

Resumen ejecutivo

ESTÁNDARES PARA UNA INTERNET LIBRE, ABIERTA E INCLUYENTE

1. ALCANCE DEL PRESENTE DOCUMENTO.....	2
2. INTRODUCCIÓN: LIBERTAD DE PENSAMIENTO Y EXPRESIÓN EN INTERNET	2
3. ESTÁNDARES PARA UN INTERNET LIBRE, ABIERTA E INCLUYENTE.....	4
A. INTERNET LIBRE Y ABIERTO: LA NEUTRALIDAD DE LA RED.....	4
B. ACCESO UNIVERSAL Y PLURALISMO	5
C. ALFABETIZACIÓN DIGITAL.....	5
D. PLURALIDAD LINGÜÍSTICA.....	6
E. IGUALDAD Y NO DISCRIMINACIÓN	6
F. PRIVACIDAD	7
E. GOBERNANZA MULTISECTORIAL	7
4. EL ROL DEL SECTOR PRIVADO	8
A. RESPONSABILIDAD DE INTERMEDIARIOS	8
B. EL DISCURSO DE ODO EN INTERNET	10
C. LA REMOCIÓN Y DESINDEXACIÓN DE CONTENIDOS: EL DERECHO AL OLVIDO	10
D. PROPIEDAD INTELECTUAL Y EL ACCESO AL CONOCIMIENTO	11
E. INICIATIVAS DE ACCESO ABIERTO	12
F. PROTECCIÓN DEL DOMINIO PÚBLICO	12
G. RESTRICCIONES Y LIMITACIONES AL DERECHO A LA LIBERTAD DE EXPRESIÓN Y ACCESO AL CONOCIMIENTO EN RELACIÓN CON LA PROTECCIÓN DE DERECHOS DE AUTOR.....	13
5. PROTECCIÓN DE LA PRIVACIDAD	13
A. DATOS PERSONALES	14
B. VIGILANCIA, MONITOREO E INTERCEPTACIÓN	14
C. ENCRIPCIÓN Y ANONIMATO.....	15
D. BIG DATA.....	16
E. INTERNET DE LAS COSAS	16
6. BIBLIOGRAFÍA.....	17

Resumen ejecutivo

ESTÁNDARES PARA UNA INTERNET LIBRE, ABIERTA E INCLUYENTE

1. Alcance del presente documento

El presente documento es un resumen del informe temático "[Estándares para una internet libre, abierta e incluyente](#)", publicado por la Relatoría Especial para la Libertad de Expresión en marzo de 2017, que previamente había sido aprobado por la Comisión Interamericana de Derechos Humanos (CIDH). Este texto se basa en todas sus partes en el informe original pero, en aras de ofrecer un insumo asequible y de ágil lectura, excluye la mayoría de referencias textuales de jurisprudencia y doctrina que se encuentran en el documento oficial. Igualmente, se eliminaron las notas a pie de página que no sean citas textuales. Igualmente, al final del presente texto se referencia la bibliografía utilizada en el informe oficial.¹

Esperamos que este insumo asista a los Estados miembros y actores relevantes de distintos sectores (organismos internacionales, sociedad civil, academia y medios de comunicación) en sus esfuerzos por incorporar un enfoque basado en los derechos humanos, particularmente en el derecho a la libertad de expresión, en la discusión, diseño, desarrollo e implementación de políticas que refieran al funcionamiento de internet.

La primera parte de este resumen desarrolla los estándares propuestos; la segunda aborda el rol del sector privado en Internet, y en tercer término analiza aspectos de la protección de la privacidad en la era digital. Este resumen no incluye el capítulo sobre acceso a la información incluido en el informe original, toda vez que el propósito de ese texto es enfocarse en los asuntos directamente relacionados con el funcionamiento de internet.

2. Introducción: libertad de pensamiento y expresión en internet

Internet aumentó exponencialmente la capacidad de las personas de recibir, buscar y difundir informaciones y opiniones. Dadas sus características –la naturaleza multidireccional y abierta, la velocidad y alcance global a un relativo bajo costo– internet permite la creación individual y conjunta de contenidos, el intercambio y la colaboración permanente. En el entorno digital, cualquier persona puede ser autor y editor.²

Esto representa una forma de democratización y descentralización del derecho a la libertad de expresión donde el discurso público deja de ser moderado por periodistas profesionales o por los medios de comunicación tradicionales. Las nuevas libertades expresivas abren también nuevas capacidades de organización y movilización, y nuevas posibilidades para innovar y generar desarrollo económico.

La libertad de pensamiento y expresión, definida en el artículo 13 de la Convención Americana de Derechos Humanos, comprende el derecho de buscar, recibir y difundir informaciones e ideas de todo tipo y sin ningún tipo de fronteras. Este derecho comprende la expresión artística, escrita, oral, impresa o por cualquier otro medio de comunicación. Las reglas para imponer limitaciones a este derecho se encuentran en los incisos 2 al 5 de dicho artículo. Dentro de dichas reglas se destaca que no podrá existir censura previa, si no la imposición de responsabilidad con posterioridad a que se realice la expresión.

¹ Disponible en: https://www.oas.org/es/cidh/expresion/docs/publicaciones/internet_2016_esp.pdf.

² CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013. Párr. 36.

Como principio general, “la libertad de expresión se aplica a internet del mismo modo que a todos los medios de comunicación”.³ Esto implica que cualquier restricción al ejercicio de este derecho en internet debe seguir los estándares establecidos en el derecho internacional de los derechos humanos, como se analiza más adelante en este capítulo. En particular, la Relatoría Especial ha enfatizado que, al momento de establecer medidas que puedan impactar a Internet, se deben tener en cuenta las características que hacen de ese medio un espacio único para el ejercicio cada vez más democrático, abierto, plural y expansivo de la libertad de expresión.⁴

Para la Relatoría Especial para la Libertad de Expresión de la CIDH, Internet es un instrumento único para el despliegue de los derechos humanos, especialmente la libertad de expresión. La creciente expansión de este medio en el mundo y en las Américas ha traído, además de mejores oportunidades para el ejercicio de esos derechos, beneficios sociales e inclusión. El debido desarrollo de estos beneficios depende de políticas y prácticas que se fundamenten en el respeto y garantía de los derechos humanos. Dentro de estos últimos, la libertad de expresión juega un rol especial, pues habilita el ejercicio de otros derechos.

El Sistema Interamericano de Derechos Humanos es el sistema internacional que ha brindado un mayor alcance a la libertad de pensamiento y expresión. Esto ha sido posible bajo un marco jurídico que busca reducir las restricciones a la libre circulación de informaciones, opiniones e ideas. De acuerdo a los instrumentos interamericanos, la libertad de expresión es la “piedra angular” de las sociedades democráticas, además de ser fundamental para el avance de los objetivos del desarrollo y una herramienta para el ejercicio de otros derechos humanos.

La CIDH ha destacado tres funciones principales que cumple la libertad de expresión en los sistemas democráticos: 1. Es un derecho individual que refleja la virtud de pensar el mundo de una forma propia y comunicarse entre sí; 2. Como medio para deliberar de forma abierta y desinhibida sobre temas que sean de interés público; 3. Como instrumento para el ejercicio de otros derechos, como la participación política, la libertad religiosa, la cultura, la educación, la igualdad, entre otros. Complementariamente, tanto la CIDH como la Corte Interamericana han reconocido que la libertad de expresión cuenta con una dimensión individual y una social, interrelacionadas entre sí. La garantía de ambas dimensiones debe ser plena y simultánea.

El Sistema Interamericano también otorga una protección amplia al tono de las expresiones. En este entendido, las expresiones inofensivas o indiferentes son protegidas al igual que aquellas que “ofenden, chocan, inquietan, resultan ingratas o perturban al Estado o a cualquier sector de la población”. Adicionalmente, la emisión de discursos erróneos, equivocados y falsos, sin perjuicio de las responsabilidades que se impongan con posterioridad, son protegidos por la libertad de expresión en el Sistema Interamericano. Complementariamente, los Estados deben mantener una posición neutral frente a los contenidos de las expresiones, de forma que no existan exclusiones de personas, grupos, ideas o medios de expresión.

La jurisprudencia ha reconocido la existencia de tres tipos de expresiones que, dado su valor dentro del sistema democrático, deben tener una mayor protección: (a) el discurso político y sobre asuntos de interés público; (b) el discurso sobre funcionarios públicos en ejercicio de sus funciones y sobre candidatos a ocupar cargos públicos; y (c) el discurso que configura un elemento de la identidad o la dignidad personales de quien se expresa⁵.

Con relación a las limitaciones permisibles a la libertad de expresión, la jurisprudencia de la Corte Interamericana ha desarrollado un “test tripartito” fundamentado en el artículo 13 de la Convención Americana. Este test exige 1) Que la limitación a imponerse esté definida de forma clara y precisa en una ley formal y material que esté orientada a lograr objetivos imperiosos que estén autorizados por la Convención;

³ Declaración conjunta sobre libertad de expresión en internet, 1 de junio de 2011. Disponible en:

<https://www.oas.org/es/cidh/expresion/showarticle.asp?artID=849&IID=2>.

⁴ CIDH. Informe Anual 2013. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo IV (Libertad de Expresión e Internet). OEA/Ser.L/V/II.149. Doc. 50. 31 de diciembre de 2013.

⁵ CIDH. Informe Anual 2008. Informe de la Relatoría Especial para la Libertad de Expresión. Capítulo III (Marco Jurídico Interamericano del Derecho a la Libertad de Expresión). OEA/Ser.L/V/II.134 Doc. 5 rev. 1. 25 de febrero de 2009. Párr. 232.

2) que la limitación cumpla con unos requisitos de necesidad e idoneidad para lograr esos objetivos y; 3) que la limitación sea estrictamente proporcional a la finalidad que se persigue. Por último, las responsabilidades que se establezcan con posterioridad a las expresiones siempre deben ser ordenadas por un juez o autoridad jurisdiccional independiente e imparcial, junto con las garantías del debido proceso.

Como efecto de lo anterior, la Relatoría ha enfatizado que el desarrollo de políticas públicas y las actuaciones de los particulares deben adecuarse a los principios de acceso a Internet en igualdad de condiciones, la promoción del pluralismo, la no discriminación y la privacidad, así como la neutralidad de la red y la gobernanza multisectorial como componentes transversales de estos principios.

3. Estándares para un internet libre, abierta e incluyente

La relevancia de internet para el goce y ejercicio de derechos humanos depende directamente de la arquitectura de la red y de los principios que la rigen: apertura, descentralización y neutralidad. Estas características especiales deben ser tenidas en cuenta al momento de establecer cualquier medida que pueda impactar la internet.

La labor del Estado, el desarrollo de políticas públicas y la actuación de los particulares en el entorno digital, deben adecuarse entonces a los siguientes principios orientadores: la protección de un internet libre y abierto; el acceso universal y plural; la igualdad y no discriminación; la protección de la privacidad y la gobernanza multisectorial.

A continuación se desarrollan los aspectos esenciales de los principios rectores propuestos:

A. Internet libre y abierto: la neutralidad de la red

El principio de neutralidad de la red es una condición necesaria para ejercer la libertad de expresión en internet. También posibilita la innovación y generación de contenidos, aplicaciones y servicios de manera descentralizada, sin mediar autorizaciones, licencias o permisos. Según este principio –que permite maximizar la utilidad de las redes– todos los paquetes de datos deben ser tratados de forma igualitaria y sin distinción alguna.

De ahí que internet se describa como una red ‘boba’ cuya especialización (‘inteligencia’) se genera en los extremos. La plataforma o aplicación opera en un extremo de la red, y sus contenidos se trasladan por la red divididos en paquetes de datos sin ser discriminados. Tales paquetes se rearmen nuevamente en el destino en función del destinatario, la plataforma o aplicación que utilizan.

El tratamiento de datos y tráfico en internet no debe ser objeto de discriminación según la fuente y el contenido. La neutralidad de la red garantiza la libertad de acceso y elección de los usuarios. Permite que éstos puedan enviar y recibir información u ofrecer cualquier contenido, aplicación o servicio legal por medio de internet sin condicionamientos ni discriminación, bloqueo, filtración o interferencia.

Los Estados deben garantizar la vigencia de este principio a través de legislaciones adecuadas. Varios países de la región ya han adoptado leyes que consagran el principio de neutralidad de la red, entre ellos, Argentina, Brasil, Chile y México. Por su parte, la Comisión Nacional de Telecomunicaciones de Paraguay refrendó el principio de neutralidad de la red, y la Comisión Federal de Comunicaciones en Estados Unidos (FCC por sus siglas en inglés) también hizo lo propio.

El principio de neutralidad de red puede estar sujeto a excepciones. No debe haber discriminación, restricción, bloqueo o interferencia en la transmisión del tráfico de internet, a menos que sea necesario y proporcional para garantizar la integridad y seguridad de la red, o para prevenir la transmisiones de contenidos no deseados expresamente por el usuario. Aún en el caso de congestiones o problemas técnicos, las medidas no deben discriminar aplicaciones o servicios.

La transparencia en la gestión de la red resulta fundamental para garantizar el principio de neutralidad de la red. Los Estados deben exigirles a los intermediarios de internet que sean transparentes frente a las prácticas que emplean en la gestión del tráfico de datos. Esta información debe estar a disposición de los usuarios en un formato asequible.

Desde 2015 surgió un debate relacionado con la neutralidad de la red, y es la oferta de planes internet de 'tarifa cero' –conocidos como *zero rating*–. Mediante estos planes, diseñados principalmente para el servicio de internet móvil, las compañías ofrecen el acceso a determinadas aplicaciones sin que constituya un gasto en el plan de datos del usuario. Existen planes de *zero rating* en distintos países de la región como Chile, Colombia, Brasil, Ecuador, Panamá y Paraguay.

Aunque la doctrina está dividida frente al impacto de los planes de *zero rating* en la neutralidad de la red, cabe hacer dos consideraciones: por una parte, las políticas de *zero rating* deberán evaluarse a la luz de la regulación de cada Estado y, en particular, de la neutralidad de la red. Los Estados que permitan la oferta de planes de *zero rating* deberán monitorear su funcionalidad y evaluar periódicamente su compatibilidad con los derechos humanos.

Por otra parte, en ningún caso los Estados podrán reemplazar sus políticas de acceso universal a internet por políticas o planes de *zero rating*. La simple sustitución de las políticas de acceso por ese tipo de programas es incompatible con los objetivos de desarrollo de las Naciones Unidas y con la obligación de los Estados de promover y proteger los derechos humanos en internet.

B. Acceso universal y pluralismo

El acceso a internet constituye una condición *sine qua non* para el ejercicio efectivo de los derechos humanos hoy en día, especialmente de los derechos a la libertad de expresión y opinión, asociación y reunión, educación, salud y cultura. El acceso a internet debe garantizarse universalmente a través de medidas que cierren la brecha digital y políticas de desarrollo de infraestructura.

A pesar de los compromisos y esfuerzos de los Estados en la región, actualmente en las Américas un tercio de la población se encuentra sin conexión a internet. Esta falta de acceso incrementa la vulnerabilidad y profundiza la desigualdad, con lo cual se perpetúa la exclusión de muchas personas. Si además de lo anterior, la transición digital de los servicios de radiodifusión se realiza sin asegurar el acceso a este tipo de servicios, las comunidades pobres, aisladas y remotas pueden verse doblemente perjudicadas.

La Relatoría estima que ampliar el acceso y cerrar la brecha digital va de la mano con la necesidad de que el Estado procure que los actores privados no impongan barreras desproporcionadas o arbitrarias para acceder a internet o usar sus servicios principales. La interrupción del acceso a internet a poblaciones –enteras o segmentos de éstas– nunca está justificada, ni siquiera por razones de seguridad nacional. Los bloqueos temporales o parciales afectan el ejercicio de los derechos humanos en línea.

El pluralismo y la diversidad son condiciones esenciales del proceso de deliberación pública y del ejercicio de la libertad de expresión, y deben ser preservados en el entorno digital. Esto implica asegurar que no se introduzcan en la red cambios que tengan como consecuencia la reducción de voces y contenidos.

Los Estados deben desarrollar planes y políticas públicas a largo plazo con el fin de desarrollar la infraestructura física necesaria para evitar la exclusión arbitraria de determinados sectores, y elaborar planes de banda ancha y medidas que permitan el desarrollo del internet móvil.

C. Alfabetización digital

La alfabetización digital se refiere al conjunto de destrezas, conocimientos y actitudes que necesita una persona para desenvolverse funcionalmente dentro de la sociedad de la información. El objetivo último es que puedan “*utilizar la tecnología de manera efectiva, desarrollando nuevas oportunidades sociales y económicas en el marco de su sociedad*”.⁶

Las diferencias en las capacidades para usar las tecnologías de la información constituyen una brecha en el conocimiento. La alfabetización digital es un proceso de fundamental importancia en la garantía de los derechos humanos, y una medida particularmente necesaria para proteger y garantizar los derechos a la igualdad y no discriminación.

Los Estados deben entonces promover y asegurar la participación de todos los sectores de la sociedad en el diseño e implementación de políticas eficaces y concretas sobre alfabetización digital. En particular, los Estados deben adoptar un doble enfoque. Primero, responder a las características y necesidades de quienes buscan y reciben información, bienes y servicios. Segundo, atender a quienes ofrecen, producen, administran o disponen de esa información, bienes o servicios.

D. Pluralidad lingüística

La pluralidad lingüística es una condición necesaria para lograr un acceso pleno a internet en condiciones de igualdad y sin discriminación. El plurilingüismo, además, esta intrínsecamente vinculado con la creación de contenidos locales, lo cual es necesario para la universalidad de internet. Como señaló la Corte Interamericana, el derecho a la libertad de expresión implica que las personas elijan el idioma en el que quieren expresarse.

Para Relatora Especial sobre derechos culturales de Naciones Unidas, “*la distribución sumamente desigual de las obras literarias publicadas en diferentes idiomas supone una barrera importante para el derecho a participar en la vida cultural de las comunidades lingüísticas sin un mercado editorial importante*”.⁷ Si bien existen servicios de traducción en línea que han sido perfeccionados en los últimos años, no constituyen soluciones efectivas a este problema.

En el desarrollo de la sociedad del conocimiento, debe priorizarse la creación, difusión, preservación y accesibilidad de contenido en varios idiomas y formatos sobre todos los temas –en especial científicos, educativos y culturales–. La traducción de sitios web en varios idiomas es un paso adelante para garantizar una sociedad verdaderamente global.

E. Igualdad y no discriminación

Además de las consideraciones en materia de acceso universal, los Estados también deben adoptar medidas de diferenciación positiva para permitir el goce efectivo de este derecho a personas o comunidades que así lo requieran por sus circunstancias de marginación, vulnerabilidad o discriminación. Esto incluye, entre otros, acceso a centros tecnológicos para algunas comunidades, estructuras de precios inclusivas y esfuerzos de capacitación en sectores pobres rurales y entre la población mayor.

Los Estados deben promover y garantizar, por ejemplo, la plena participación de las mujeres en la sociedad del conocimiento, incluyendo los procesos de adopción de decisiones. Los Estados deben tomar medidas proactivas para combatir la brecha de género en internet y en todos los aspectos que hacen a su gobernanza.

De la misma manera, tal y como establece la Convención sobre los Derechos de las Personas con Discapacidad (CDPD), los Estados deben adoptar medidas que les garanticen a las personas con discapacidad el acceso en

⁶ Organización Panamericana de la Salud. Conversaciones sobre Salud. Gestión de información, diálogos e intercambio de conocimientos para acercarnos al acceso universal a la salud. Washington DC, 2014.

⁷ Naciones Unidas. Consejo de Derechos Humanos. Informe de la Relatora Especial sobre los derechos culturales, Farida Shaheed. UN Doc. A/HRC/28/57. 24 de diciembre de 2014. Párr. 68.

igualdad de condiciones a la información y las comunicaciones. Esto abarca, por supuesto, el acceso y disfrute de internet y de los sistemas y las tecnologías de la información y las comunicaciones.

El acceso a internet es particularmente importante para las personas en situación de vulnerabilidad. Sin acceso a internet, las personas en situación de pobreza extrema corren el riesgo de quedar marginadas. Internet debe ser un medio para que estos grupos desfavorecidos difundan sus opiniones y sus problemas, a fin de no quedar excluidas de los debates públicos y poder gozar plenamente de sus derechos humanos.

La obligación de igualdad y no discriminación también implica la obligación del Estado de garantizar a las personas el ejercicio de los derechos humanos tanto en el contexto 'online' como en el 'offline'. En el entorno digital, de la misma forma como en el entorno físico, las personas tienen derecho a ejercer sus derechos de reunión, asociación, libertad de expresión, acceso a la información, libertad de religión, entre otros, sin discriminación.

Lamentablemente se han documentado instancias de discriminación en línea en detrimento de grupos particularmente vulnerables, incluyendo mujeres, niños, la comunidad LGBTI, migrantes y personas con discapacidad, entre otros. Los Estados deben adoptar medidas para promover la igualdad y la no discriminación, prohibiendo el discurso de odio que incite a la violencia, documentando las instancias de discriminación y promoviendo la tolerancia a través de programas sociales de capacitación y educación.

F. Privacidad

La Relatoría Especial ha subrayado que el respecto a la privacidad debe ser también un principio orientador del entorno digital. El derecho a la privacidad, según el cual nadie puede ser objeto de injerencias arbitrarias o abusivas en su vida privada, en la de su familia, en su domicilio o en su correspondencia, es un presupuesto del ejercicio del derecho a la libertad de expresión en línea. La vulneración de la privacidad de las comunicaciones tiene un efecto inhibitorio y afecta el pleno ejercicio del derecho a comunicarse. Por lo tanto, este derecho debe ser protegido por la ley y estrictamente promovido mediante políticas públicas.

Por tratarse de un asunto transversal, el último capítulo de este documento desarrolla en detalle la protección de la privacidad en internet.

E. Gobernanza multisectorial

Si bien internet ha sido desarrollado y operado por una serie de empresas privadas que desempeñan diferentes funciones, su carácter de medio de comunicación global lo hace un espacio público. Por lo tanto, la gobernanza de internet debe ser ejercida bajo los principios de un recurso público y no simplemente como un asunto de contratos privados.

La gobernanza de internet se define como *“el desarrollo y aplicación por los gobiernos, el sector privado y la sociedad civil, en el desempeño de sus respectivos papeles, de principios, normas, reglas, procedimientos de toma de decisiones y programas comunes que dan forma a la evolución y a la utilización de internet”*.⁸ Debe ser transparente, multisectorial y democrática, y la participación de los Estados debe ser equilibrada.

La cooperación de los múltiples interesados implica la verdadera participación de gobiernos, sociedad civil, organizaciones internacionales, comunidad técnica y comunidad académica. Este proceso debe darse también a nivel local, y contar con mecanismo de transparencia y medición de impacto.

⁸ Cumbre Mundial sobre la Sociedad de la Información. [Agenda de Túnez para la Sociedad de la Información](#). Doc. WSIS-05/TUNIS/DOC/6(Rev.1)-S. 28 de junio de 2006. Párr. 34.

4. El rol del sector privado

Internet depende en gran medida de entidades privadas que ofrecen diferentes servicios: facilitan la conexión; diseñan y mantienen el *hardware* y los sistemas operativos que permiten el procesamiento de información; asignan los dominios web; alojan información; facilitan la agregación, repartición y búsqueda de información; producen y regulan el acceso al contenido creado por los usuarios; conectan usuarios y comunidades; venden bienes y servicios y facilitan transacciones, y recolectan y venden datos, entre otros. Las entidades privadas han pasado a ejercer un rol sin precedentes como mediadores del derecho a la libertad de expresión y acceso a la información. En suma, internet es un ámbito público basado en una serie de plataformas privadas.

Si bien los Estados son los principales titulares de las obligaciones en materia de derechos humanos, las empresas y organizaciones privadas también son responsables del respeto de los derechos y libertades fundamentales. El Consejo de Derechos Humanos de Naciones Unidas adoptó en 2011 los Principios Rectores sobre las empresas y los derechos humanos donde se establece que las empresas deben abstenerse de afectar los derechos humanos de terceros y reparar las violaciones en las que tengan una participación directa o indirecta.

Los actores privados deben asumir un compromiso formal y de alto nivel con medidas y sistemas internos concretos, diseñados para prevenir actividades que pueden generar impactos negativos. En particular, en el diseño y conformación de los términos de servicio y reglas comunitarias, las empresas no deben limitar o restringir la libertad de expresión de manera desproporcionada o innecesaria. Igualmente, deben establecer sistemas asequibles y eficaces de denuncia y mecanismos de vigilancia y evaluación de impacto para identificar los daños reales o potenciales a los derechos humanos causados por sus servicios o actividades.

Los Estados, en tanto responsables últimos de proteger y respetar el derecho a la libertad de opinión y expresión, no deben requerir ni presionar a las entidades privadas para que violen los derechos humanos o interfieran de forma desproporcionada e innecesaria en la libertad de expresión. Al contrario, están llamados a fomentar el desarrollo del sector privado y de medidas técnicas, productos y servicios que protejan la libertad de expresión.

A. Responsabilidad de intermediarios

La transmisión de contenidos en internet depende de los intermediarios. En términos generales, los intermediarios son *“cualquier entidad que permita la comunicación de información de una parte hacia otra”*.⁹ Sin embargo, la definición legal de ‘intermediario’ puede ser distinta entre jurisdicciones o entre países. Para efectos prácticos, son intermediarios los proveedores de servicios de internet, los motores de búsqueda, los servicios de blogs, las plataformas de comercio electrónico, los servidores web y las redes sociales, entre otros.

Una de las medidas que más directamente puede afectar la actuación de los intermediarios en internet es el régimen de responsabilidad que legalmente se les imponga por contenidos de terceros. El régimen de responsabilidad es fundamental para generar los incentivos adecuados para la protección y garantía de los derechos humanos. En todos los casos el régimen de responsabilidad debe seguir el test tripartito de legalidad, necesidad y proporcionalidad, establecido por el sistema interamericano de derechos humanos.

Ningún actor que se limite a ofrecer servicios técnicos de internet como acceso, búsquedas o conservación de información en la memoria caché, debe ser responsable por los contenidos generados por terceros que se difunden o almacenan en sus servicios. Lo anterior se aplica, siempre que el intermediario no intervenga en dichos contenidos o se niegue a cumplir una orden judicial cuando esté en condiciones de hacerlo. En el

⁹ UNESCO. [Fostering Freedom Online: The role of internet Intermediaries](#). Unesco Series on internet Freedom. internet Society (2014). Pág. 19.

mismo sentido, las responsabilidades posteriores deben ser impuestas sobre los autores de la expresión y no sobre los intermediarios.

La responsabilidad objetiva o ‘estricta’ que responsabiliza al intermediario por cualquier contenido considerado ilícito en su plataforma, es incompatible con la Convención Americana por ser desproporcionada e innecesaria en una sociedad democrática. Este tipo de regímenes promueve el monitoreo y la censura de los intermediarios para con sus propios usuarios.

En cambio, los sistemas de responsabilidad condicionada se alinean en mayor medida con los estándares internacionales, siempre que cumplan con los principios de necesidad y proporcionalidad. Bajo la responsabilidad condicionada, se ofrece al intermediario un ‘puerto seguro’ a salvo de cualquier responsabilidad legal siempre y cuando cumpla con ciertos deberes concretos.

Estos regímenes incluyen los sistemas de ‘notificación y retiro’, en el marco del cual el intermediario deberá retirar el contenido una vez notificado de su existencia; el sistema de ‘notificación y notificación’, en el cual el intermediario deberá notificar al autor de cualquier denuncia recibida respecto a sus contenidos, y el sistema de ‘notificación y desconexión’, en el cual el intermediario desconectará al usuario cuando luego de notificarlo aquel no tome medidas para remover el contenido denunciado.

Estos modelos de responsabilidad condicionada no imponen un deber de monitoreo o filtrado de contenidos en forma proactiva. Sin embargo, no siempre respetan el derecho al debido proceso y garantías mínimas, en tanto trasladan al intermediario la responsabilidad estatal de analizar y decidir sobre la licitud o ilicitud del contenido susceptible de remoción. Para la Relatoría Especial, estos modelos serán compatibles con la Convención Americana en la medida en que protejan la libertad de expresión y no impongan obligaciones ambiguas o desproporcionadas.

Los Principios de Manila sobre Responsabilidad de los Intermediarios, propuestos por organizaciones de la sociedad civil de todo el mundo, proponen un marco de referencia de garantías mínimas y buenas prácticas para los Estados en materia de responsabilidad de intermediarios sobre la base de los instrumentos internacionales sobre derechos humanos.

A través de la autorregulación y la co-regulación, los intermediarios deben comprometerse con el respeto y promoción de la libertad de expresión y actuar con transparencia. Es de suma importancia que proporcionen información clara sobre el tipo de contenidos que pueden ser removidos de la plataforma según sus términos de servicio o directrices comunitarias. Igualmente importante es señalar claramente cómo funciona esta remoción y qué mecanismos tiene el usuario para cuestionar la eliminación equivocada de su contenido.

Conviene destacar que teniendo en cuenta el alcance global y transnacional de internet, los Estados deben aspirar a lograr uniformidad en las normas que rigen la responsabilidad de intermediarios como un aspecto fundamental para mantener un internet libre, abierto y global. Al momento de dirimir cuestiones de responsabilidad, los jueces competentes deberían ser aquellos que cuenten con los contactos ‘más estrechos’ con el caso, atendiendo a donde reside el damnificado, donde se originó el contenido, o donde reside su autor. Los jueces tienen la responsabilidad de evitar lo que se conoce como ‘turismo de difamación’ o *forum-shopping*, declarándose incompetentes cuando no exista un perjuicio sustancial demostrable en su jurisdicción.

Esta cuestión se ha planteado reiteradamente en las decisiones judiciales relativas al denominado ‘derecho al olvido’ (véase más adelante), en las que un juez de un país ordena la dexindexación de un resultado de búsqueda específico no sólo de la plataforma vinculada a la jurisdicción competente, sino también de otros países (o incluso globalmente). Esto podría dar lugar a una aplicación extraterritorial de una orden judicial nacional y plantea cuestiones complejas sobre el futuro de la jurisdicción en internet y su interacción con la soberanía nacional.

B. El discurso de odio en internet

Solo a través de una política comprensiva y sostenida, que exceda las medidas legales e incluya mecanismos de prevención y educación, podrá combatirse efectivamente el discurso de odio y garantizarse el derecho a la igualdad y no discriminación de las personas tanto en internet como en el entorno físico.

Para combatir este grave problema en Internet, los Estados no deben tomar medidas especialmente restrictivas de la libertad de expresión en internet. Las medidas de bloqueo o filtrado de contenidos tendientes a combatir el discurso de odio son medidas de *ultima ratio*, y solamente deben adoptarse cuando sean necesarias y proporcionales con la finalidad imperativa que persiguen. Los Estados que adopten estas medidas deben además diseñarlas de forma tal que no alcancen discursos legítimos que merezcan protección.

Unesco destaca como medidas adecuadas y pertinentes contra el discurso de odio, la alfabetización digital, el acceso universal y la promoción de técnicas como las contra-narrativas (o *counter-speech*). El propósito es enseñar a las personas a detectar el discurso de odio y contrarrestarlo mediante discursos tolerantes y anti-discriminatorios.

C. La remoción y desindexación de contenidos: el derecho al olvido

La Relatoría Especial ha advertido sobre el impacto que pueden tener en el ejercicio del derecho a la libertad de expresión –en su dimensión individual y colectiva– las medidas de remoción o desindexación de contenidos de internet que realizan los intermediarios, ya sea por iniciativa propia o como consecuencia de una orden de los Estados.

A raíz de la decisión de 2014 adoptada por el Tribunal de Justicia de la Unión Europea (TJUE) –conocido como el ‘caso Costeja’– surgió un nuevo debate sobre la legitimidad de las medidas de remoción y desindexación de contenidos en línea y la adecuada ponderación de los límites entre el derecho a la privacidad y el derecho a la libertad de expresión e información en internet. La decisión –que dio origen a un denominado ‘derecho al olvido’– reconoce una eventual posibilidad de desindexación limitada a la información enlistada o vinculada directamente con el nombre propio de la persona física.

Con base en esta doctrina y en las normas de protección de datos personales en América Latina, en la región se han registrado solicitudes de remoción y desindexación de contenidos a las empresas administradoras de motores de búsqueda. También se han documentado solicitudes que expanden significativamente el concepto del ‘derecho al olvido’ para exigir a periódicos, blogs y periodistas la remoción o eliminación de contenidos en lugar de su desindexación.

Organizaciones de la sociedad civil también han denunciado que funcionarios públicos de diversos países están utilizando el ‘derecho al olvido’ para restringir la circulación de información de interés público. En muchos casos, han optado por reemplazar acciones de calumnias e injurias ante los tribunales por acciones de oposición ante la autoridad de protección de datos personales.

Sobre el particular, es necesario hacer las siguientes consideraciones:

- El derecho internacional de los derechos humanos no protege o reconoce el llamado ‘derecho al olvido’ en los términos delineados por el TJUE. Por el contrario, su aplicación en las Américas resulta particularmente problemática a la luz de la protección de la libertad de expresión del artículo 13 de la Convención Americana sobre Derechos Humanos.
- La remoción de contenidos en internet tiene un impacto evidente en el derecho a la libertad de expresión, tanto en su dimensión individual como social, y en el derecho de acceso a la información por parte del público.

- En las Américas las personas y organizaciones de la sociedad civil mantienen un legítimo reclamo de mayor acceso a información sobre la actividad gubernamental, sobre el autoritarismo del pasado y las graves violaciones de los derechos humanos. Es importante reconocer el contexto particular de la región y cómo un mecanismo legal como el llamado ‘derecho al olvido’ y su incentivo para la desindexación puede afectar el derecho a la verdad y a la memoria.
- Si bien la protección de datos personales constituye un objetivo legítimo, en ningún momento puede ser invocada para limitar o restringir la circulación de información de interés público, sobre funcionarios o personas públicas, o candidatos en el ejercicio de sus funciones, o que involucran violaciones de derechos humanos.
- Los funcionarios públicos están sujetos a un mayor escrutinio por parte de la sociedad. Debe existir una fuerte presunción en contra de solicitudes de desindexación o cancelación de información presentadas por funcionarios públicos, personas públicas, o candidatos a ejercer cargos públicos.
- Esto es particularmente relevante en relación con la información producida y divulgada por los medios de comunicación que utilizan internet. La protección de datos personales a la que se refiere el derecho al olvido no puede conllevar restricciones a la información divulgada por los medios de comunicación que puedan eventualmente afectar los derechos a la privacidad y la reputación de una persona.
- Las plataformas digitales de los medios informativos no son controladores de datos personales, sino fuentes públicas de información y plataformas para la transmisión de informaciones, opiniones e ideas sobre temas de interés público, y como tal no pueden ser susceptibles de una orden de desindexación, ni tampoco la supresión de un contenido en línea de interés público.
- Los procedimientos de desindexación o cancelación de contenidos no pueden utilizarse como un mecanismo preventivo o cautelar para proteger el honor o la reputación. Para eso existen acciones específicas.

En conclusión, la legislación sobre desindexación deberá quedar restringida a aquellos casos en que el solicitante demuestre un daño sustantivo a la privacidad y la dignidad y siempre a través de una orden judicial adoptada en el marco de un proceso respetuoso del debido proceso y en el que puedan ejercer su defensa todas las partes involucradas, incluyendo quien se expresa, el medio de comunicación o editor del sitio web que pudiera verse afectado, y los intermediarios.

La transparencia en torno a las políticas de desindexación practicadas por tanto entidades privadas como por organismos estatales (incluidas las autoridades de aplicación de las leyes de privacidad o el poder judicial) es de fundamental importancia.

D. Propiedad intelectual y el acceso al conocimiento

El propósito de la propiedad intelectual es *“la promoción de la creatividad literaria, musical y artística, el enriquecimiento del patrimonio cultural y la difusión de los bienes del conocimiento y de la información al público general”*.¹⁰ No obstante, debe haber un equilibrio entre el reconocimiento y la recompensa a la creatividad humana y la posibilidad de que el público acceda a esas creaciones.

¹⁰ Article 19. El Derecho a Compartir: Principios de la Libertad de Expresión y los derechos de propiedad intelectual en la Era Digital (2013). Pág. 11.

La protección de los derechos de autor tiene un fin legítimo que podría llevar a la imposición de limitaciones a los derechos humanos a la educación, la cultura y la libertad de expresión. Sin embargo, la protección de estos derechos no podría implementarse de una forma en la que desaliente la creatividad o el libre intercambio de información e ideas en internet.

En años recientes se han promovido distintas iniciativas tendientes a promover licencias abiertas y la adopción de excepciones en los regímenes de derechos de autor existentes. La Relatora Especial sobre derecho a la cultura de Naciones Unidas recomendó la adopción de excepciones –como el *fair use*– vinculada a la información y el debate político; y usos no remunerados de material afectado por derecho de autor para escuelas y bibliotecas, con el fin de promover un mejor balance entre los derechos culturales y los derechos de propiedad intelectual.

Los Estados deben prestar particular atención a la adecuación de las medidas requeridas por los tratados internacionales con las necesidades locales y con la protección de los derechos de los usuarios de internet. La especial naturaleza de estos acuerdos y su proceso de negociación, generalmente secreta, en muchos casos carece del control, transparencia y participación social, necesarios para legislar legítimamente en materia de excepciones a la libertad de expresión y al derecho a la cultura.

E. Iniciativas de Acceso Abierto

El acceso abierto es una forma de diseminar el conocimiento para obtener el máximo beneficio para la ciencia y la sociedad mediante la publicación en internet en forma pública y gratuita de literatura académica y científica, desprovista de barreras técnicas, económicas y legales, y con la posibilidad de usarla, copiarla y compartirla. Las contribuciones de acceso abierto incluyen los resultados de la investigación científica original, datos primarios y metadatos, materiales, fuentes, representaciones digitales de materiales gráficos y pictóricos, y materiales eruditos en multimedia.

La Relatora sobre derechos culturales de Naciones Unidas destacó la importancia y el potencial de las licencias abiertas sobre todo en la construcción y difusión del conocimiento científico y académico. Es importante que los Estados difundan y promuevan la capacitación y la adopción de licencias de acceso abierto, particularmente entre las comunidades académicas y científicas así como entre quienes mantienen el patrimonio cultural.

F. Protección del dominio público

El dominio público es *“la suma neta de la totalidad de información y de bienes culturales que no es objeto de los derechos de propiedad intelectual y que el público general puede aprovechar e intercambiar sin restricción alguna. Forma parte del patrimonio cultural de toda la humanidad que se debe preservar”*.¹¹

Un dominio público rico es un factor esencial para el crecimiento de la Sociedad de la Información, en tanto fomenta y promueve la diversificación del público instruido, generando con ello nuevos empleos, innovación, oportunidades comerciales y el avance de las ciencias. La información del dominio público debe ser fácilmente accesible y debe estar protegida de toda apropiación indebida. Los Estados deben fortalecer, proteger y promover las instituciones públicas –tales como museos y bibliotecas– y la preservación de documentos y archivos públicos.

Siendo tan importante el aporte de materiales existentes para el desarrollo de nuevas obras, el plazo de protección del derecho a la propiedad intelectual no debería prolongarse más que el tiempo necesario para lograr su propósito sin perjudicar la libertad de expresión.

¹¹ Article 19. El Derecho a Compartir: Principios de la Libertad de Expresión y los derechos de propiedad intelectual en la Era Digital (2013). Parr.13.

El patrimonio digital también hace parte del acervo público y ha de ser protegido y conservado para las generaciones futuras. Los Estados deben desarrollar mecanismos y políticas para preservarlo, y poner a disposición de cualquier persona el patrimonio digital de todas las regiones, naciones y comunidades con fin de propiciar, con el tiempo, una representación de todos los pueblos, naciones, culturas e idiomas.

G. Restricciones y limitaciones al derecho a la libertad de expresión y acceso al conocimiento en relación con la protección de derechos de autor

Las restricciones al derecho a la libertad de expresión y acceso al conocimiento en internet en virtud de la protección de derechos de autor deben cumplir con los requisitos establecidos en la Convención Americana, ya mencionados en este informe.

La desconexión de usuarios como sanción por violaciones al derecho de autor constituye una medida desproporcionada y radical incompatible con el derecho internacional de los derechos humanos, incluso cuando se trata de mecanismos graduados (como el sistema que prevé la desconexión de internet luego de tres infracciones o *strikes*). El bloqueo obligatorio de sitios enteros también constituye una medida desproporcionada e incompatible con la protección de los derechos humanos en línea, tal y como señaló este informe anteriormente.

Además de las pruebas de proporcionalidad y el impacto que tales bloqueos pueden tener sobre la libertad de expresión, es importante destacar la ineficacia de este tipo de medidas. Es necesario optar y promover la adopción de enfoques alternativos.

Por otra parte, la responsabilidad penal por infracciones no comerciales al derecho de propiedad intelectual constituye una interferencia desproporcionada de la libertad de expresión. Este tipo de medidas inhiben la libre circulación de información e ideas. Además, en ningún caso estos delitos deben contemplar penas más rigurosas que aquellos perpetrados en el contexto ‘offline’.

5. Protección de la privacidad

Los Estados tienen la obligación de respetar y proteger el derecho a la privacidad en la era digital, y en esa medida deben adaptar su legislación a los retos que presenta el desarrollo de Internet.

Con internet, la capacidad técnica para reunir, almacenar e intercambiar información personal que brindan las tecnologías digitales generó un nuevo desafío en la protección de la privacidad. Las empresas de redes sociales se basan en un modelo de negocios que ofrecen servicios ‘gratuitos’ a cambio de la propiedad de los datos que generen los usuarios, y ello necesariamente implica la generación de datos y ‘rastros digitales’.

Esto complica el derecho de las personas a determinar cuándo, cómo y en qué medida se comparte la información sobre ellas mismas. El creciente poder de procesamiento de las computadoras permite recabar información desde múltiples fuentes, procesar y re-procesar para luego venderse. Es claro que el modelo de negocios de las empresas más exitosas incide directamente sobre el derecho a la privacidad.

Las nuevas tecnologías también crean la posibilidad de localizar y rastrear datos personales, algo que antes no era posible. Cada computadora, teléfono móvil u otro dispositivo conectado a internet tiene una dirección única (dirección IP) que le proporciona un identificador específico al dispositivo y posibilita su rastreo. Los sistemas GPS, adicionalmente, permiten rastrear a través de distintas aplicaciones la ubicación exacta de una persona. Por otra parte, existen diversas herramientas para extraer información personal del usuario o que permite identificarlo –como las *cookies* y los *web bugs* o *beacons*–.

El informe de la Relatoría Especial desarrolla cinco desafíos relacionados con la privacidad en el entorno digital.

A. Datos personales

En América Latina en general se ha adoptado una noción amplia de datos personales, que incluye cualquier dato propio de personas físicas o jurídicas, identificadas o identificables. Resulta fundamental que se desarrollen regímenes de protección de datos que regulen el almacenamiento, procesamiento, uso y transferencia de datos personales, ya sea entre entidades estatales o entre terceros. Debido a la naturaleza transfronteriza de internet, la necesidad de regular el tratamiento de datos no se limita al ámbito nacional.

Los Estados deben adoptar políticas tendientes a regular el tratamiento de datos, incluido el almacenamiento, análisis, y divulgación de datos personales salvo cuando estén legitimados para hacerlo o exista consentimiento informado de la persona afectada. Además, deben adoptar medidas positivas tendientes a educar a las personas en torno a sus derechos y para entender las condiciones legales para el tratamiento de datos personales (recolección, almacenamiento, tratamiento o divulgación de datos).

Los Estados deben garantizar una política de transparencia respecto a la legislación aplicable al manejo de datos tanto por parte del estado como del sector privado. Las prácticas en torno a su tratamiento, los procedimientos para cuestionar dicho tratamiento y la autoridad competente para resolver cualquier planteo. Resulta fundamental que las personas puedan acceder a la información almacenada sobre sí mismas, actualizarla, corregirla y, llegado el caso, eliminarla cuando fuera necesario.

El derecho de acceso y la obligación de transparencia en torno a los datos personales almacenados por el Estado incluye también los datos biométricos, que son aquellos que permiten *“el reconocimiento sistemático de individuos basado en sus características conductuales y biológicas”*.¹² La sistematización de todos esos datos, combinada con otras fuentes de información conductual, permiten, bajo un sistema de probabilidad, identificar a las personas.

Cuando los Estados realizan tareas de recolección de datos deben observar estrictos criterios de necesidad y proporcionalidad al momento de determinar qué datos recolecta y cómo lo hace. Deben establecer protocolos en torno a la recolección, respetuosos de los derechos humanos y garantizar el derecho de acceso a la información respecto de las políticas y prácticas vigentes en la materia. Este proceso debe estar sujeto a control tanto administrativo como judicial.

B. Vigilancia, monitoreo e interceptación

La vigilancia individualizada está generalmente amparada en procesos penales o de investigaciones de otra índole, y comprende la interceptación o el monitoreo de comunicaciones. La vigilancia masiva de comunicaciones y datos, por su parte, supone la interceptación e inspección de cables enteros, redes, o equipos, o la compra de datos de servidores o intermediarios a un tercero.

Las tecnologías desarrolladas en las últimas décadas han simplificado y reducido dramáticamente los costos – tanto humanos como financieros– de la vigilancia digital. De ahí que su uso se haya incrementado radicalmente. Considerando estos y otros peligros que traen consigo los desarrollos tecnológicos, es mayor el compromiso que deben asumir los Estados para proteger la vida privada de los ciudadanos.

La vigilancia en internet, en cualquiera de sus formatos o matices, constituye una injerencia en la vida privada de las personas y, de ejercerse ilegítimamente y de manera masiva, puede afectar además los derechos al debido proceso y a un juicio justo, a la libertad de expresión y al acceso a la información.

¹² Asociación por los Derechos Civiles (ADC). *Si nos conocemos más, nos cuidamos mejor: Informe sobre políticas de biometría en la Argentina*. Mayo de 2015. Disponible en: <https://adcdigital.org.ar/wp-content/uploads/2016/01/Si-nos-conocemos-mas.pdf>

No toda injerencia es *per se* ilegítima. Existen supuestos excepcionales que justifican distintos niveles de injerencia de acuerdo a las circunstancias. El terrorismo y la lucha contra la delincuencia organizada, por ejemplo, suponen una obligación estatal de prevención y protección que constituye un objetivo legítimo para el uso excepcional y supervisado de tecnologías y mecanismos de vigilancia. Sin embargo, los Estados deben garantizar la adecuación de estas medidas a los derechos humanos.

En la misma línea, la recolección sistematizada de datos públicos –voluntariamente expuestos por el propietario de dichos datos, como publicaciones en blogs redes sociales, o cualquier otra intervención de dominio público- constituye una injerencia en la vida privada de las personas. El hecho de que la persona deje rastros públicos de sus actividades no habilita al Estado a recolectarla sistemáticamente, salvo en las circunstancias específicas donde dicha injerencia estuviera justificada. Es necesario, en esos casos, analizar la medida a la luz del test tripartito –la medida debe ser legal, en sentido formal y material, necesaria y proporcionada–.

En vista del riesgo intrínseco de abuso de cualquier sistema de vigilancia, estas medidas deben basarse en legislación particularmente precisa, con reglas claras y detalladas. Los objetivos conforme a los cuales se habilite el monitoreo o la interceptación de comunicaciones deben constar expresamente en la ley y en todos los casos deberán establecer la necesidad de una orden judicial previa. La naturaleza de las medidas, al igual que su alcance y duración han de estar reguladas, estableciendo los hechos que podrían dar lugar a dichas medidas y los organismos competentes para autorizarlas, implementarlas y supervisarlas.

Algunos Estados en la región han adquirido nuevas tecnologías de vigilancia cuyo proceso de adquisición, uso, disposición y supervisión carecen de regulación o difusión suficiente. Las leyes y políticas en torno a la naturaleza, alcance, e implementación de mecanismos de interceptación y monitoreo deben ser públicas y el Estado está obligado a aplicar el principio de máxima divulgación en el acceso a esa información. Esto abarca tanto las políticas y prácticas en torno a la vigilancia electrónica, como la adquisición, desarrollo, o actualización de los sistemas disponibles para ello.

Al establecer una restricción al acceso a la información sobre los sistemas de vigilancia, los Estados deben demostrar la necesidad de cualquier medida tendiente a mantener en secreto cierta información para proteger la seguridad nacional y el orden público. El concepto de seguridad nacional no puede ser interpretado de cualquier forma y debe ser definido desde una perspectiva democrática.

Cabe reiterar que las medidas de vigilancia deben ser ordenadas por un juez u órgano jurisdiccional competente, independiente e imparcial, y la orden debe estar debidamente fundada y observar el debido proceso.

En términos de transparencia, los Estados deben publicar estadísticas respecto al número de solicitudes realizadas, aprobadas y rechazadas, el tipo de investigación de la que hacen parte, la duración de dichas medidas y el desglose de solicitudes por proveedor, entre otros. Los intermediarios, por su parte, tienen un rol particularmente importante en esta materia. Los Estados muchas veces dependen de la aquiescencia o colaboración de estos actores privados, y existen numerosas iniciativas tendientes a obligarlos a llevar registros, o a que controlen o monitoreen las actividades de sus usuarios.

Los intermediarios deben difundir información respecto a los procesos que implementen, indicando por lo menos de manera agregada el número y alcance de las solicitudes que reciben para entregar datos por solicitud oficial.

C. Encriptación y anonimato

Para muchos individuos, la expresión de una opinión en Internet pueden conllevar represalias. Es por ello, que los Estados tienen la obligación de respetar el discurso anónimo como ejercicio de la privacidad y la

libertad de expresión, y solo excepcionalmente exigir la autenticación o identificación fehaciente de quien se expresa, aplicando un criterio de proporcionalidad.

El sector privado también debe proteger el discurso anónimo, evitando imponer en sus plataformas requisitos de identificación que la propia ley no establece. El anonimato protege la privacidad de los individuos y potencia la libertad de expresión al permitir la participación no identificada en el debate público.

Sin perjuicio de lo anterior, los Estados pueden tomar medidas para identificar a una persona en el marco de una investigación judicial en los términos que señala este informe. El anonimato puede levantarse, por ejemplo, cuando el discurso no estuviera amparado por el derecho a la libertad de expresión –como es el caso del discurso que hace propaganda en favor de la guerra, la apología del odio que incite a la violencia, la incitación al genocidio y la explotación sexual de menores–.

En la misma medida, la encriptación es un recurso tendiente a proteger la privacidad de la información en la era digital, y consiste en la codificación de los datos para que solo los destinatarios puedan acceder a ellos. Las medidas que restringen la encriptación reducen entonces la habilidad de las personas para protegerse frente a invasiones ilegítimas de su privacidad e intimidad. Estas medidas no deben ser adoptadas por los Estados salvo excepcionalmente y en tanto sean legales, necesarias y proporcionales.

D. Big Data

Big Data es un término que refiere a la inmensa cantidad de datos generados en la red, susceptibles de ser almacenados, administrados, analizados y sistematizados en busca de tendencias y perfiles.

El análisis de datos permitiría evaluar necesidades y tendencias sociales que potencialmente permitirían la adopción de más y mejores políticas públicas en aras de garantizar los derechos humanos de las personas. Pero, en la misma medida, grandes empresas privadas están actualmente dedicadas al desarrollo de tecnologías que les permitan analizar datos a gran escala para evaluar tendencias de mercado, preferencias, perfiles demográficos e inclinaciones políticas y culturales, entre muchas otras variables.

Muchas de las tecnologías que se están utilizando no solo permiten el análisis objetivo de datos y tendencias, sino que inescindiblemente permiten la identificación de los usuarios que conforman la masa crítica analizada, o generan riesgos de discriminación y arbitrariedad. Los Estados deben procurar que tanto en el ámbito público como en el privado la tecnología y desarrollos del *Big Data* garanticen la protección de los derechos humanos en internet.

E. Internet de las Cosas

En el futuro próximo los objetos serán capaces de comunicarse entre sí sin intervención humana. Internet se convertirá entonces en una experiencia física de objetos que recogerán constantemente información sobre las personas –un internet de las cosas (*internet of things*)–. La Relatoría Especial reconoce que el rápido cambio tecnológico que caracteriza esta época dificulta la comprensión anticipada de las consecuencias sociales que tiene una tecnología. Corresponde a los Estados, en nombre de sus ciudadanos, comprender lo que implican las nuevas tecnologías en materia de políticas públicas y asegurar que funcionen en aras del interés público con las suficientes protecciones para los usuarios y sus derechos humanos.

6. Bibliografía

- Access Now. 'Position Paper: Understanding the "right to be forgotten" globally'. Septiembre 2016.
- APC y Derechos Digitales, Coding Rights. Latin America in a Glimpse, 2015.
- Artículo 19. El Derecho a Compartir: Principios de la Libertad de Expresión y los derechos de propiedad intelectual en la Era Digital, 2013.
- Artículo 19. 'The "Right to be forgotten": remembering freedom of expression'. Policy Brief, 2016.
- Asociación por los Derechos Civiles (ADC). Si nos conocemos más, nos cuidamos mejor: Informe sobre políticas de biometría en la Argentina, 2015.
- Comisión Interamericana de Derechos Humanos, Informe Anual de la Relatoría Especial para la Libertad de Expresión, 2008.
- Comisión Interamericana de Derechos Humanos. Informe Anual de la Relatoría Especial para la Libertad de Expresión, 2013.
- Comisión Interamericana de Derechos Humanos Informe Anual de la Relatoría Especial para la Libertad de Expresión 2015.
- Comisión Interamericana de Derechos Humanos Relatoría Especial para la Libertad de Expresión. Comunicado de prensa R80/15, 21 de julio de 2015.
- Corte Interamericana de Derechos Humanos. Caso Escher vs. Brasil. Sentencia de 6 de julio de 2009. Fondo, Reparaciones y Costas. Serie C No. 200.
- Comisión Interamericana de Derechos Humanos. Demanda ante la Corte Interamericana de Derechos Humanos contra la República de Costa Rica. No. 12.367, Caso 'La Nación Mauricio Herrera Ulloa y Fernán Vargas Rohrmoser', 28 de enero de 2002.
- Convención Americana sobre Derechos Humanos.
- Cumbre Mundial sobre la Sociedad de la Información. Declaración de Principios, Construir la Sociedad de la Información: un desafío global para el nuevo milenio. Ginebra 2003- Túnez 2005. Doc. WSIS-03/GENEVA/4-S. 12 de mayo de 2004.
- Cumbre Mundial sobre la Sociedad de la Información. Agenda de Túnez para la Sociedad de la Información. Doc. WSIS-05/TUNIS/DOC/6(Rev.1)-S. 28 de junio de 2006.
- Declaración de Berlín sobre Acceso Abierto al Conocimiento en Ciencias y Humanidades, promovida por la Sociedad Max Planck en 22 de octubre de 2003 y firmada por alrededor de 400 instituciones académicas y científicas.
- Declaración sobre la Iniciativa de Budapest para el Acceso Abierto. Iniciativa de Acceso Abierto de Budapest, 14 de febrero de 2002.
- Federal Communications Commission. Protecting and Promoting the Open internet. 80 FR 19737. 13 de abril de 2015.
- Internet Rights and Principles Coalition. Carta de Derechos Humanos y Principios de Internet, 2015.
- Organización de Naciones Unidas, Comité de Derechos Humanos. Observación General N° 31, Naturaleza de la obligación jurídica general impuesta a los Estados Partes en el Pacto. UN Doc. CCPR/C/21/Rev.1/Add.13. 26 de mayo de 2004.
- Organización de Estados Americanos. Comité Jurídico Interamericano. Privacidad y Protección de Datos Personales. OEA/Ser.Q CJI/doc. 474/15 rev.2. (86° período ordinario de sesiones, Río de Janeiro, Brasil). 26 de marzo de 2015.
- Organización de Naciones Unidas. Asamblea General. El derecho a la privacidad en la era digital. UN Doc. A/RES/68/167. 21 de enero de 2014.
- Organización de Estados Americanos. Asamblea General. Declaración de Santo Domingo. Gobernabilidad y Desarrollo en la Sociedad del Conocimiento. OEA Doc. AG/DEC. 46 (XXXVI-O/06). 6 de junio de 2006.

- Organización de Naciones Unidas, Asamblea General. Resolución 70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información. UN Doc. A/RES/70/125. 1 de febrero de 2016.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, Frank La Rue. UN Doc. A/HRC/23/40. 17 de abril de 2013.
- Organización de Naciones Unidas. Asamblea General. 'Outcome document of the high-level meeting of the General Assembly on the overall review of the implementation of the outcomes of the World Summit on the Information Society'. UN Doc. A/70/L.33. 13 de diciembre de 2015.
- Organización de Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. A/HRC/17/27. 16 de mayo de 2011.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe de la Relatora Especial sobre los derechos culturales, Farida Shaheed. UN Doc. A/HRC/28/57. 24 de diciembre de 2014.
- Organización de Naciones Unidas. Asamblea General. Informe del Relator Especial sobre la promoción y la protección del derecho a la libertad de opinión y expresión, Frank La Rue. UN Doc. A/66/290. 10 de agosto de 2011.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, Frank La Rue. UN Doc. A/HRC/11/4. 30 de abril de 2009.
- Organización de Naciones Unidas. Asamblea General. Resolución 68/181. Promoción de la Declaración sobre el Derecho y el Deber de los Individuos, los Grupos y las Instituciones de Promover y Proteger los Derechos Humanos y las Libertades Fundamentales Universalmente Reconocidos: protección de las defensoras de los derechos humanos y los defensores de los derechos de la mujer. UN Doc. A/RES/68/181. 30 de enero de 2014.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. El derecho a la privacidad en la era digital. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos. A/HRC/27/37. 30 de junio de 2014.
- Organización de Naciones Unidas. Asamblea General. Resolución 70/125. Documento final de la reunión de alto nivel de la Asamblea General sobre el examen general de la aplicación de los resultados de la Cumbre Mundial sobre la Sociedad de la Información, UN Doc. A/RES/70/125. 1 de febrero de 2016.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, David Kaye. UN Doc. A/HRC/32/38. 11 de mayo de 2016.
- Organización de Naciones Unidas, Oficina del Alto Comisionado de Derechos Humanos. Principios rectores sobre las empresas y los derechos humanos. Puesta en práctica del marco de las Naciones Unidas para "proteger, respetar y remediar". 2011.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y expresión, David Kaye. UN Doc. A/HRC/32/38. 11 de mayo de 2016.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe de la Relatora Especial sobre los derechos culturales, Farida Shaheed. UN Doc. A/HRC/28/57. 24 de diciembre de 2014.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe de la Oficina del Alto Comisionado de las Naciones Unidas para los Derechos Humanos: El derecho a la privacidad en la era digital. UN Doc. A/HRC/27/37. 30 de junio de 2014.
- Organización de Naciones Unidas. Consejo de Derechos Humanos. Informe del Relator Especial sobre la promoción y protección del derecho a la libertad de opinión y de expresión, David Kaye. UN Doc. A/HRC/29/32. 22 de mayo de 2015.

- Organización Panamericana de la Salud. Conversaciones sobre Salud. Gestión de información, diálogos e intercambio de conocimientos para acercarnos al acceso universal a la salud, 2014. Organización de Estados Americanos. Asamblea General. Declaración de Santo Domingo. Gobernabilidad y Desarrollo en la Sociedad del Conocimiento. OEA Doc. AG/DEC. 46 (XXXVI-O/06). 6 de junio de 2006.
- Principios globales sobre seguridad nacional y el derecho a la información ('Principios de Tshwane'), publicado por Open Society Foundations. 12 de junio de 2013.
- Relator Especial de Naciones Unidas sobre la promoción y protección del Derecho a la Libertad de Opinión y Expresión (ONU), el Representante para la Libertad de Medios de Comunicación de la Organización de Seguridad y Cooperación en Europa (OSCE), y el Relator Especial para la Libertad de Expresión de la Comisión Interamericana (OEA). Declaración Conjunta sobre Desafíos a la Libertad de Expresión en el Nuevo Siglo. 2001.
- Relator Especial de las Naciones Unidas para la Libertad de Opinión y Expresión, Representante de la Organización para la Seguridad y Cooperación en Europa para la Libertad de los Medios de Comunicación y Relator Especial de la OEA para la Libertad de Expresión. Declaración Conjunta Sobre internet y sobre Medidas Anti-Terroristas, 21 de diciembre de 2005.
- Relator Especial de las Naciones Unidas para la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos. Declaración Conjunta sobre Wikileaks, 21 de diciembre de 2010.
- Relator Especial de las Naciones Unidas (ONU) sobre la Promoción y Protección del derecho a la Libertad de Opinión y de Expresión, Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE), Relatora Especial de la Organización de Estados Americanos (OEA) para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). Declaración conjunta sobre libertad de expresión e internet, 1 de junio de 2011.
- Relator Especial de las Naciones Unidas (ONU) sobre la Protección y Promoción del Derecho a la Libertad de Opinión y de Expresión y Relatora Especial para la Libertad de Expresión de la Comisión Interamericana de Derechos Humanos (OEA). Declaración conjunta sobre programas de vigilancia y su impacto en la libertad de expresión. 21 de junio de 2013.
- Relator Especial de las Naciones Unidas (ONU) para la Libertad de Opinión y de Expresión; Representante para la Libertad de los Medios de Comunicación de la Organización para la Seguridad y la Cooperación en Europa (OSCE); Relator Especial de la OEA para la Libertad de Expresión, y Relatora Especial sobre Libertad de Expresión y Acceso a la Información de la Comisión Africana de Derechos Humanos y de los Pueblos (CADHP). Declaración Conjunta sobre Libertad de Expresión y Noticias Falsas ('Fake News'), Desinformación y Propaganda, marzo de 2017.
- República de Argentina. Ley 25.078 Argentina Digital. Boletín Oficial No. 33.034. 19 de Diciembre de 2014. Artículos 1, 56 y 57.
- República Federativa de Brasil. Ley No. 12.965. Marco Civil de Internet. 23 de abril de 2014.
- República de Chile. Ley 20.453. 20 de agosto de 2010.
- Estados Unidos Mexicanos. Ley Federal de Telecomunicaciones y Radiodifusión. 14 de julio de 2014.
- República de Paraguay. Comisión Nacional de Telecomunicaciones. Resolución 190/2009, 11 de marzo de 2009.
- Tribunal de Justicia de la Unión Europea. Google Spain, S.L., Google Inc. / Agencia Española de Protección de Datos, Mario Costeja González. Sentencia del 13 de mayo de 2014.
- Unesco, Universalidad de internet: un medio para crear sociedades del conocimiento y la agenda de desarrollo sostenible después de 2015, 2 de septiembre de 2013.
- Unesco, Digital Literacy in Education. Policy Brief, mayo 2011.
- Unesco, Fostering Freedom Online: The role of internet Intermediaries. Unesco Series on internet Freedom. Internet Society (2014).
- Unesco Countering Online Hate Speech. Unesco Series on internet Freedom. internet Society. 2015.

- Unesco, Carta sobre la Preservación del Patrimonio Digital. 15 de octubre de 2003. The internet Society. The internet of Things (IoT): An Overview Understanding the Issues and Challenges of a More Connected World. Octubre de 2015.
- Unión Internacional de Telecomunicaciones. 'Big Data – Cloud computing based requirements and capabilities'. ITU-T Series Y: Global information infrastructure, internet protocol aspects and next-generation networks. Recommendation ITU-T Y.3600. Noviembre de 2015.