además requerir a ciertas entidades privadas que lleven a cabo análisis altamente intrusivos de sus datos, con el fin de detectar infracciones probables (o simplemente posibles) de los derechos de propiedad, a menudo derechos de propiedad intelectual. Se les puede requerir que "extraigan" datos, incluidos datos gubernamentales, comerciales y personales, desde servidores en otros países, con fines policiales o de seguridad nacional, sin necesidad de obtener el consentimiento del otro país - o el consentimiento de las empresas o titulares de los datos en el otro país –vulnerando así la soberanía del otro país, la confidencialidad comercial a la que las empresas tienen derecho, así como los derechos humanos de los titulares de los datos.

Los principios de Ruggie de las Naciones Unidas si bien indican la importancia de abordar estas cuestiones, no proporcionan las respuestas. Como ya se ha mencionado, se necesitan, por tanto, nuevos enfoques y directrices. El Consejo de Europa ha hecho importantes contribuciones a este debate al sugerir tanto que los Estados podrían ser declarados responsables por no garantizar que las entidades privadas no vulneren los derechos humanos de sus ciudadanos, como que los Estados tienen la obligación de garantizar que los términos y condiciones generales de las empresas privadas que no estén en conformidad con las normas internacionales de derechos humanos sean declarados nulos y sin efectos.

Protección de datos

La legislación europea de protección de datos se basa en un conjunto de principios básicos (tratamiento leal; especificación de sus fines y limitación de su alcance; minimización de los datos; calidad de los datos y seguridad de los datos) y en un conjunto de derechos de los titulares de los datos y de remedios (supervisión por parte de autoridades de protección de datos independientes) que son un especial reflejo de los principios generales de la "primacía del derecho" desarrollados por el Tribunal Europeo de Derechos Humanos. El Convenio para la protección de datos del Consejo de Europa (Convenio nº 108) y las normas de la UE sobre la materia, especifican cómo el cumplimiento de los requisitos generales de la legislación sobre derechos humanos debe garantizarse en el contexto específico del tratamiento de datos personales. El modelo europeo de protección de datos esta siendo cada vez mejor acogido fuera de la zona del Consejo de Europa: el Convenio nº 108 (actualmente en proceso de modernización) se está convirtiendo en el modelo de referencia mundial para

garantizar la primacía del derecho internacional en este aspecto concreto, lo que es crucial para internet y el mundo digital en general.

La protección de datos europea se ha reforzado aún más tras una sentencia del Tribunal de Justicia de la Unión Europea que ha rechazado la retención de datos obligatoria, carente de sospecha y sin un fin concreto. Con respecto al debate sobre las prácticas de los servicios de inteligencia y seguridad impulsado por las revelaciones de Edward Snowden, es cada vez más evidente que los programas de vigilancia secretos, masivos e indiscriminados no son conformes con la ley europea de derechos humanos y no se puede justificar su uso para la lucha contra el terrorismo u otras amenazas importantes para la seguridad nacional. Tales interferencias sólo pueden admitirse si son estrictamente necesarias y proporcionadas a un objetivo legítimamente perseguido.

La protección de datos en las redes europeas proporciona la primera y más importante piedra angular para la primacía del derecho en internet y en el mundo digital en general. Como resultado de ello será crucial garantizar que la revisión (modernización) del Convenio nº 108, actualmente en curso, no de lugar a ninguna merma normativa. La adhesión por parte de los EE.UU. al Convenio nº108 sería particularmente valiosa, no sólo para los ciudadanos estadounidenses, sino como un avance hacia un enfoque global más exhaustivo en el respeto al derecho fundamental a la protección de datos y a los derechos que aquel posibilita.

Ciberdelincuencia

El Convenio sobre la ciberdelincuencia exige a los Estados Partes que tipifiquen ciertos actos - como el acceso ilegal a los sistemas informáticos (piratería), interceptación ilegal de comunicaciones electrónicas, el envío de software malicioso, violaciones de derechos de autor y la producción o difusión de pornografía infantil – como delitos con arreglo a su derecho interno; su protocolo adicional exige a los Estados Partes que penalicen la difusión de material racista y xenófobo (incitación al odio). Establece además amplias disposiciones sobre cooperación internacional en la lucha contra este tipo de delitos, incluida la asistencia jurídica mutua en la investigación y conservación de pruebas, la extradición y otros asuntos similares. El Convenio está abierto a Estados no europeos y ha sido ratificado por cinco de esos Estados, incluidos los EE.UU.

Aunque la necesidad de un acuerdo para combatir la delincuencia en el entorno digital mundial está fuera de toda duda - y el Consejo de Europa es digno de elogio por iniciar un proceso de este tipo – el Convenio aún no está totalmente articulado para garantizar el respeto a la primacía del derecho en su aplicación por los Estados Partes.

Una de las razones para ello es que el Convenio no contiene una cláusula exhaustiva de derechos humanos, por lo que no ofrece protección contra los Estados que establecen delitos con márgenes excesivamente amplios o que no incluyen excepciones o defensas en su derecho sustantivo (como una defensa de interés colectivo para los denunciantes); ni protege contra la excepción de cosa juzgada o la prestación de asistencia (formal o informal) a los Estados Partes cuando ello pueda vulnerar los derechos humanos.

Otra de las razones es que el Convenio no está vinculado a otros instrumentos fundamentales desarrollados por el Consejo de Europa que apoyan la primacía del derecho en contextos digitales y / o transnacionales. Tal vinculación parece tanto más necesaria desde el momento en que el Convenio está abierto a aquellos Estados que

no son parte del CEDH o que no han aceptado plenamente las exigencias similares del PIDCP (como los EE.UU. en relación a sus actividades extra-territoriales o los derechos de los "no estadounidenses"). Desde la perspectiva de la primacía del derecho en Europa, la adhesión al Convenio sobre la ciberdelincuencia requiere tanto la plena aceptación por los Estados de sus obligaciones derivadas del CEDH y / o el PIDCP como la ratificación del Convenio para la protección de datos, el Convenio europeo de extradición y el Convenio europeo de asistencia judicial en materia penal.

Por último, los artículos 26 y 32 del Convenio parecen apoyar la tendencia de las fuerzas de orden público de recurrir a medios "informales" de recopilación de la información, incluso más allá de las fronteras, sin establecer salvaguardias claras (por ejemplo, que no recurran a medios informales para llevar a cabo actividades intrusivas de recopilación de información que normalmente, en un Estado bajo la primacía del derecho, requerirían una orden judicial); ambos artículos parecen también apoyar la tendencia al alza de dichas autoridades a obtener datos directamente de los servidores en otros países o a exigir que las empresas dentro de su jurisdicción - en particular los principales gigantes de internet - lo hagan por ellos, sin recurrir a acuerdos formales de asistencia jurídica mutua entre los Estados, lo que constituye una violación de la soberanía del Estado en donde se encuentran los datos.

El principio - establecido en el artículo 16 del Convenio nº 108, en relación a la asistencia mutua entre las autoridades de protección de datos – por el que existen claras limitaciones a las circunstancias en las que los datos personales pueden ser recogidos y / o transmitidos en actividades transnacionales, debería igualmente inspirar de una manera más adecuada al Convenio sobre la ciberdelincuencia. Una serie de recomendaciones y declaraciones del Comité de Ministros del Consejo de Europa constituyen una buena guía sobre cómo encontrar un equilibrio entre la defensa de los principios de protección de datos y la ejecución adecuada de la ley. Su cumplimiento debería reforzarse por parte de los Estados Miembros que son Partes en el Convenio sobre la ciberdelincuencia.

La redacción de la nueva propuesta de Protocolo Adicional al Convenio sobre la ciberdelincuencia brinda la oportunidad de resolver al menos algunos de estos problemas. Con dichas mejoras, el Convenio sobre ciberdelincuencia podría constituirse en segunda piedra angular de la primacía del derecho en internet y en el resto del mundo digital.

Seguridad nacional

Tanto el Convenio Europeo de Derechos Humanos como el Convenio del Consejo de Europa sobre protección de datos se aplican, en principio, a todas las actividades de los Estados que son parte: Aunque ambos incluyen ciertas reglas especiales y algunas excepciones, no se excluyen explícitamente las cuestiones de seguridad nacional. En esto, el mandato del Consejo de Europa y el alcance de dichos instrumentos difieren de la legislación comunitaria, que expresamente excluye la seguridad nacional de la competencia y jurisdicción de la Unión. Esto significa que cuando se lleve a cabo la regulación jurídica internacional de las actividades de las agencias de inteligencia y de seguridad nacional, el Consejo de Europa deberá asumir un papel de liderazgo, si no a escala mundial, si al menos en Europa.

La necesidad de garantizar la primacía del derecho sobre las actividades de las agencias de seguridad e inteligencia nacionales resulta evidente a la luz de las revelaciones de Edward Snowden acerca de las operaciones de vigilancia mundial llevadas a cabo

por la Agencia de Seguridad Nacional de EE.UU. (NSA), los Cuarteles generales de Comunicaciones del Reino Unido (GCHQ) y por sus socios en el grupo 5EYES (Australia, Canadá y Nueva Zelanda), en particular. Estas revelaciones muestran que dichas agencias intervienen de forma rutinaria los cables de fibra óptica de gran capacidad que forman la columna vertebral de internet e interceptan teléfonos móviles y otras comunicaciones de forma masiva a nivel mundial, por ejemplo, interceptando las comunicaciones por radio a través de "puertas traseras "que han sido instaladas en los principales sistemas de comunicación y aprovechando los puntos débiles, en cuanto a seguridad, de dichos sistemas.

En la legislación europea e internacional de derechos humanos, la seguridad nacional no debe imponerse a otras consideraciones. De hecho, la cuestión misma de lo que legítimamente se puede decir bajo el concepto de "seguridad nacional" es justiciable: debería corresponder a los tribunales la decisión de lo que legítimamente, a la luz del derecho internacional en materia de derechos humanos, abarca o no dicho término. *Los Principios de Johannesburgo sobre la Seguridad Nacional, la Libertad de Expresión y el Acceso a la Información*, elaborados por la ONG Artículo 19 y avalados por diversos foros internacionales, como el Relator Especial de la ONU para la libertad de opinión y de expresión, ofrecen una orientación útil al respecto. Estos principios dejan claro que los Estados sólo podrán invocar la seguridad nacional como medio de interferir en los derechos humanos cuando se trate de asuntos que amenacen la estructura y las instituciones básicas de la nación. A veces, el terrorismo puede alcanzar este nivel, pero en la mayoría de los casos se trataría más de una cuestión de orden público que de un paradigma de la seguridad nacional. Lo mismo sucede con las actuaciones de los Estados respecto a internet y a las comunicaciones electrónicas.

Existe una carencia de reglas convencionales claras que rijan la actuación de los organismos de inteligencia y seguridad nacional, así como la base sobre la que operan y el intercambio de información. En numerosos países, la legislación publicada que regula el trabajo de estas agencias de forma clara, es escasa. En otros, no hay normas publicadas en absoluto. Hasta que no se conozcan las normas bajo las cuales estas agencias y servicios funcionan - a nivel nacional, extraterritorial o en cooperación con otros - no se podrá decir que sus actividades son acordes al estado de derecho. Otro gran motivo de preocupación es la ineficacia manifiesta de muchos de los sistemas de supervisión.

En otras palabras, en relación con la seguridad nacional, no existe todavía ninguna piedra angular real para defender la primacía del derecho- aunque hay, al menos, principios básicos que podrían constituir la base de esta parte tan esencial de los derechos humanos universales.

Dado el incremento de las alianzas entre las fuerzas del orden y las de inteligencia y seguridad, esta negación de la primacía del derecho amenaza con propagarse también a los policías y fiscales. La ausencia de marcos legales claros en este sentido, tanto a nivel nacional como internacional, constituye una amenaza adicional a la primacía del derecho en internet y en el entorno digital mundial.

Recomendaciones del Comisario

Teniendo en cuenta los resultados y las conclusiones de este documento temático, el Comisario hace las siguientes recomendaciones con el objetivo de mejorar el respeto de la primacía del derecho en internet y en general, en el entorno digital.

I. Respecto a la universalidad de los derechos humanos y su aplicación por igual tanto en la red como fuera de ella.

1. Las exigencias básicas de la primacía del derecho son aplicables tanto en la red como fuera de ella y debería procurarse que lo fueran en la práctica. Esto significa concretamente:

- que ningún Estado (y ninguna de sus agencias, incluidas las fuerzas del orden y las agencias de inteligencia y seguridad nacional), europeo o no, debería tener acceso a los datos almacenados en otro país - o aquellos datos que pasan a través de cables que constituyen "la columna vertebral" de internet y de las comunicaciones electrónicas que conectan los diferentes países - sin el claro y expreso consentimiento del país o países afectados. La obtención del consentimiento de los titulares de los datos (ya sea indirectamente, a través de los términos del servicio de los proveedores de comunicaciones, o directamente, en circunstancias en las que no se puede demostrar que se obtuviera de manera libre, o fuera suficientemente específico o bien documentado) o la cooperación de las entidades privadas establecidas en el primer Estado (o en el[los] Estado[s] afectado[s]) no exime de la necesidad de obtener igualmente el consentimiento del Estado afectado;
- que el Convenio Europeo de Derechos Humanos (CEDH) y toda la normativa de protección de datos del Consejo de Europa es aplicable a todas las actividades de tratamiento de datos personales por parte de todas las agencias de todos los Estados miembros del Consejo de Europa, incluidas las agencias de inteligencia y de seguridad nacional;
- que las obligaciones derivadas de la primacía del derecho, incluidas las derivadas de los artículos 8 (derecho al respeto de la vida privada y familiar) y 10 (libertad de expresión) del CEDH, no pueden eludirse mediante acuerdos ad hoc con los actores privados que controlan internet y, en general, el entorno digital; y
- que los Estados miembros del Consejo de Europa deberían esforzarse por asegurar que los Estados no europeos cumplan de forma similar con sus obligaciones internacionales de derechos humanos en aquellas acciones que afecten a las personas que utilizan internet o que son activas en general, en el entorno digital.

II. Respecto a la protección de datos

2. Los Estados miembros que aún no lo hayan hecho deberían ratificar el Convenio del Consejo de Europa para la protección de las personas con respecto al tratamiento automatizado de los datos de carácter personal (Convenio nº 108). Dicho Convenio está abierto también a los Estados no miembros y, en caso de adoptarse ampliamente, podría convertirse en la piedra angular más importante para la primacía del derecho en internet y en general, en el entorno digital.

3. Los Estados miembros que ya lo hayan ratificado deberán velar por que dicho Convenio se aplique plenamente a nivel nacional.

4. La revisión del Convenio nº 108, actualmente en curso, no debería conllevar ninguna disminución de los estándares europeos o mundiales de protección de datos. Por el contrario, debería conducir a una clarificación y una mejor aplicación de las normas, especialmente en relación con internet y el mundo digital en general, así como respecto a la vigilancia con fines de seguridad nacional y de inteligencia.

5. En el contexto de la actual reforma de la normativa de protección de datos de la UE, aquellas normas que pudieran socavar la primacía del derecho, como son las relativas al consentimiento, a la creación de perfiles o al acceso de las autoridades policiales y judiciales extranjeras a los datos personales, deberían aclararse y adecuarse a las obligaciones internacionales de derechos humanos, incluidas las derivadas del Convenio nº 108, y a las principales recomendaciones y directrices del Consejo de Europa.

6. La retención masiva de datos de comunicaciones sin dejar rastro es absolutamente contraria al estado de derecho , incompatible con los principios básicos de protección de datos e ineficaz. Los Estados miembros no deberían recurrir a ella o imponer la retención obligatoria de datos por parte de terceros.

III. Respecto a la ciberdelincuencia

7. Los Estados partes en el Convenio del Consejo de Europa sobre la ciberdelincuencia deben cumplir plenamente con sus obligaciones internacionales de derechos humanos en todo aquello que hagan (o no hagan) en virtud del Convenio, tanto a la hora de definir los delitos pertinentes (así como los elementos, excepciones y defensas relativas a ellos), como en cualquier investigación o proceso penal, o en relación a la asistencia jurídica mutua y la extradición.

8. Si un Estado parte adopta medidas que afectan a personas fuera de su territorio, ello no le exime de sus obligaciones en virtud del Convenio sobre la ciberdelincuencia o en virtud de otros tratados internacionales de derechos humanos (en particular, el CEDH y el PIDCP); al contrario, dichas obligaciones son aplicables igualmente a tales actos extraterritoriales.

9. Todos los Estados partes en el Convenio sobre la ciberdelincuencia deberían igualmente ratificar y aplicar rigurosamente el Convenio sobre la protección de datos, el Convenio europeo de extradición y el Convenio europeo de asistencia judicial en materia penal.

10. Los Estados miembros, incluidas sus fuerzas de orden público, deberían implementar la Recomendación nº R (1987) 15 del Comité de Ministros del Consejo de Europa por la que se regula el uso de datos personales en el ámbito policial, su Recomendación CM/Rec (2010) 13 sobre la protección de las personas con respecto al tratamiento

automatizado de datos de carácter personal en el contexto de la creación de perfiles, y su Declaración de 2013 sobre los riesgos derivados del rastreo digital y de otras tecnologías de vigilancia para los derechos fundamentales.

11. Los Estados miembros deberían asegurarse de que sus fuerzas de orden público no obtienen datos de los servidores y de la infraestructura de otro país en virtud de acuerdos informales. Más bien, deberían utilizar los acuerdos de asistencia mutua y las disposiciones especiales sobre conservación rápida de datos, establecidos ambos por el Convenio sobre la ciberdelincuencia. Las fuerzas de orden público de un país no pueden confiar en el hecho de que entidades privadas - como los proveedores de servicios de internet, las redes sociales o los operadores de redes móviles – situadas en otros países, estén autorizadas para revelar datos de sus clientes conforme a sus condiciones generales, dado que la recopilación de dichos datos en tales circunstancias es contraria a la primacía del derecho y no debería realizarse.

IV. Respecto a la jurisdicción

12. Deberían establecerse límites al ejercicio extraterritorial de la jurisdicción nacional cuando se trate de ciberdelincuencia transnacional. Estos límites deberían tener en cuenta el efecto de las limitaciones sustantivas a los delitos así como de las excepciones o defensas, en el país de origen de la persona (o en el país en el que los hechos se cometieron) en relación con la jurisdicción reclamada por otros Estados que no reconocen dichas limitaciones, excepciones o defensas.

13. En lo que respecta al derecho a la libertad de expresión en particular, los individuos y empresas que faciliten información proveniente de su país de residencia o establecimiento están, en principio, obligados únicamente por la legislación de dicho país; mientras que aquellas personas que accedan o descarguen materiales de sitios web extranjeros (cuando pueden y deben saber que dichos materiales son ilegales en su país de residencia) deberían cumplir con las leyes de este último país. Al margen del contenido que es ilegal según el derecho internacional, los Estados únicamente deberían ejercer jurisdicción sobre los materiales digitales extranjeros en circunstancias muy concretas, cuando haya un nexo claro y cercano entre el material y/o el difusor y el país en cuestión.

V. Respecto a los derechos humanos y las entidades privadas

14. Los Estados miembros deberían dejar de apoyarse en las empresas privadas que controlan internet y el entorno digital en general, para imponer restricciones que vulneran las obligaciones de derechos humanos del Estado. Para evitarlo serían necesarias orientaciones complementarias que establecieran en que circunstancias las acciones u omisiones de las empresas privadas que infringen los derechos humanos implicarían la responsabilidad del Estado. Lo anterior incluiría orientación sobre el grado de participación del Estado que sería necesaria para que la infracción entrañe su responsabilidad y sobre las obligaciones que tiene el Estado para garantizar que las condiciones generales de las empresas privadas no entren en contradicción con la normativa de derechos humanos. Sería necesario examinar igualmente la responsabilidad del Estado con respecto a las medidas puestas en práctica por particulares, por razones comerciales, sin la participación directa de aquel.

15. Partiendo de los Principios Rectores de la ONU sobre las empresas y los derechos humanos (Principios de Ruggie), sería deseable una mayor orientación acerca de cuales

son las responsabilidades de las empresas en relación con sus actividades en (o que afecten a) internet o el entorno digital en general, en particular para cubrir aquellas situaciones en las que las empresas se enfrenten (o puedan ponerse en situaciones de hacerlo) a exigencias de los gobiernos que podrían vulnerar la legislación internacional de los derechos humanos.

VI. Respecto al bloqueo y filtrado

16. Los Estados miembros deberían velar por que cualquier restricción en el acceso a los contenidos de internet que afecta a los usuarios bajo su jurisdicción se base en un marco jurídico estricto y predecible, que regule el ámbito de aplicación de dichas restricciones y que ofrezca la garantía del control judicial (o de evaluaciones ex post en aquellos casos verdadera y manifiestamente urgentes) para evitar posibles abusos. Además, los tribunales nacionales deben examinar si cualquier medida de bloqueo es necesaria, efectiva y proporcionada, y especialmente si dicha medida es lo suficientemente precisa como para afectar únicamente al contenido concreto que requiere ser bloqueado.

17. Los Estados miembros no deberían apoyar o fomentar a los actores privados que controlan internet y el entorno digital en general, para que realicen bloqueos al margen de un marco que recoja los criterios descritos anteriormente.

VII. Respecto a las actividades de seguridad nacional

18. El CEDH y el Convenio nº 108 deben aplicarse a todas las actividades de los Estados que son parte en dichos convenios, incluidas las actividades de seguridad nacional y de inteligencia.

19. En concreto, con el fin de lograr el respeto a la primacía del derecho en internet y en el entorno digital en general:

- a los Estados sólo se les debería permitir invocar la seguridad nacional como medio de interferir en los derechos humanos, cuando se trate de asuntos que amenacen la estructura y las instituciones básicas de la nación;
- aquellos Estados que quieran obstaculizar derechos fundamentales en base a una supuesta amenaza a la seguridad nacional deben demostrar que la amenaza no puede resolverse a través del derecho penal ordinario, que cumple con las normas internacionales relativas al proceso y al derecho penal;
- lo anterior también se aplica a las acciones de los Estados relativas a internet y a las comunicaciones electrónicas.

20. Los Estados miembros deberían incluir las actividades de las agencias de seguridad nacional e inteligencia dentro de un marco jurídico general. Hasta que no haya un aumento de la transparencia en las reglas bajo las cuales operan estos servicios - a nivel nacional, extraterritorial y / o en cooperación entre ellos – no podrá asumirse que sus actividades son conformes con el estado de derecho .

21. Los Estados miembros también deberían asegurarse de que exista una supervisión democrática eficaz sobre los servicios de seguridad nacional, y para ello sería necesario promover una cultura de respeto de los derechos humanos y de la primacía del derecho, en particular entre los funcionarios de los servicios de seguridad.

Hoy en día ejercemos gran parte de nuestros derechos humanos gracias a internet y al entorno digital en general. Pero tales derechos pueden ser igualmente vulnerados utilizando esos mismos medios.

Existe consenso en cuanto que los derechos humanos deben ser disfrutados a través de la red, de la misma manera que fuera de la red. Sin embargo, en la práctica, los actores que pueden garantizarnos el disfrute de tales derechos no son exactamente los mismos en ambos entornos. En particular, la influencia y el control desproporcionados que algunos Estados y ciertas empresas privadas ejercen a nivel mundial sobre internet y sobre su infraestructura física, son dos elementos esenciales que marcan esta diferencia.

Este documento temático analiza cómo se puede mantener la primacía del derecho en un entorno caracterizado por estos problemas de gobernanza tan específicos, y se centra en algunos ámbitos de especial relevancia en materia de derechos humanos: la libertad de expresión, la protección de datos y la privacidad, la ciberdelincuencia y la seguridad nacional. Sugiere finalmente posibles vías que permitan garantizar que la primacía del derecho se aplique a nuestras actividades en línea.

www.commissioner.coe.int

PREMS 214214 ESP

ESP

www.coe.int

El Consejo de Europa es la principal organización del continente que defiende los derechos humanos. Cuenta con 47 Estados miembros, 28 de los cuales son miembros de la Unión Europea.
Todos los Estados miembros han suscrito el Convenio Europeo de Derechos Humanos, tratado concebido para proteger los derechos humanos, la democracia y el Estado de derecho. El Tribunal Europeo de Derechos Humanos supervisa la aplicación del Convenio en los Estados miembros.

COUNCIL OF EUROPE

CONSEIL DE L'EUROPE